SOP-EDM-01-M02 Políticas del Sistema de Gestión Integral

Dirección de Operaciones

Teléfono. (55) 63631905
Mail info@tecnologiaseficientesdevilla.com
RFC TEV150303HR6
Dirección AV. ADOLFO RUIZ CORTINEZ, NÚM. EXT. 1344, NÚM. INT. ED-2, COL. GALAXIAS TABASCO 2000, VILLAHERMOSA TABASCO, C.P. 86035.
https://tecnologiaseficientesdevilla.com
TECNOLOGÍAS EFICIENTES DE VILLA, S.A.P.I. DE C.V.

Índice

1. Introducción

Para consolidar un Sistema de Gestión Integral (SGI) que responda con excelencia a los desafíos de **Tecnologías Eficientes de Villa**, es imperativo implementar controles eficaces que garanticen la integridad de nuestra operación. El presente documento establece las políticas marco del SGI, cuyo cumplimiento es de carácter obligatorio para todo el personal, la alta dirección, proveedores, visitantes y terceros vinculados con la organización.

Nuestro marco normativo se fundamenta en el cumplimiento de la legislación mexicana, los compromisos contractuales y las mejores prácticas internacionales certificadas bajo los estándares **ISO 9001, 14001, 20000-1, 22301, 27001 y 37001**. La alta dirección ratifica estas directrices como una prioridad estratégica y exhorta a todos los colaboradores y aliados a velar por el cumplimiento de las políticas aquí establecidas para asegurar la sostenibilidad y la confianza en nuestros servicios.

2. Objetivo

Establecer y comunicar formalmente las políticas que regulan la operación de **Tecnologías Eficientes de Villa**, detallando los componentes esenciales para su ejecución. La entidad garantiza que estas disposiciones sean conocidas y acatadas por todos los grupos de interés internos y externos que interactúan con la organización, consolidando así un entorno de cumplimiento y transparencia.

3. Alcance

Las políticas aplican a los artefactos con los que se busca satisfacer las necesidades de los clientes; a los activos de información que los apoyan; y al personal, la dirección, proveedores, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con **Tecnologías Eficientes de Villa**.

4. Aplicabilidad

Las políticas del Sistema de Gestión Integral de **Tecnologías Eficientes de Villa.**aplican de manera obligatoria a todo el personal, a la dirección, a las personas proveedoras, visitantes y terceras partes que brinden servicios o tengan relación con **Tecnologías Eficientes de Villa**, así como a la totalidad de sus personas usuarias.

5. Términos y Definiciones

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

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

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

Alta dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

ARCO: Son los derechos de Acceso, Rectificación, Cancelación y Oposición que manejan los particulares.
Auditor: Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

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

Aspecto ambiental: Es un elemento de las labores, los productos o los servicios que realiza una empresa y que, a su vez, puede tener una relación con el medio ambiente.
Buzón de sugerencias: Herramienta física o electrónica que sirve para recolectar las sugerencias de mejora hechas por las partes interesadas del SGSI.

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

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

Compromisos Antisoborno: Son las acciones específicas que una organización toma para prevenir el soborno, como establecer políticas claras, asignar responsabilidades y capacitar al personal.

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

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

Conflicto de intereses situación donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el juicio de valor del personal (3.25) en el desempeño de sus obligaciones hacia la organización (3.2

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

Contexto externo:
Ambiente externo en el que la organización busca alcanzar sus objetivos.
[Fuente: Guía ISO 73: 2009]: El contexto externo puede incluir el entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local. También factores y tendencias clave que tienen impacto en los objetivos de la organización o relaciones y percepciones y valores de partes interesadas externas.

Contexto interno: Ambiente interno en el que la organización busca alcanzar sus objetivos.

[Fuente: Guía ISO 73: 2009]: El contexto interno puede incluir:
- gobernanza, estructura organizativa, roles y responsabilidades;
- políticas, objetivos y las estrategias que existen para lograrlos;
- las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías);
- sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales);
- relaciones y percepciones y valores de las partes interesadas internas;
- la cultura de la organización;

- normas, directrices y modelos adoptados por la organización;
- forma y alcance de las relaciones contractuales.

Control: Medida por la que se modifica el riesgo.

[Fuente: ISO Guide 73:2009] Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

Declaración de aplicabilidad (SOA - Statement of Applicability): Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Debida Diligencia: Proceso mediante el cual se investiga y evalúa a terceros (como proveedores, socios comerciales o clientes) para identificar posibles riesgos de soborno.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

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

Desempeño ambiental: Son los resultados de la Gestión Ambiental de la empresa respecto a sus objetivos ambientales, estos resultados pueden ser medidos.

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

Eficacia grado en el cual se realizan las actividades planificadas y se logran los resultados planificados

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

[Fuente: ISO Guide 73: 2009]: Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente".

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

Función de cumplimiento antisoborno personas con responsabilidad y autoridad para la operación del sistema de gestión antisoborno

Funcionario público toda persona que ocupe un cargo legislativo, administrativo o judicial, por designación, elección o como sucesor, o cualquier persona que ejerza una función pública, incluso para un organismo público o una empresa pública, o cualquier funcionario o agente de una organización pública local o internacional, o cualquier candidato a un cargo público

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [Fuente: ISO Guide 73:2009].

Hueco de seguridad: Vulnerabilidad de un sistema de información que permite mediante su explotación violar la seguridad.

Impacto: El coste para la empresa de un incidente.

Impacto ambiental: Es cualquier modificación del medio, el impacto puede ser negativo, positivo o sinérgico, siendo generado por la empresa.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las área de Operaciones del negocio y amenazar la seguridad de la información.

Información: Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida.

La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros).

Información pública: Todas las personas, dentro y fuera de la organización, tienen acceso. Su divulgación no causa perjuicios.

Información privada: Será clasificada como información privada aquella cuya publicación comprometa la seguridad de **Tecnologías Eficientes de Villa**. Es información crítica que solo podrá ser accedida por personal autorizado que requiera de su conocimiento para estricto cumplimiento de sus funciones.

Información confidencial: Es Información crítica, de alta importancia para la empresa que solo puede ser accedida al interior de la empresa por el personal autorizado de acuerdo al SGSI.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. propiedad/característica de salvaguardar la exactitud y completitud de los activos.

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

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

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

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

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

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas.

Objetivo ambiental: Es una meta ambiental que se propone la empresa de manera coherente con su política ambiental.

Objetivo: Resultado a alcanzar.

Un objetivo puede ser estratégico, táctico u operativo. Los objetivos pueden relacionarse con diferentes disciplinas (como las metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, proyecto, producto y proceso). Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de seguridad de la información o mediante el uso de otras palabras con un significado similar (por ejemplo, propósito, meta o hito).

Organización: persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones con lograr sus objetivos.

Órgano de gobierno grupo u órgano que tiene la responsabilidad y autoridad final respecto de las actividades, la gobernanza y las políticas de una organización (3.2), y al cual la alta dirección (3.6) informa y por el cual rinde cuentas

Monitoreo: determinar el estado de un sistema, un proceso o una actividad.

Medio ambiente: Es el contexto donde una empresa actúa, pudiendo incluirse el agua, el aire, el suelo, los recursos naturales, la flora y la fauna, los seres humanos y todas sus interacciones.

Medición: proceso para determinar un valor.

Meta ambiental: Tiene como origen los objetivos ambientales y es necesario implantar y ejecutar para poder alcanzar dichos objetivos.
No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

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

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

Partes interesadas internas del SGSI: Factor humano (personal), gobernanza organizacional (Dirección y comités), infraestructura física y tecnológica (Soporte, Desarrollo e Infraestructura), dentro de **Tecnologías Eficientes de Villa**.

Partes interesadas externas del SGI: Clientes, usuarios, proveedores, contratistas, Gobierno, Autoridades y visitantes de **Tecnologías Eficientes de Villa**.

Partes interesadas del SGSI: Incluyes las partes interesadas internas y externas del SGSI.

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

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

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

Prevención de la contaminación: Es la utilización de cualquier técnica, producto, material o práctica que sirva para reducir en la medida de lo posible que se genere un impacto ambiental.

Requisito: necesidad o expectativa establecida, generalmente implícita u obligatoria.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Un efecto es una desviación de lo esperado: positivo o negativo.

La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.

El riesgo a menudo se caracteriza por la referencia a posibles "eventos" (Guía ISO 73: 2009) y "consecuencias" (Guía ISO 73: 2009) o una combinación de estos.

El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la "probabilidad" asociada (Guía ISO 73: 2009) de ocurrencia.

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Sistema de Gestión Ambiental: Es una parte del Sistema de Gestión de la empresa que permite fomentar y llevar a cabo la política ambiental y los objetivos marcados por la organización.

Sistema de Gestión Antisoborno: Es un conjunto de políticas, procedimientos y prácticas que una organización implementa para prevenir, detectar y tratar el riesgo de soborno.

SGSI Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Tratamiento de riesgos: Proceso para modificar el riesgo [Fuente: Guía ISO 73: 2009].

Las acciones de tratamiento del riesgo pueden contemplar:

- evitar el riesgo al decidir no comenzar o continuar con la actividad que da lugar al riesgo;
- asumir o aumentar el riesgo para aprovechar una oportunidad;
- eliminar la fuente de riesgo;
- modificar la probabilidad;
- modificar las consecuencias;
- compartir el riesgo con otra parte o partes (incluidos contratos y financiación del riesgo);
- retener el riesgo mediante una elección informada.

Las acciones de tratamiento del riesgo sobre consecuencias negativas a veces se denominan "mitigación de riesgos", "eliminación de riesgos", "prevención de riesgos" y "reducción de riesgos".

El tratamiento del riesgo puede crear nuevos riesgos o modificar los riesgos existentes.

Tercera parte persona u organismo que es independiente de la organización

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Valoración de riesgos: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

6. SOP-EDM-01-P01 Política de Seguridad de la Información

Para **Tecnologías Eficientes de Villa**, la información es un activo estratégico fundamental para el cumplimiento de nuestra visión. En consecuencia, establecemos un compromiso firme con su protección mediante una gestión integral de riesgos que abarca la prevención, vigilancia y control proactivo de las amenazas que puedan afectar la seguridad de la información y la resiliencia del negocio. La organización garantiza la asignación de recursos físicos, tecnológicos y humanos necesarios para fortalecer el **Sistema de Gestión de Integral (SGI)**. A través de su implementación y mejora continua, aseguramos los tres pilares fundamentales: **Confidencialidad, Integridad y Disponibilidad**.

6.1. Objetivo

Establecer y mantener un marco de gobernanza de Seguridad de la Información robusto y alineado a la visión de **Tecnologías Eficientes de Villa**. Este marco garantiza que la Política General permanezca vigente y responda de manera proactiva a los requisitos normativos, compromisos contractuales y estándares internacionales de excelencia adoptados por la organización.

6.2. Alcance

La política de seguridad de la información aplica a los procesos con los que se busca satisfacer las necesidades de los clientes; a los activos de información que los apoyan; y al personal, la dirección, proveedores, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con **Tecnologías Eficientes de Villa.**

6.3. Responsabilidades

6.3.1. Las partes interesadas internas del SGI son responsables de implementar las políticas, lineamientos y controles del Sistema de Gestión Integral dentro del ámbito de sus funciones y áreas de responsabilidad.

6.3.2. Todas las partes interesadas del SGI deben cumplir las disposiciones establecidas en el Sistema de Gestión Integral, abstenerse de incurrir en incumplimientos y notificar oportunamente a las instancias correspondientes cualquier omisión o desviación detectada.

6.3.3. El Senior Management Team es responsable de elaborar, actualizar y aprobar la Política de Seguridad de la Información; no obstante, las partes interesadas del SGI pueden proponer mejoras a la misma.

6.3.4. El Oficial de Seguridad de la Información es encargada de establecer el modelo de gestión en esta materia y evaluar la correcta aplicación de la metodología de identificación, análisis y valoración de riesgos dentro del SGI.

6.3.5. El Auditor es responsable de monitorear y dar seguimiento del cumplimiento a temas inherentes en la presente política; verificar que la misma se encuentre actualizada y que sea difundida, incluyendo los cambios o actualizaciones que se propongan.

6.3.6. El Gerente de Recursos Humanos es responsable de notificar al personal de **Tecnologías Eficientes de Villa.**de nuevo ingreso sobre las obligaciones respecto del cumplimiento de la presente política, asimismo, notificar los cambios que en ella se produzcan.

6.3.7. El Director de Operaciones es responsable de notificar a las partes interesadas externas del SGSI sobre las obligaciones respecto del cumplimiento de la presente política, asimismo, notificar los cambios que en ella se produzcan.

6.3.8. El Director de Operaciones es responsable de definir e implementar los mecanismos de control para la operación, administración, comunicación de los sistemas y recursos de tecnología de **Tecnologías Eficientes de Villa**.

6.3.9. El Auditor Interno es responsable de diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, que verifiquen el cumplimiento de la política de seguridad de la información.

6.3.10. Los Líderes de la Dirección de Área de Operaciones deben asegurarse de que todos los procedimientos (SOP´s) de seguridad de la información dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de **Tecnologías Eficientes de Villa**.

6.3.11. El Oficial de Seguridad de la Información es responsable de determinar Semestralmente las vulnerabilidades, amenazas y riesgos en materia de Seguridad de la Información a los que pudiera estar expuesto **Tecnologías Eficientes de Villa,** de acuerdo con el modelo de gestión de riesgos de la empresa.

6.3.12. Generalidades de la Política de Seguridad de la Información.

6.3.12.1. **Tecnologías Eficientes de Villa** estipula el compromiso de mantener íntegra, disponible y confidencial la información bajo su resguardo independientemente de la manera en que se almacene, procese o transmita, dando cumplimento a las

regulaciones y normatividad aplicables.

6.3.12.2. La Política de Seguridad de la Información, una vez aprobada y publicada, debe ser difundida a las partes interesadas del SGSI, independientemente de niveles y rangos jerárquicos al momento de su entrada en vigor, misma que debe ser revisada por lo menos una vez al año para confirmar que siga siendo actual y apropiada al entorno de **Tecnologías Eficientes de Villa.**

6.3.12.3. La Política de Seguridad de la Información deberá revisarse de forma proactiva cuando se presenten cambios que puedan afectar su pertinencia, suficiencia o eficacia. Entre los factores que detonan su revisión se consideran: la evolución del análisis riesgo beneficio de los controles implementados, el impacto derivado de incidentes de seguridad de la información y la identificación de nuevas amenazas o vulnerabilidades. Asimismo, deberán integrarse los resultados de auditorías internas o externas, las modificaciones en el marco legal y regulatorio aplicable, así como cualquier cambio tecnológico, operativo o del entorno digital que influya en la gestión de la seguridad de la información de la organización.

6.3.12.4. Los cambios en la Política de Seguridad de la Información deben estar registrados, aprobados e informados para su difusión oportuna a las partes interesadas del SGI.

7. SOP-EDM-01-P01 Política de la Organización de la Seguridad de la Información

7.1. Objetivo

El Sistema de Gestión Integral (SGI) de **Tecnologías Eficientes de Villa** se implementa a través de una estructura organizacional orientada a la gestión y mitigación de riesgos. Este modelo define roles y responsabilidades específicas que articulan las actividades de seguridad de la información con el Senior Management Team (SMT), garantizando la continuidad operativa, el soporte técnico y el cumplimiento de los estándares y niveles de servicio establecidos.

7.2. Alcance

La presente política es de cumplimiento obligatorio para todas las partes interesadas vinculadas al Sistema de Gestión Integral y aplica a la totalidad de los activos de información de la organización. La gestión y supervisión de estos activos se realiza bajo los lineamientos del documento **SOP-BAI-09-F03 Inventario de Activos**, asegurando que cada recurso tecnológico y de información cuente con los controles de seguridad adecuados a su criticidad.

7.3. Responsabilidades

7.3.1. Las partes interesadas internas del SGI son responsables de implementar la Política de la Organización de la Seguridad de la Información dentro de sus áreas de responsabilidad.

7.3.2. Las partes interesadas del SGI son responsables de dar cumplimiento a la Política de la Organización Seguridad de la Información y abstenerse de cometer infracciones a la misma, así como notificar a las partes interesadas relevantes cualquier omisión que se conozca sobre el cumplimiento de dicha política.

7.3.3. El Director de Operaciones es responsable de establecer y conformar los roles y responsabilidades para la Seguridad en los Sistemas de Información y la Tecnología.

7.3.4. El Gerente de Recursos Humanos es responsable de establecer el perfil de puestos de las áreas que conforman a **Tecnologías Eficientes de Villa**; y deberá llevar a cabo la formalización y asignación de los roles y responsabilidades requeridos en materia de Seguridad de la Información.

7.3.5. El Gerente de Recursos Humanos es responsable de coordinar el directorio de contactos relacionados con protección civil.

7.3.6. El Director de Operaciones es responsable de definir e implementar los mecanismos de control para el manejo de dispositivos móviles que se conectan a redes públicas, y los mecanismos de control para salvaguardar la información que se almacena en ellos.

7.3.7. El Oficial de Seguridad de la Información es responsable de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política de Seguridad de la Información, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

7.3.8. El Gerente de Recursos Humanos es responsable de notificar al personal de **Tecnologías Eficientes de Villa** de nuevo ingreso sobre las obligaciones respecto del cumplimiento de la presente política, asimismo, notificar los cambios que en ella se produzcan.

7.3.9. SOP-EDM-01-P01-01 Roles y responsabilidades de la Seguridad de la Información.

7.3.9.1. El Gerente de Recursos Humanos con apoyo del Oficial de Seguridad de la Información deben establecer y formalizar, las funciones, los roles y responsabilidades en materia de Seguridad de la Información en los perfiles de

puesto, los cuales deben ser revisados por lo menos una vez al año para confirmar que sigan siendo actuales y apropiados, o cuando sea requerido un cambio que afecte a la Seguridad de la Información.

7.3.9.2. El Gerente de Recursos Humanos debe contar con el organigrama pertinente que marquen los niveles de jerarquía y autorización en materia de Seguridad de la Información.

7.3.9.3. El Gerente de Recursos Humanos debe tener evidencia sobre la asignación de los roles y responsabilidades en materia de Seguridad de la Información y que son cubiertos por el personal competente para el ejercicio de sus funciones.

7.3.9.4. El Oficial de Seguridad de la Información debe asegurarse que la definición de los roles y responsabilidades en materia de Seguridad de la Información, estén basados en sensibilidad de los activos de información que se utilizan en las funciones del puesto.

7.3.9.5. El Oficial de Seguridad de la Información debe asegurarse que los roles y responsabilidades en materia de Seguridad de la Información empaten o tengan coherencia con el inventario de activos, en el cual se define al responsable del activo.

7.3.10. SOP-EDM-01-P01-02 Segregación de funciones.

7.3.10.1. El Director de Operaciones, debe asegurar la segregación entre las funciones de gestión y ejecución, con el propósito de reducir el riesgo de modificaciones no autorizadas o el uso indebido de los activos de información. Esta disposición incluye los procesos delegados a personas proveedoras o terceras partes.

7.3.10.2. El Oficial de Seguridad de la Información debe realizar revisiones periódicas y programadas para verificar que ninguna persona ejecute actividades dentro de un ámbito de responsabilidad exclusiva sin los mecanismos de supervisión o monitoreo correspondientes.

7.3.11. SOP-EDM-01-P01-03 Contacto con autoridades.

7.3.11.1. El Oficial de Seguridad de la Información es responsable de mantener y validar un directorio de contactos de emergencia para la atención de incidentes que afecten la integridad de los activos o la continuidad operativa. Este registro debe someterse a revisiones periódicas y actualizaciones inmediatas ante cualquier cambio en la estructura de los contactos identificados.

7.3.11.2. El Oficial de Seguridad de la Información debe asegurarse que existe un protocolo que especifique el método de contacto de acuerdo con la naturaleza de cada incidente.

7.3.11.3. El Oficial de Seguridad de la Información debe asegurarse que, para el contacto con autoridades de servicios de emergencia como policías, bomberos, grupos de asistencia, entre otros, el directorio sea público y que facilite determinar el protocolo de contacto.

7.3.11.4. El personal de **Tecnologías Eficientes de Villa** debe evitar el mal uso del protocolo de contacto y el acceso no autorizado al directorio de contactos.

7.3.12. SOP-EDM-01-P01-04 Contacto con Grupos de Interés.

7.3.12.1. El Oficial de Seguridad de la Información debe mantener un directorio actualizado de personas proveedoras, en el que se identifiquen las áreas o responsables designados dentro de **Tecnologías Eficientes de Villa,** así como el objeto y alcance de la relación contractual o de servicio con la organización.

7.3.12.2. El Oficial de Seguridad de la Información debe asegurarse que cualquier intercambio de información relacionada con **Tecnologías Eficientes de Villa**, debe estar controlado formalmente por medio de acuerdos de confidencialidad con cada proveedor.

7.3.13. SOP-EDM-01-P01-05 Seguridad de Información de los Proyectos.

7.3.13.1. Los Líderes de la Dirección de Operaciones deben definir e implementar mecanismos de control para corroborar la integridad, disponibilidad y confidencialidad de la información que es gestionada en la administración de proyectos.

7.3.13.1.1. El Director de Operaciones de la información debe asegurarse que la planeación de un proyecto o de la implementación de un nuevo servicio, debe incluir una evaluación en materia de Seguridad de la Información para verificar la alineación y cumplimiento con la estrategia y políticas de seguridad de la información aplicables.

7.3.13.2. El Director de Operaciones debe asegurarse que derivado de la evaluación del proyecto, se deben definir e implementar los mecanismos de control aplicables en

materia de Seguridad de la Información, dentro del desarrollo del proyecto o nuevo servicio.

7.3.13.3. El Director de Operaciones debe asegurarse que la planeación de un proyecto o la implementación de un nuevo servicio debe incluir una evaluación en materia de Gobierno de Datos para identificar y establecer los requerimientos de calidad de la información, así como la integración y estandarización de la información que será generada, recibida, transmitida, procesada y almacenada en los sistemas y aplicaciones de **Tecnologías Eficientes de Villa**.

7.3.13.4. Los Líderes de la Dirección de Área de Operaciones deben definir e implementar los mecanismos de control automáticos que corroboren el cumplimiento de los requerimientos de calidad, integración y estandarización de la información con los sistemas y aplicaciones de **Tecnologías Eficientes de Villa.**

7.3.14. SOP-EDM-01-P01-06 Uso de dispositivos móviles.

7.3.14.1. El uso de dispositivos de almacenamiento externo podrá autorizarse exclusivamente para fines laborales relacionados con el intercambio de información, siempre que dichos dispositivos cuenten con controles que garanticen la integridad, confidencialidad y disponibilidad de la información. Esta autorización deberá ser otorgada por una persona con nivel jerárquico no inferior a Dirección, quien asumirá corresponsabilidad respecto al uso adecuado y la protección de la información.

7.3.14.2. El personal con acceso a información de **Tecnologías Eficientes de Villa**, por medio de dispositivos móviles o dispositivos de almacenamiento externo, debe hacer uso responsable de la información. En caso de pérdida del dispositivo ya sea propiedad de **Tecnologías Eficientes de Villa** o personal, debe ser reportado de manera inmediata como un incidente de seguridad de la información, buscando cuidar la información en uso y custodia de **Tecnologías Eficientes de Villa**.

7.3.14.3. Está prohibido copiar, almacenar o transportar cualquier tipo de información que sea confidencial o sensible, en dispositivos móviles o de almacenamiento externo que no estén autorizados o en equipo personal.

7.3.14.4. Para la transmisión de la información solo es posible utilizar los repositorios seguros propiedad/arrendados de **Tecnologías Eficientes de Villa.**

7.3.14.5. El acceso y uso de servicios de almacenamiento personal en línea, es decir, aquellas unidades virtuales de almacenamiento personal por medio de Internet

están prohibidos, las cuales incluyen, pero no se limitan a Google Drive, Dropbox, Rapidshare, MediaFire, etcétera.

7.3.14.6. Está prohibido otorgar acceso a información y sus activos relacionados por medio de dispositivos móviles, al personal externo, aliados estratégicos, contratistas y usuarios de terceras partes, exceptuando el acceso por medio la plataforma institucional de colaboración o de una laptop que cuente con los mecanismos de control para el manejo de dispositivos móviles establecidos y cuente con las autorizaciones correspondientes.

7.3.14.7. Para los dispositivos móviles personales se deben considerar la elaboración de un instructivo de uso de dispositivos móviles de acuerdo a los requisitos de seguridad de la información.

7.3.15. SOP-EDM-01-P01-07 Trabajo Remoto.

7.3.15.1. Se deben definir e implementar mecanismos de autenticación y uso de redes seguras para el uso de los aplicativos Institucionales cuando se acceda a ellos a través de redes públicas, ya sea por dispositivos propiedad de **Tecnologías Eficientes de Villa.**o personales.

7.3.15.2. Solo el personal de nivel estratégico y táctico de **Tecnologías Eficientes de Villa.**debe contar con mecanismos de Autenticación y uso de redes seguras para el uso de los aplicativos Institucionales, a través de redes públicas; en caso de que otro nivel requiera el acceso, éste debe estar aprobado y justificado por un nivel no menor a director.

7.3.15.3. Los mecanismos de Autenticación y uso de redes seguras para el uso de los aplicativos Institucionales serán los siguientes:

- Bóveda de contraseñas
- Doble factor de autenticación (Administración de Servidores)

7.3.15.4. Cuando ocupe equipos personales para el desempeño de sus funciones en **Tecnologías Eficientes de Villa**, como equipos de telefonía celular, computadoras personales, Tablet o cualquier herramienta, se deberá de firmar la carta de uso de aplicativos personales, donde el colaborador se responsabiliza del uso que se le dé a la información.

8. SOP-EDM-01-P02 Política de Seguridad de la Información en los Recursos Humanos

8.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para corroborar que el personal de **Tecnologías Eficientes de Villa** cuente con el acceso a la información acorde al rol que desempeñan, entiendan sus responsabilidades en el ejercicio de sus funciones previo, durante y al finalizar la relación laboral con **Tecnologías Eficientes de Villa**.

Establecer las medidas de control preventivas, de detección y correctivas para corroborar que el personal externo, aliados estratégicos, contratistas y usuarios de terceras partes tengan acceso a la información acorde al rol que desempeñan, entiendan sus responsabilidades en el ejercicio de sus funciones previo, durante y al finalizar la prestación de servicio.

8.2. Alcance

Esta política aplica a las partes interesadas en el SGSI; así como a los activos de información con los que cuenta **Tecnologías Eficientes de Villa.**y los cuales están detallados en el Registro de Activos de **Tecnologías Eficientes de Villa**.

8.3. Responsabilidades

8.3.1. Las partes interesadas internas son responsables de implementar y dar cumplimiento a la Política de Seguridad de la Información en los Recursos Humanos dentro de sus áreas de responsabilidad.

8.3.2. Las partes interesadas del SGSI son responsables de dar cumplimiento a la Política de Seguridad de la Información en los Recursos Humanos y abstenerse de cometer infracciones a la misma, así como notificar a las partes interesadas relevantes cualquier omisión que se conozca sobre el cumplimiento de dicha política.

8.3.3. El personal Directivo de **Tecnologías Eficientes de Villa.**es responsable de exhortar y facilitar la adopción y conciencia de la Seguridad de la Información.

8.3.4. El Gerente de Recursos Humanos es responsable de definir e implementar los mecanismos de control para la verificación de antecedentes de los candidatos, los términos y condiciones del empleo, así como para el cambio de funciones y término de la relación laboral en materia de Seguridad de la Información.

8.3.5. El Gerente de Recursos Humanos con apoyo del Oficial de Seguridad de la Información son responsables de definir e implementar el plan de entrenamiento y concienciación en materia de Seguridad la Información.

8.3.6. La Consejería Jurídica es responsable de apoyar al área que realiza las funciones de recursos humanos a determinar los términos para el cumplimiento de los requerimientos normativos, las leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa.**referentes a esta política.

8.3.7. El Oficial de Seguridad de la Información y el auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

8.3.8. El Gerente de Recursos Humanos es responsable de notificar al personal de **Tecnologías Eficientes de Villa** de nuevo ingreso sobre las obligaciones respecto del cumplimiento de la presente política, asimismo, notificar los cambios que en ella se produzcan.

8.3.9. La Dirección de Operaciones y la Gerencia de Compras son responsable de notificar al personal externo sobre las obligaciones respecto del cumplimiento de la presente política, asimismo, notificar los cambios que en ella se produzcan.

8.3.10. SOP-EDM-01-P02-01 Verificación de antecedentes

8.3.10.1. Se debe llevar a cabo la verificación de autenticidad de la información del candidato entre las cuales se debe incluir: identidad, currículum vitae, títulos académicos y profesionales, referencias personales y profesionales satisfactorias, exámenes psicométricos, estudio socioeconómico.

8.3.10.2. La verificación de autenticidad debe realizarse por medio de los canales formales de comunicación como correo electrónico.

8.3.10.3. Se debe contar con la autorización por parte del candidato sobre el uso y tratamiento de sus datos personales dentro de **Tecnologías Eficientes de Villa** de acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

8.3.10.4. Se debe corroborar que el personal cuente con competencia profesional para el

ejercicio de sus funciones con base en los roles y responsabilidades que le serán asignados.

8.3.11. SOP-EDM-01-P02-02 Términos y condiciones del empleo

8.3.11.1. El personal de **Tecnologías Eficientes de Villa** debe contar con un acuerdo de confidencialidad y no divulgación de información del **Tecnologías Eficientes de Villa**, así como del uso aceptable de los activos de información que utilizará en el ejercicio de sus funciones.

8.3.11.2. El personal externo, aliados estratégicos, contratistas y usuarios de terceras partes deben contar con un acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa**, así como del uso aceptable de los activos de información que utilizará en el ejercicio de sus funciones durante la prestación del servicio.

8.3.11.3. Los derechos y obligaciones del personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes en materia de Seguridad de la Información deben estar incluidos en contrato laboral, el contrato colectivo de trabajo y/o contrato de prestación de servicios en los instrumentos jurídicos con terceras partes, incluyendo los relacionados a la protección de la propiedad intelectual, protección de datos personales y prevención del fraude.

8.3.11.4. Se debe formalizar la notificación al personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes sobre las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de toda la normativa interna y prácticas que de ella surjan.

8.3.11.5. El Personal Directivo en el ejercicio de sus funciones debe exhortar al personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes la adopción de la Política de Seguridad de la Información y concientizar sobre las actividades de control y monitoreo que son llevadas a cabo para corroborar el adecuado uso de la información y sus activos.

8.3.12. SOP-EDM-01-P02-03 Entrenamiento y conciencia en materia de seguridad de la información

8.3.12.1. El personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes deben recibir concienciación

en materia de la Seguridad de la Información, por lo menos una vez al año, de manera que sean conscientes de los riesgos a los que está expuesto **Tecnologías Eficientes de Villa.**y cómo pueden apoyar a la protección de la información que manejan.

8.3.12.2. El curso de inducción al nuevo personal debe incluir los tópicos generales en materia de Seguridad de la Información.

8.3.12.3. El personal Directivo debe facilitar los elementos necesarios para que se pueda efectuar la capacitación y concienciación de Seguridad de la Información al personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes.

8.3.13. SOP-EDM-01-P02-04 Proceso sancionatorio

8.3.13.1. En el caso de incumplimientos a las Políticas de Seguridad de la Información o infracciones a las mismas, se deben llevar a cabo las acciones necesarias a fin de determinar la responsabilidad y en su caso la posible sanción que corresponda, misma que se documentará mediante un acta administrativa al colaborador (infractor).

8.3.13.2. En lo referente a las denuncias, la Consejería Jurídica debe encargarse de la investigación y seguimiento de las mismas, con la finalidad de obtener o concluir si existe infracción o no.

8.3.13.3. En cuanto a las quejas en materia de Seguridad de la Información, se debe vigilar su atención oportuna por parte de las áreas responsables de la misma, así como emitir recomendaciones y proponer acciones de mejora.

8.3.14. SOP-EDM-01-P02-05 Cambio de funciones y término de la relación laboral

8.3.14.1. En caso de cambio de funciones, término de la relación laboral, contrato o acuerdo, se debe corroborar con el responsable del activo y su jefe inmediato o contacto para la devolución de los activos de información de **Tecnologías Eficientes de Villa** en su posesión y se cancelen los accesos lógicos asignados, previo a finiquitar la relación o vinculo jurídico.

8.3.14.2. Se debe notificar a la Dirección de Operaciones , el término de la relación laboral o contractual de manera inmediata para eliminar y/o modificar los accesos lógicos asignados con el objeto de reducir el riesgo de robo, o mal uso de la información y sus activos.

8.3.14.3. En el caso del cambio de funciones se deben actualizar los términos y condiciones del empleo de acuerdo con el nuevo perfil de puesto asignado.

8.3.14.4. En el caso de término de la relación laboral o contractual se debe informar al personal de **Tecnologías Eficientes de Villa**, personal externo, contratistas o usuarios de terceras partes sobre las responsabilidades y obligaciones contraídas en el acuerdo de confidencialidad y no divulgación de información, así como en el uso aceptable de los activos de información.

8.3.14.5. En caso de cambio de funciones o término de la relación laboral se deben revocar los poderes vigentes del personal, en caso de contar con ellos.

9. SOP-EDM-01-P03 Gestión de Activos

9.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas que los activos de información cuenten con medidas de protección de acuerdo con su sensibilidad y criticidad, así como definir el nivel de protección y medidas de tratamiento acordes a su sensibilidad.

9.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes de Villa.**en el ejercicio de sus funciones y al personal externo, aliados estratégicos, contratistas y usuarios de terceras partes vinculados a través de instrumentos jurídicos.

9.3. Responsabilidades

9.3.1. Las partes interesadas internas son responsables de implementar la Política de Gestión de Activos dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

9.3.2. Las partes interesadas del SGI de **Tecnologías Eficientes de Villa** son responsables de dar cumplimiento a la Política de Gestión de Activos dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

9.3.3. El Director de Operaciones, de **Tecnologías Eficientes de Villa.**es responsable de designar al responsable del activo y corroborar que los activos sean identificados y gestionados de acuerdo con la Política de Gestión de Activos.

9.3.4. El Área de Operaciones y el responsable del activo es responsable de corroborar que los activos sean devueltos en caso de cambio de funciones o término de la relación laboral del personal de **Tecnologías Eficientes de Villa**, o del término del instrumento jurídico del personal externo, aliados estratégicos, contratistas y usuarios de terceras partes.

9.3.5. El Cesionario de los Activos es responsable de resguardar los activos que le fueron delegados de acuerdo con los requerimientos de seguridad de estos.

9.3.6. El Gerente de Recursos Humanos es responsable de:

- Informar al personal de **Tecnologías Eficientes de Villa.**y al personal externo, al momento de su contratación, del inventario, propiedad, uso aceptable, devolución, sensibilidad, etiquetado, manejo de medios, eliminación y transporte de los activos de información.
- Corroborar la devolución de los activos físicos y electrónicos Institucionales.

9.3.7. El Líder de Infraestructura es responsable de definir e implementar los mecanismos de borrado seguro.

9.3.8. La Consejería Jurídica es responsable de establecer un esquema de clasificación de la información.

9.3.9. El Área de Operaciones y el responsable del activo son responsables de establecer un esquema que determine la sensibilidad de los activos de información.

9.3.10. Las partes interesadas del SGI de **Tecnologías Eficientes de Villa**, son responsables del manejo de cualquier recurso que utilice información bajo su responsabilidad, como correo electrónico, aplicativos Institucionales, estaciones de trabajo, dispositivos móviles, herramientas y equipamiento de publicación de contenidos, etcétera.

9.3.11. El Oficial de Seguridad de la Información y el auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de esta de manera correcta.

9.3.12. El Director de Operaciones , es responsable de hacer del conocimiento al personal

externo, aliados estratégicos, contratistas y usuarios de terceras partes la Política de Gestión de Activos y exhortarlos a su cumplimiento.

9.3.13. SOP-EDM-01-P03-01 Inventario de activos

9.3.13.1. Se deben identificar los activos de información de **Tecnologías Eficientes de Villa**, entre los cuales se incluirán: aplicativos o aplicaciones, componentes, bases de datos, esquemas de bases de datos, software de infraestructura, licencias, servidores físicos, servidores virtuales, clústeres, dispositivos de red, almacenamientos, computadoras de escritorio, laptops, monitores e impresoras.

9.3.13.2. Los activos identificados deben estar documentados en un Inventario de Activos. Este inventario debe contener el nombre del activo, su impacto y sensibilidad, así como su localización física cuando aplique, y debe ser actualizado por lo menos una vez al año o ante una modificación de la información registrada.

9.3.14. SOP-EDM-01-P03-02 Propiedad de activos

9.3.14.1. Los activos de información son propiedad de **Tecnologías Eficientes de Villa** y/o partes interesadas del SGI**.**

9.3.14.2. Los activos de información deben tener designado un responsable que sea personal de **Tecnologías Eficientes de Villa**, el cual fungirá como el responsable del Activo; esta responsabilidad debe quedar registrada en el Inventario de Activos.

9.3.14.3. Si es requerido, se debe documentar en el inventario el nombre del Cesionario de los Activos, quien debe vigilar las medidas de tratamiento de los activos de información.

SOP-EDM-01-P03-03 Uso aceptable de los activos

9.3.14.4. Se deben definir e implementar los mecanismos para el uso y resguardo apropiado de los activos de información, alineados a la sensibilidad éstos, los requerimientos normativos, las leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa.**

9.3.14.5. Se deben definir los mecanismos de control y monitoreo para corroborar el adecuado uso de la información y sus activos, incluyendo aquellos gestionados por contratistas vinculados a través de instrumentos jurídicos.

9.3.14.6. El Cesionario de los Activos debe implementar los controles específicos que le fueron delegados por el responsable del activo.

9.3.14.7. Las partes interesadas del SGI que tengan acceso a los activos de información deben seguir los mecanismos definidos para el uso apropiado de los activos de información.

9.3.14.8. En caso de robo o pérdida de los activos de **Tecnologías Eficientes de Villa** se debe notificar de manera inmediata a la Dirección de Operaciones y/o al responsable del activo quien dará seguimiento y solución del incidente.

SOP-EDM-01-P03-04 Devolución de activos

9.3.14.9. El personal de **Tecnologías Eficientes de Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes deben devolver los activos Institucionales en su posesión en caso de cambio de funciones o terminación del empleo, o del instrumento jurídico. Los activos pueden incluir dispositivos móviles y de almacenamiento externo, software, equipamiento, tarjetas de crédito, tarjetas de ingreso, documentos corporativos, entre otros.

9.3.14.10. En caso de uso de un dispositivo personal se deben seguir procesos para corroborar que la información de **Tecnologías Eficientes de Villa** sea devuelta, y sea borrada de manera segura.

SOP-EDM-01-P03-05 Criterios de sensibilidad de activos

9.3.14.11. Se debe establecer un esquema de clasificación de la información que incluya reglas para la clasificación y protección de la información, que es recibida, generada, adquirida, procesada, almacenada o en posesión de partes interesadas del SGI.

9.3.14.12. Se debe establecer un esquema que determine la sensibilidad de los activos de información en términos de su valor, uso y requisitos legales.

9.3.14.13. Se debe determinar la sensibilidad de los activos de información; la sensibilidad de los activos de software y físicos debe ser determinada con base en la información que reciban, generen, transmitan, procesen y almacenen.

9.3.14.14. Se deben revisar periódicamente los activos de información para actualizar los criterios de sensibilidad que les competen, para determinar si ésta sigue manteniendo su sensibilidad.

SOP-EDM-01-P03-06 Etiquetado de la información

9.3.14.15. Se deben revisar periódicamente los activos de información para actualizar los criterios de sensibilidad que les competen, para determinar si ésta sigue manteniendo su sensibilidad

- Copia.
- Salida de **Tecnologías Eficientes de Villa** vía sistema (cuando se trate de información confidencial o sensible).
- Transmisión por correo, correo electrónico.
- Transmisión a través de mecanismos de intercambio de archivos (SFTP, almacenamiento masivo remoto, etcétera).
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

SOP-EDM-01-P03-07 Manejo de activos

9.3.14.16. Para cada uno de los niveles de sensibilidad de los activos de información se deben definir e implementar los mecanismos de control para el manejo seguro de los mismos, incluyendo las actividades de procesamiento, almacenaje, transmisión y destrucción.

SOP-EDM-01-P03-08 Gestión de medios de almacenamiento externo

9.3.14.17. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa.**se llevan a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos. Sin embargo, si algún cliente maneja almacenamiento externo, entonces se deben definir e implementar los mecanismos para salvaguardar la información confidencial y sensible contenida en medios de almacenamiento externo, como cintas, discos, USB, considerando las siguientes acciones:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por **Tecnologías Eficientes de Villa.**
- Requerir aprobación para retirar cualquier medio de **Tecnologías Eficientes de Villa**, y realizar un control de todos los retiros a fin de mantener una bitácora.
- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o contratistas y la criticidad de la información almacenada.
- La información debe protegerse por medio de contraseñas en los archivos o encriptación del medio de almacenamiento.

9.3.14.18. Está prohibido copiar, almacenar o transportar cualquier tipo de información que

sea considerada confidencial o de sensibilidad crítica, así como cualquier material de trabajo, videos, fotografías, audios o información de **Tecnologías Eficientes de Villa** en medios de almacenamiento externo. En caso de ser necesario el copiar o almacenar información confidencial por temas contractuales con las partes interesadas debe contar con aprobación del inmediato superior, director general o SMT.

SOP-EDM-01-P03-09 Eliminación de medios

9.3.14.19. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** se lleva a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos. Sin embargo, si se utilizan almacenamientos externos se deben definir e implementar mecanismos para la destrucción o borrado seguro de los medios de almacenamiento, que contengan información confidencial o sensible de **Tecnologías Eficientes de Villa**, reduciendo el riesgo de fuga de dicha información a personas no autorizadas; dichos mecanismos deben guardar evidencia del proceso realizado.

9.3.14.20. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** se lleva a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos. Sin embargo, si existen almacenamientos externos se deben considerar mecanismos para la destrucción o borrado seguro de:

- Documentos en papel.
- Voces u otras grabaciones.
- Informes de salida.
- Cintas de impresora de un solo uso.
- Cintas magnéticas.
- Discos u otros dispositivos externos.
- Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o contratista).

9.3.14.21. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** lleva a cabo sobre Tecnología de nube, por lo que no se realiza documentación física. Sin embargo, si existen documentación física se debe realizar la destrucción de documentación física sensible mediante pulverizadoras o trituradoras, una vez vencidos los plazos de conservación conforme a las disposiciones jurídicas aplicables.

SOP-EDM-01-P03-10 Transporte de medios físicos

9.3.14.22. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** lleva a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos.

Sin embargo, si se utilizan almacenamientos externos, cuando se requiera del transporte de activos de información sensibles dentro y fuera de las instalaciones de **Tecnologías Eficientes de Villa**, se debe contar con la autorización del responsable del activo.

9.3.14.23. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** se lleva a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos. Sin embargo, si se utilizan almacenamientos externos, cuando se requiera el transporte de medios físicos por servicios de contratistas, el responsable del activo de Información debe determinar el servicio de mensajería requerido de acuerdo con la sensibilidad de los activos; se debe corroborar que dichos servicios de mensajería cuenten con mecanismos de control para:

- El rastreo de la transferencia de información, permitiendo conocer el estatus y la cadena de custodia mientras se encuentra en tránsito.
- Salvaguardar los activos de acuerdo con las especificaciones de los fabricantes o contratistas.

9.3.14.24. Actualmente el área de Operaciones de **Tecnologías Eficientes de Villa** se lleva a cabo sobre Tecnología de nube, por lo que no se realizan almacenamientos externos. Sin embargo, si se utilizan almacenamientos externos, el transporte de medios físicos con información sensible debe incluir mecanismos de control a fin de protegerla contra divulgación o modificación no autorizada; dichos controles deben incluir:

- Uso de recipientes cerrados.
- Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
- Estándares de identificación del mensajero.
- Entrega en mano al destinatario autorizado.
- Evidencia de recepción por parte del destinatario autorizado.
- Registro y monitoreo del proceso de envío (fecha y hora de envío, así como recepción de la información).
- En casos excepcionales, se debe considerar la definición de diferentes rutas de envío.

10.SOP-EDM-01-P04 Control de Accesos

10.1. Objetivo

Establecer los criterios y medidas de control preventivas, de detección y correctivas para gestionar y controlar los accesos a los activos de información y sus recursos.

10.2. Alcance

Aplica en todos los ámbitos de TECNOLOGÍAS EFICIENTES DE VILLA; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de TECNOLOGÍAS EFICIENTES DE VILLA en el ejercicio de sus funciones y al personal externo, aliados estratégicos, contratistas y usuarios de terceras partes vinculados a través de instrumentos jurídicos. Incluye el acceso y procesamiento de información fuera de las instalaciones de TECNOLOGÍAS EFICIENTES DE VILLA.y uso de dispositivos móviles con acceso autorizado, a la información de TECNOLOGÍAS EFICIENTES DE VILLA.

10.3. Responsabilidades

10.3.1. Las partes interesadas internas de **Tecnologías Eficientes de Villa** son responsables de implementar y dar cumplimiento a la Política de Control de Accesos dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

10.3.2. El Área de Operaciones es responsable de:

- Establecer la normativa para gestionar los accesos y privilegios del personal de **Tecnologías Eficientes de Villa** a la infraestructura tecnológica, sistemas y aplicaciones Institucionales.
- Definir e implementar los mecanismos de control de la operación de los aplicativos.
- Evaluar los requerimientos de seguridad de los proyectos o nuevos servicios a ser implementados.

10.3.3. El Director de Operaciones, es responsable de establecer la normativa para la operación de los servicios, así como los mecanismos de control de Autenticación de los Usuarios.

10.3.4. El Oficial de Seguridad de la Información es responsable de establecer la normativa necesaria para la atención de los incidentes de seguridad.

10.3.5. Las partes interesadas del SGI son responsables de mantener la confidencialidad de la información de Autenticación y, de reportar al Oficial de Seguridad de la Información, los eventos y debilidades de seguridad al momento de identificarse.

10.3.6. El Oficial de Seguridad de la Información y el auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la

manera correcta.

10.3.7. El Área de Operaciones es responsable de hacer del conocimiento a las partes interesadas externas del SGSI la Política de Control de Accesos y exhortarlos a su cumplimiento.

10.3.8. SOP-EDM-01-P04-01 Derechos de acceso

10.3.8.1. El Área de Operaciones y el responsable del activo deben establecer y documentar el perfil de acceso (derechos de acceso) para cada uno de los activos de información.

10.3.8.2. La definición de los perfiles de acceso debe incluir los atributos de acceso para los activos y sus restricciones sobre el acceso, procesamiento, modificación o eliminación de los mismos, además, deben estar alineados a:

- Los roles y responsabilidades, así como la segregación de funciones que fueron definidos.
- El tipo de activos a los cuales se va a acceder de acuerdo con su sensibilidad.
- El tipo de acceso que puede proporcionarse (usuario o usuario con derecho de acceso privilegiado).
- Los requerimientos normativos, las leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa**.

10.3.8.3. La revisión de accesos a los aplicativos será llevada a cabo por el SMT por lo menos una vez al año en la que se verificará que el personal se encuentre activo, que el acceso cumpla con el perfil de puesto asignado.

10.3.9. SOP-EDM-01-P04-02 Acceso a redes y servicios en red

10.3.9.1. El acceso remoto a servicios de red de **Tecnologías Eficientes De Villa** se debe realizar por medio de un canal cifrado.

10.3.9.2. Los usuarios que accedan a la red y servicios de red de **Tecnologías Eficientes de Villa** deben autentificarse, restringiendo el uso de dichos servicios, con base en el perfil de acceso establecido.

10.3.9.3. Las redes inalámbricas de **Tecnologías Eficientes De Villa** deben estar segregadas de manera que el personal externo, aliados estratégicos, contratistas y usuarios de terceras partes tengan accesos restringidos.

10.3.9.4. El acceso a servicios de red de **Tecnologías Eficientes de Villa** solo debe realizarse a través de los equipos y medios de comunicación de **Tecnologías Eficientes De Villa**, evitando las conexiones con equipos que no se encuentren autorizados.

10.3.10. SOP-EDM-01-P04-03 Registro y baja de usuarios

10.3.10.1. El responsable del activo debe garantizar el contar con nomenclatura de usuario, por lo que se debe contar con usuarios únicos, evitando la existencia de múltiples identificadores de acceso para una misma persona.

10.3.10.2. El responsable del activo debe asegurarse de las excepciones de identificadores de usuario único deben estar documentadas, justificadas y aprobadas por el responsable del activo al que se esté solicitando el acceso.

10.3.10.3. El Director de Operaciones debe garantizar el bloqueo de usuarios redundantes o que intenten accesos no autorizados.

10.3.10.4. El Oficial de Seguridad de la Información y el Director de Operaciones deben asegurar que los usuarios que se encuentren involucrados en algún incidente que afecte la información y sus activos, o la Seguridad de la Información deben ser bloqueados.

10.3.10.5. El responsable del activo debe establecer un procedimiento para habilitar un usuario bloqueado.

10.3.10.6. El responsable del activo debe garantizar que no se activará usuarios que han causado baja.

10.3.11. SOP-EDM-01-P04-04 Otorgamiento de acceso a usuarios

10.3.11.1. El acceso a la información y a sus activos debe ser solicitado formalmente por el responsable del activo y estar basado en el perfil de acceso definido para cada uno de los activos de información.

10.3.11.2. El responsable del activo debe garantizar el definir el período en que el usuario tendrá acceso a la información y sus activos (indeterminado o temporal a una fecha establecida).

10.3.11.3. El responsable del activo debe garantizar que el perfil de acceso de un usuario

que no se encuentre formalizado o acorde a su perfil debe ser cancelado.

10.3.11.4. Las excepciones de acceso no acordes al perfil definido deben estar debidamente justificadas, documentadas y aprobadas por el responsable del activo al que se solicite el acceso.

10.3.11.5. El Oficial de Seguridad de la Información y el responsable del activo deben garantizar la asignación de un identificador de usuario e información de Autenticación debe ser personal e intransferible.

10.3.11.6. El Oficial de Seguridad de la Información y el responsable del activo deben garantizar que cuando el personal solicite habilitar un usuario bloqueado, se debe verificar la identidad del personal que lo solicita; solo el personal responsable del usuario debe solicitar la habilitación del mismo.

10.3.11.7. El responsable del activo debe garantizar que los usuarios que causaron baja no deben contar con perfiles asignados.

10.3.12. SOP-EDM-01-P04-05 Gestión de perfiles de acceso privilegiado

10.3.12.1. El responsable del activo debe identificar los perfiles de acceso privilegiado, es decir, los perfiles de acceso que cuenten con facultades para la gestión operativa, tecnológica y/o aplicativa sin restricciones.

10.3.12.2. El Área de Operaciones en conjunto con Gerencia de RRHH deben asignar el acceso privilegiado a usuarios según los principios de “necesidad de su uso” y “caso por caso”, los cuales deben ser acordes a sus roles y responsabilidades.

10.3.12.3. Está prohibido el uso de identificadores de usuarios genéricos, asimismo, no se permite el uso de usuarios por defecto proporcionados por un fabricante de software.

10.3.12.4. Está prohibida la asignación de perfiles de acceso privilegiado a usuarios, para desarrollar y ejecutar rutinas relacionadas con los procesos operativos, la generación de información para la toma de decisiones, así como la generada para el reporte a autoridades de cumplimiento regulatorio o legal.

10.3.12.5. Está prohibida la asignación de perfiles de acceso privilegiado a las partes interesadas externas del SGSI.

10.3.13. SOP-EDM-01-P04-06 Gestión de información de Autenticación de usuarios

10.3.13.1. Las partes interesadas del SGSI con acceso a la información y a los activos de **Tecnologías Eficientes de Villa** deben mantener confidencial la información de Autenticación proporcionada para el acceso a los activos de **Tecnologías Eficientes de Villa**, de acuerdo con lo establecido en el acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa**, así como del uso aceptable de los activos de información.

10.3.13.2. La Gerencia de Recursos Humanos y el Coordinador de Soporte Técnico son responsables de otorgar la información para la identificación y Autenticación de los usuarios, esta debe ser entregada a través de medios oficiales, a las partes interesadas del SGI.

10.3.13.3. La información de Autenticación proporcionada por las partes interesadas externas del SGI, posterior a la entrega de un servicio, debe ser cambiada por el Director de Operaciones , manteniendo la confidencialidad de los activos de información que contienen.

10.3.13.4. El dueño del activo debe verificar la identidad del personal cuando se requiera reiniciar la información de Autenticación de algún usuario.

10.3.13.5. La información de identificación inicial o de reinicio debe ser temporal y cambiada por el personal en su primer inicio de sesión, misma que debe cumplir con la Política de composición de información de Autenticación, y no debe ser genérica.

10.3.13.6. El Coordinador de Soporte Técnico debe contar con un registro formal de la entrega de la información de Autenticación al personal de **Tecnologías Eficientes De Villa**, personal externo, aliados estratégicos, contratistas y usuarios de terceras partes.

10.3.13.7. El Dueño del activo debe garantizar que la información de identificación y Autenticación de usuario debe resguardarse de manera segura.

10.3.13.8. La información de Autenticación estática (contraseñas) a los sistemas de información y aplicaciones debe almacenarse como una cadena de digestión (hash), es decir, no debe almacenarse en texto sin protección.

10.3.14. SOP-EDM-01-P04-07 Monitoreo de derechos de acceso asignados

10.3.14.1. El propietario del activo debe monitorear semestralmente los derechos de acceso

asignados a los usuarios de las partes interesadas del SGI sean vigentes y acorde al perfil aprobado, derivado de cambios en funciones, término de la relación laboral.

10.3.14.2. El propietario del activo derivado del resultado del monitoreo a los derechos de acceso, debe eliminar o actualizar el perfil de acceso asignado a los usuarios.

10.3.15. SOP-EDM-01-P04-08 Eliminación o ajuste de derechos de acceso

10.3.15.1. El Gerente de Recursos Humanos debe comunicar al propietario del activo cuando exista un cambio de funciones, término de la relación laboral, contractual o acuerdo. El propietario del activo debe eliminar los accesos lógicos asignados con el objeto de reducir el riesgo de robo, pérdida de la integridad de la información, o mal uso de la información y sus activos.

10.3.15.2. El propietario del activo debe corroborar que los derechos de accesos, en el caso de accesos temporales otorgados fuera del período establecido, sean eliminados.

10.3.16. SOP-EDM-01-P04-09 Uso de información de Autenticación de Usuarios

10.3.16.1. La información para la Autenticación de los usuarios es de uso personal e intransferible; por lo tanto, toda actividad registrada por un usuario es responsabilidad de las partes interesadas del SGSI al que se encuentra asignado.

10.3.16.2. Si existe algún indicio de que la información de Autenticación se encuentra comprometida, ésta debe ser cambiada inmediatamente y se debe reportar como un incidente de seguridad de la información al Coordinador de Soporte Técnico, buscando cuidar la información en uso y custodia de **Tecnologías Eficientes de Villa**.

10.3.16.3. Está prohibido mantener la información de identificación y Autenticación de usuarios en papel, cualquier medio o dispositivo, con el objeto de reducir el riesgo de acceso no autorizado.

10.3.17. SOP-EDM-01-P04-10 Restricción de acceso a la información

10.3.17.1. El Director de Operaciones debe restringir el acceso a la información dentro de los aplicativos Institucionales e infraestructura tecnológica, limitando el acceso de acuerdo con la Política de Derechos y accesos definida.

10.3.18. SOP-EDM-01-P04-11 Inicio de sesión segura

10.3.18.1. El Área de Operaciones debe implementar un registro para autenticar a los usuarios que acceden a información sensible, así como para las aplicaciones de uso de los usuarios.

10.3.18.2. Se deben definir e implementar mecanismos de control para iniciar de manera segura la sesión en los aplicativos Institucionales. El inicio seguro debe incluir:

- Restricción de información del sistema al que se está conectando hasta que el inicio de sesión se haya generado exitosamente.
- La información que se ingresa para el inicio de sesión (identificador de usuario y Autenticación) debe ser verificada hasta completar todos los datos, evitando proporcionar información sobre los datos que son incorrectos.
- La información de Autenticación que se ingresa no puede ser leída en la pantalla del dispositivo por el cual está accediendo.
- Los mensajes de error derivados de un inicio de sesión fallida no deben incluir información que pueda ayudar al acceso de usuarios no autorizados.
- Protección contra intentos de inicio de sesión de manera automática.
- Registros de inicios de sesión exitoso y fallido.
- Generación de incidentes de seguridad en caso de identificar intentos de acceso o accesos no autorizados.
- Resguardo y transmisión por la red de manera de segura de la información de identificación y Autenticación de usuarios.
- Registros de inicio y cierre de sesión que incluya; fechas, horas e identificador de usuario, intentos exitosos y fallidos.

10.3.18.3. El acceso a los aplicativos Institucionales a través de la red debe realizarse mediante uso de redes seguras.

10.3.19. SOP-EDM-01-P04-12 Composición de información de Autenticación

10.3.19.1. La información de Autenticación de los usuarios debe tener una composición robusta con el objeto de otorgar un grado de seguridad elevado para la protección de la información y reducir el riesgo de pérdida de la integridad de la información por acceso no autorizado.

10.3.19.2. Todas las contraseñas deben cumplir con la composición de la información de Autenticación; esto incluye:

- Longitud mínima de 8 caracteres que incluya por lo menos una letra mayúscula, un número y un carácter especial.
- No utilizar contraseñas con información por defecto, que sean comunes o que

contengan números consecutivos.
- Cambio periódico por lo menos cada 90 días naturales.

10.3.19.3. Está prohibido el uso de contraseñas que contengan nombres, apellidos, fechas, teléfonos, nombres de sistemas o cualquier información de fácil identificación, así como palabras asociadas a **Tecnologías Eficientes de Villa**.

10.3.20. SOP-EDM-01-P04-13 Acceso a las utilerías de hardware y software

10.3.20.1. El Coordinador de Soporte Técnico deberá dar acceso a las utilerías o herramientas de administración del hardware y software, el cual se debe otorgar solo al personal de **Tecnologías Eficientes de Villa** que lo necesite para el cumplimiento de sus funciones, manteniendo un registro de su nombre.

10.3.20.2. Está prohibida la asignación de acceso a las utilerías o herramientas de administración del hardware y software a las partes interesadas externas del SGSI.

10.3.21. SOP-EDM-01-P04-14 Control de acceso a los componentes de los sistemas

10.3.21.1. La información de los componentes de los aplicativos tales como, código fuente, librerías, información del diseño y arquitectura, especificaciones técnicas y líneas base de configuraciones debe ser resguardada por el propietario del activo y su acceso debe estar restringido.

10.3.21.2. Cualquier modificación a los componentes de los sistemas debe estar controlada por el responsable de Gestión de Cambios para cumplir con la Política de gestión de cambios.

10.3.21.3. La Dirección de Operaciones debe contar con un inventario de los componentes de los sistemas el cual incluya la información en uso, indicando nombre del componente, versión, fecha de última modificación, responsable de modificación y estatus del componente (en modificación, en producción).

10.3.22. SOP-EDM-01-P04-15 Control de acceso a aplicaciones

10.3.22.1. El Gerente de Recursos Humanos debe establecer el instructivo para el alta y baja de usuarios, reduciendo el acceso de pérdida de la integridad de la información por acceso no autorizado, y de pérdida de la confidencialidad de la información de los usuarios.

10.3.22.2. El Propietario del Activo en coordinación con la Gerencia de Recursos Humanos, de acuerdo con el instructivo de alta y baja de usuarios, debe definir e implementar los mecanismos de control y monitoreo, para salvaguardar la información de las área de Operaciones y servicios, que es transmitida, almacenada y procesada por medios electrónicos.

11. SOP-EDM-01-P05 Cifrado.

11.1. Objetivo

Determinar las medidas de control preventivas, de detección y correctivas para el uso eficaz de herramientas de cifrado y llaves de cifrado autorizadas en la infraestructura tecnológica en donde se almacena o transfiere información sensible, y que esté en uso o custodia de **Tecnologías Eficientes De Villa**, con el fin de proteger su integridad, confidencialidad y/o reserva.

11.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes De Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones y al personal externo, aliados estratégicos, contratistas y usuarios de terceras partes vinculados a través de instrumentos jurídicos.

11.3. Responsabilidades

11.3.1. Las partes interesadas internas del SGI son responsables de implementar y dar cumplimiento a la Política de Cifrado dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad de la Información, cualquier omisión que se conozca sobre el cumplimiento de dicha política.

11.3.2. La Dirección de Operaciones es responsable de definir, implementar y gestionar los mecanismos de control para el cifrado de la información sensible y, para que se almacene y transmita dentro de la infraestructura de **Tecnologías Eficientes De Villa** o se transporte fuera de éste.

11.3.3. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como

monitorear la implementación de los mecanismos de control para el acatamiento de la de manera correcta.

11.3.4. SOP-EDM-01-P05-01 Uso de controles de cifrado

11.3.4.1. La Dirección de Operaciones debe definir e implementar los mecanismos de control de cifrado para el almacenamiento, procesamiento y transferencia de la información sensible de **Tecnologías Eficientes de Villa.**

11.3.4.2. La Dirección de Operaciones debe asegurar que toda la información sensible cifrada que requiera de Autenticación a través de un usuario y contraseña para su acceso se apegue y de cumplimiento a la Política de Control de Accesos.

11.3.4.3. La Dirección de Operaciones debe asegurar que las área de Operaciones financieras que impliquen transferencia de información sensible, y que sean efectuadas en las instalaciones de **Tecnologías Eficientes de Villa**, cuenten con mecanismos de control de cifrado y protocolos seguros.

11.3.4.4. La Dirección de Operaciones debe asegurar que la infraestructura tecnológica que contenga información sensible utilice protocolos que transmitan la información por medio de mensajes cifrados.

11.3.4.5. La Dirección de Operaciones debe asegurar que se cifre la información sensible que se encuentre almacenada en servidores de archivos, aplicaciones y bases de datos.

11.3.4.6. Las excepciones para el cifrado de aplicaciones y bases de datos deben estar debidamente justificadas, documentadas y aprobadas por el propietario del activo; para estos casos se debe contar con controles compensatorios que corroboren la confidencialidad de la información.

11.3.4.7. La Dirección de Operaciones debe asegurar que se cifre la información sensible contenida en los dispositivos de almacenamiento externo que salgan de **Tecnologías Eficientes de Villa**.

11.3.4.8. El responsable de llaves de cifrado será el propietario de cada activo, el cual gestiona las llaves de las partes interesadas del SGI.

11.3.5. SOP-EDM-01-P05-02 Gestión de Llaves

11.3.5.1. Cada dueño del activo es responsable de almacenar las llaves de cifrado para su gestión, evitando en todo momento exponerlas a un incidente de seguridad de la información.

11.3.5.2. El propietario del activo debe definir e implementar los mecanismos de control para el resguardo de las llaves de cifrado de manera que permanezcan seguras y evitando que se haga mal uso de estas.

11.3.5.3. El propietario del activo debe definir y formalizar los tiempos de verificación de llaves de cifrado administradas y establecer los tiempos de renovación y caducidad de las mismas.

12.SOP-EDM-01-P06 Seguridad Física y del Entorno.

12.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para el acceso físico para prevenir accesos no autorizados, daños o interferencias a los activos tecnológicos o de información e instalaciones que no realizan de procesamiento de información de **Tecnologías Eficientes de Villa**.

12.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa;** sus recursos, información, sus procesos internos, así como a las partes interesadas internas y externas del SGI.

12.3. Responsabilidades

12.3.1. El personal de **Tecnologías Eficientes De Villa** es responsable de implementar y dar cumplimiento a la Política de Seguridad Física y del Entorno dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

12.3.2. El Gerente de Recursos Humanos es responsable de identificar y delimitar los perímetros de seguridad.

12.3.3. El Gerente de Recursos Humanos es responsable de:

- Impartir la inducción institucional y del sistema de gestión al personal de **Tecnologías Eficientes De Villa** de nuevo ingreso.
- Gestionar los accesos físicos a las instalaciones de **Tecnologías Eficientes De Villa**.

- Establecer los objetos no permitidos.
- Establecer un proceso formal de alta, baja o modificación de privilegios de usuarios.
- Establecer el esquema de Protección Civil.
- Definir, implementar, capacitar y coordinar las brigadas de emergencia.
- Identificar y comunicar riesgos internos y externos de seguridad física.
- Determinar la ubicación de las zonas de riesgo y señales de protección civil en las instalaciones de **Tecnologías Eficientes de Villa**.
- Gestionar el directorio de brigadistas y números de emergencia.
- Establecer rondas de seguridad de manera programada.

12.3.4. El Director de Operaciones es responsable de:

- Establecer los mecanismos de control de las estaciones de trabajo.
- Gestionar el mantenimiento a la infraestructura tecnológica de **Tecnologías Eficientes de Villa.**
- Establecer los mecanismos de control para el cableado de comunicaciones y la protección de los equipos de cómputo.

12.3.5. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

12.3.6. El Área de Operaciones es responsable de hacer del conocimiento a las partes interesadas externas del SGI la Política de Seguridad Física y del Entorno y exhortarlos a su cumplimiento.

12.3.7. Las partes interesadas externas del SGI son responsables de implementar y dar cumplimiento a la Política de Seguridad Física y del Entorno dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

12.3.8. SOP-EDM-01-P06-02 Mecanismos de control para el acceso a edificios.

12.3.8.1. El Gerente de Recursos de Humanos en coordinación con la Dirección de Operaciones debe asegurar que se cuenta con un Sistema Integral de Administración de Seguridad y Vigilancia que permita monitorear los accesos físicos a las instalaciones, salvaguardando el patrimonio de las actividades administrativas y operativas de **Tecnologías Eficientes de Villa.**

12.3.8.2. El personal de **Tecnologías Eficientes de Villa** que requiera tener acceso a las

instalaciones de **Tecnologías Eficientes de Villa** registrarse en la bitácora, presentando una identificación oficial en una bitácora física que debe contener por lo menos la siguiente información:

- Nombre del personal
- Área o empresa.
- Motivo de visita.
- Fecha.
- Hora de entrada.
- Hora de salida.
- Firma

12.3.8.3. Los visitantes, deben presentar en el módulo de recepción una identificación oficial vigente, la cual deben intercambiar por un gafete de visitante que deben portar en un lugar visible en todo momento mientras estén en las instalaciones de **Tecnologías Eficientes de Villa.** Asimismo, deben registrarse en una bitácora física que contenga por lo menos la siguiente información:

- Nombre del visitante
- Área o empresa.
- Motivo de visita.
- Fecha.
- Hora de entrada.
- Hora de salida.
- Firma

12.3.8.4. El personal del módulo de recepción debe corroborar la correspondencia de la fotografía de la identificación oficial con el personal externo, contratistas, usuarios de terceras partes o visitantes.

12.3.8.5. El visitante debe esperar a que el personal del módulo de recepción se comunique con el personal de **Tecnologías Eficientes De Villa** a quien visita y a que éste autorice su ingreso.

12.3.8.6. En caso de que el personal externo, contratistas, usuarios de terceras partes o visitantes porten bolsas, mochilas, portafolios o paquetes, éstos deben ser revisados por el personal de **Tecnologías Eficientes de Villa** responsable de la recepción a la entrada y a la salida de **Tecnologías Eficientes de Villa**, a fin de detectar objetos no permitidos.

12.3.8.7. Los registros de las visitas deben resguardarse durante 365 días contemplando

mecanismos para evitar su alteración, así como manteniendo mecanismos de control para su acceso y disponibilidad.

12.3.9. SOP-EDM-01-P06-03 Mecanismos de control para áreas comunes

12.3.9.1. Las áreas comunes dentro de las instalaciones de **Tecnologías Eficientes De Villa** deben ser monitoreadas, implementando rondas de seguridad por parte del personal de vigilancia y sistemas de video vigilancia con el fin de detectar actividades no permitidas.

12.3.9.2. Las grabaciones de vigilancia a las áreas comunes deben resguardarse durante 10 días para evitar su alteración.

12.3.10. SOP-EDM-01-P06-04 Mecanismos de seguridad para oficinas y estaciones de trabajo.

12.3.10.1. Las estaciones de trabajo del personal de **Tecnologías Eficientes de Villa** deben ser monitoreadas, implementando rondas de seguridad por parte del personal de vigilancia y sistemas de video vigilancia con el fin de detectar actividades no permitidas.

12.3.10.2. Las grabaciones de vigilancia en sala de juntas deben resguardarse durante 10 días para evitar su alteración.

12.3.10.3. Las oficinas del personal de **Tecnologías Eficientes de Villa** deben permanecer cerradas cuando se encuentren desatendidas y al término de la jornada laboral; en caso de que se requiera acceso en horario no laborable, se deberá solicitar autorización a la Dirección de Administración y finanzas, justificando el motivo.

12.3.11. SOP-EDM-01-P06-05 Protección contra amenazas externas y del ambiente

12.3.11.1. Gerente de Recursos Humanos debe establecer un esquema de Protección Civil, el cual tenga por objetivo prevenir, auxiliar y coordinar la recuperación de las instalaciones de **Tecnologías Eficientes de Villa** ante la eventualidad de fenómenos, siniestros, desastres o emergencias.

12.3.11.2. El Gerente de Recursos Humanos debe realizar un análisis de riesgos físicos con el fin de identificar los riesgos internos y externos de **Tecnologías Eficientes de Villa** que pudieran producir algún incidente que implique la interrupción de la operación.

12.3.11.3. El Gerente de Recursos Humanos debe proveer un programa interno de protección civil basado en el análisis de riesgos físicos y cumpliendo con las leyes y

regulaciones de protección civil que le apliquen a **Tecnologías Eficientes de Villa**, el cual debe contener los protocolos de cómo reaccionar antes, durante y después de algún fenómeno, siniestro, desastre o emergencia.

12.3.11.4. El Gerente de Recursos Humanos debe definir las brigadas de emergencia, así como llevar a cabo la integración, formación, capacitación y entrenamiento al personal de **Tecnologías Eficientes de Villa** y al equipo de brigadistas que de manera voluntaria se integren a la Unidad Interna de Protección Civil.

12.3.11.5. El Gerente de Recursos Humanos debe equipar los inmuebles con señalización, además de establecer las áreas de menor riesgo dentro del inmueble y puntos de reunión fuera de éste, así como las rutas de evacuación.

12.3.11.6. El Gerente de Recursos Humanos debe publicar y mantener actualizado el directorio de brigadistas y de números de emergencias en cumplimiento con la Política de Contacto con Autoridades.

12.3.12. SOP-EDM-01-P06-06 Instalación y protección de equipo

12.3.12.1. El Coordinador de Soporte Técnico debe asegurarse que las instalaciones que no realizan procesamiento de información y que cuentan con un cuarto de comunicaciones (MDF/IDF) en donde existen activos físicos.

12.3.12.1.1. Analicen la capacidad de las instalaciones, aire acondicionado, red eléctrica y unidades de energía ininterrumpida para las instalaciones de los cuartos de comunicaciones de manera que se puedan determinar las acciones necesarias para prevenir incidentes por capacidad.

12.3.12.1.2. Se cuente con sistemas de tierra física de comunicación y de alimentación eléctrica que minimicen el riesgo de descargas eléctricas.

12.3.13. SOP-EDM-01-P06-07 Servicios de soporte remoto

12.3.13.1. La Dirección de Operaciones debe asegurarse que las instalaciones de procesamiento de información que soporten aplicaciones criticas deberán estar implementadas con proveedores de nube que estén certificados en ISO 27001:2022.

12.3.14. SOP-EDM-01-P06-08 Seguridad en el cableado

12.3.14.1. El Coordinador de Soporte Técnico debe asegurarse que la red de comunicaciones esté diseñada bajo normas de cableado estructurado.

12.3.14.2. El Coordinador de Soporte Técnico debe asegurarse que las redes de comunicaciones y de energía eléctrica estén separadas a efecto de prevenir interferencias.

12.3.14.3. El Coordinador de Soporte Técnico debe asegurarse que las instalaciones de control de energía eléctrica sean identificadas y protegidas físicamente a fin de que solo personal calificado de **Tecnologías Eficientes de Villa** o contratistas autorizados puedan efectuar cambios.

12.3.15. SOP-EDM-01-P06-09 Mantenimiento de equipos

12.3.15.1. El Líder de Soporte Técnico debe asegurarse que se cuente con un programa de mantenimiento preventivo periódico, y de acuerdo con las especificaciones de la infraestructura tecnológica de **Tecnologías Eficientes de Villa**.

12.3.15.2. El Líder de Soporte Técnico debe asegurarse que los servicios de mantenimiento sean realizados por personal autorizado y competente para tales efectos. Una vez realizados los mantenimientos, se deben hacer pruebas comprobando la funcionalidad de los equipos.

12.3.15.3. El Líder de Soporte Técnico debe asegurarse que se cuente un registro de los mantenimientos realizados a la infraestructura tecnológica de **Tecnologías Eficientes de Villa**. Estos registros se deben conservar por lo menos un año.

12.3.15.4. El Coordinador de Soporte Técnico debe dar mantenimiento preventivo al equipamiento de **Tecnologías Eficientes de Villa**, tal como, unidades de energía ininterrumpida (UPS) y aires acondicionados, incluyendo los que se encuentran en las instalaciones de procesamiento de la información, de manera periódica y programada.

12.3.16. SOP-EDM-01-P06-10 Retiro de activos

12.3.16.1. El personal del módulo de recepción debe asegurarse que los activos físicos que deban entrar o salir de las instalaciones de **Tecnologías Eficientes de Villa**, sean registrados tanto a la entrada como a la salida en una bitácora que debe contener por lo menos:

- Fecha y hora de la entrada y/o salida.
- Detalles del activo (tipo de activo, marca, modelo y número de serie).
- Nombre del responsable del activo.
- Personal de **Tecnologías Eficientes de Villa** que aprueba la salida.
- Nombre de la persona que realiza la entrada/salida del activo.
- El motivo de la salida.

12.3.16.2. El personal del módulo de recepción debe asegurarse que los equipos de cómputo propiedad del personal de **Tecnologías Eficientes de Villa**, de visitas, de personal externo o usuarios de terceras partes sean registrados tanto a la entrada

como a la salida en una bitácora que, para tal efecto, se encontrará en el módulo de recepción de cada inmueble. El registro debe contener por lo menos:

- Nombre del propietario.
- Fecha.
- Hora de entrada.
- Hora de salida.
- Detalles del activo (tipo de activo, marca, modelo y número de serie).

12.3.16.3. Los registros de las entradas y salidas de equipos de cómputo deben resguardarse con los mecanismos de control adecuados para evitar alteraciones durante 365 días.

12.3.16.4. Para la salida de activos físicos se debe contar con una carta responsiva que debe ser firmada por el responsable de soporte, el usuario y la Dirección de Operaciones.

12.3.17. SOP-EDM-01-P06-11 Seguridad del equipo y activos fuera de las instalaciones

12.3.17.1. El Coordinador de Soporte Técnico debe establecer y verificar el cumplimiento de los mecanismos de seguridad para los equipos de **Tecnologías Eficientes de Villa** que estarán fuera de las instalaciones, tomando en cuenta:

- Cifrado del activo al que se dará salida cuando incluya información sensible.
- Conciencia de seguridad al usuario para el resguardo del equipo.

12.3.17.2. En caso de robo o daños al equipo, las partes interesadas internas y externas del SGSI deben avisar de manera inmediata, de acuerdo con los instructivos establecidos para la atención de incidentes de seguridad, en cumplimiento con la Política de Incidentes de Seguridad.

12.3.18. SOP-EDM-01-P06-12 Eliminación segura o reutilización del equipo

12.3.18.1. El Coordinador de Soporte Técnico debe definir e implementar mecanismos de control para el borrado seguro de equipamiento informático, medios magnéticos y de almacenamiento externo que se requiera reasignar o reutilizar.

12.3.19. SOP-EDM-01-P06-13 Equipo de usuario desatendido

12.3.19.1. El personal de **Tecnologías Eficientes de Villa**, personal externo y usuarios de terceras partes, una vez que se retiren de su estación de trabajo, debe mantener bloqueados y/o apagados los equipos de cómputo o dispositivos móviles, evitando accesos no autorizados.

12.3.19.2. El Dueño del Activo debe asegurarse que la información que no sea de uso público se resguarde en un lugar seguro mientras no sea utilizada, especialmente cuando la estación de trabajo se encuentre desatendida, y esta debe ser acorde al tratamiento

que le corresponda de acuerdo con su sensibilidad.

12.3.20. SOP-EDM-01-P06-14 Escritorio limpio y pantalla limpia

12.3.20.1. El Gerente de Recursos Humanos en coordinación con el Líder de Soporte Técnico debe concientizar al personal de **Tecnologías Eficientes de Villa**, personal externo y usuarios de terceras partes respecto a mantener las estaciones de trabajo limpias, evitando tener alimentos y bebidas cerca de información impresa o de los equipos de cómputo, dispositivos móviles, infraestructura tecnológica o medios de almacenamiento que contengan información de **Tecnologías Eficientes de Villa**.

12.3.20.2. El personal de **Tecnologías Eficientes de Villa** debe asegurarse que las estaciones de trabajo se mantengan despejadas con el objetivo de no exponer información impresa o digital sensible, a fin de evitar la divulgación no autorizada, daño o robo de la misma, así como resguardar los medios electrónicos de almacenamiento, ya sea en gabinetes o archiveros cuando no se encuentran en uso y especialmente al término de la jornada laboral.

12.3.20.3. El personal de **Tecnologías Eficientes de Villa** no debe contar con accesos directos en el escritorio lógico de sus equipos de ningún tipo, previniendo el acceso no autorizado.

13.SOP-EDM-01-P07 Seguridad en las Área de Operaciones

13.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para la operación correcta y continua de los procesos y servicios de **Tecnologías Eficientes de Villa**.

13.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos, así como a las partes interesadas internas y externas del SGSI.

13.3. Responsabilidades

13.3.1. El personal de **Tecnologías Eficientes de Villa**.es responsable de implementar y dar

cumplimiento a la Política de Seguridad en las Área de Operaciones dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones.

13.3.2. El Director de Operaciones es responsable de establecer la normativa operativa bajo su responsabilidad, incluyendo la gestión de la infraestructura tecnológica y software.

13.3.3. El Gerente de Recursos Humanos es responsable de apoyar a las áreas interesadas en implementar mecanismos de difusión sobre temas específicos de seguridad que le sean solicitados.

13.3.4. El propietario de los activos de información es responsable de definir la periodicidad y el tiempo de retención de los respaldos de información de **Tecnologías Eficientes de Villa**, considerando que dicho periodo no podrá ser menor a cinco (5) años, conforme a la sensibilidad de la información.

13.3.5. El Oficial de Seguridad de la Información y el Auditor Interno son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

13.3.6. El Director de Operaciones y el Gerente de compras son responsables de hacer del conocimiento a las partes interesadas externas del SGI la Política de Seguridad en las Área de Operaciones y exhortarlos a su cumplimiento.

13.3.7. Las partes interesadas internas del SGI son responsables de dar cumplimiento a la Política de Seguridad en las Áreas de Operaciones dentro de sus ámbitos de responsabilidad y de abstenerse de incumplirla.

13.3.8. SOP-EDM-01-P07-01 Procesos operativos documentados

13.3.8.1. Se debe establecer una base de conocimientos que contenga los procesos operativos, incluyendo los que son administrados por partes interesadas externas del SGI, como:

- Solución de Incidentes/Problemas.
- Procedimientos operativos.

13.3.8.2. La base de conocimientos debe estar disponible para las partes interesadas internas del SGI que puedan necesitarlos dentro de su área de responsabilidad.

13.3.9. SOP-EDM-01-P07-02 Gestión de cambios

13.3.9.1. De acuerdo a su tipificación los aplicativos deben realizar sus funciones basándose en el Plan de Desarrollo y deben contar con el registro adecuado de sus cambios.

13.3.9.2. Se debe establecer un procedimiento para el control de cambios en los procesos, y en los sistemas, aplicaciones e infraestructura tecnológica donde se procesa la información, evitando que se pudiera afectar la seguridad de la misma.

13.3.9.3. El procedimiento de administración de cambios debe establecer todos los detalles para:

- Definición de tipo de cambio.
- Identificación, registro, planificación y pruebas del cambio, de acuerdo con el tipo de cambio.
- Evaluación de impactos potenciales.
- El proceso de autorizaciones y aprobaciones por parte de los involucrados en el cambio.
- La liberación en producción.

13.3.10. SOP-EDM-01-P07-03 Gestión de la capacidad

13.3.10.1. Se deben proveer los mecanismos para el monitoreo de la capacidad de la infraestructura tecnológica que soporten los procesos de **Tecnologías Eficientes De Villa**, determinando las líneas base de capacidad y sus umbrales, de tal forma que se tomen las acciones necesarias para evitar incidentes de servicio, mejorando con esto la disponibilidad y eficiencia de los servicios de **Tecnologías Eficientes de Villa**.

13.3.10.2. Se debe establecer un plan de capacidad, considerando las tendencias y proyecciones en el consumo de la capacidad.

13.3.11. SOP-EDM-01-P07-04 Separación de los ambientes de desarrollo, pruebas y producción

13.3.11.1. Los Líderes de Infraestructura y Desarrollo deben gestionar los accesos a los ambientes de desarrollo, pruebas y producción, de tal manera que no exista conflicto de intereses y se mantenga una correcta segregación de tareas e implementación de cambios.

13.3.11.2. Los Líderes de Infraestructura y Desarrollo deben verificar que los ambientes de

desarrollo, pruebas y producción no compartan un mismo espacio lógico entre sí, es decir, que la información que se almacene y procese se encuentre en espacios separados lógica o físicamente.

13.3.11.3. **SOP-EDM-01-P07-05 Desarrollo por terceros**

13.3.11.3.1 El desarrollo de software por terceros deberá ser supervisado y controlado por el Director de Operaciones y el Líder de Desarrollo.

13.3.11.3.2 Los contenidos desarrollados por terceros para **Tecnologías Eficientes de Villa**, serán propiedad de la empresa (código y los derechos de propiedad intelectual).

13.3.11.3.3 Dirección de área de Operaciones comunicará a los terceros los requisitos contractuales para las prácticas de diseño y desarrollo seguro, codificación y pruebas.

13.3.11.3.4 La Dirección de Operaciones y el Área de Operaciones deberán recibir y revisar la presentación de evidencias de que se han realizado suficientes pruebas para proteger los entregables contra la presencia de contenido malicioso, tanto intencionado como no intencionado.

13.3.11.3.5 El Director de Operaciones tiene la facultad de auditar todo proceso desarrollado por terceros.

13.3.11.3.6 Todo desarrollo por terceros generará un entregable (ajustándose a los lineamientos de la empresa) a Dirección de Operaciones en donde se documente el entorno de desarrollo.

13.3.11.3.7 La Consejería Jurídica deberá revisar que los Desarrollos realizados por terceros cumplan con requisitos legales de la empresa.

13.3.12. SOP-EDM-01-P07-06 Controles contra software malicioso

13.3.12.1. El Área de Operaciones y el Líder de Infraestructura deben implementar y gestionar los mecanismos necesarios para la detección, prevención, recuperación y eliminación de software malicioso en la infraestructura tecnológica y en las estaciones de trabajo del personal de **Tecnologías Eficientes de Villa**.

13.3.12.2. El Área de Operaciones y el Líder de Infraestructura deberán enviar semestralmente correos electrónicos como parte de concienciación de seguridad al personal de **Tecnologías Eficientes de Villa**, donde se incluyan temas sobre la descarga y uso de software no autorizado, consulta de páginas de internet no permitidas o sospechosas, así como el uso de dispositivos móviles y de

almacenamiento que pudieran contener software malicioso. La información proporcionada al personal de **Tecnologías Eficientes de Villa** debe sensibilizarlos sobre el impacto que pudiera ocasionar a **Tecnologías Eficientes de Villa**.

13.3.12.3. La infección y propagación de software malicioso en la infraestructura tecnológica de **Tecnologías Eficientes de Villa** debe ser tratada como un incidente de seguridad de la información y debe ser comunicado por el Líder de Soporte Técnico al Oficial de seguridad de la información.

13.3.13. SOP-EDM-01-P07-07 Respaldo de información

13.3.13.1. El Director de Operaciones y el Líder de Infraestructura deberán minimizar el riesgo de interrupción de la operación con base en mecanismos de respaldo y procesos de recuperación de la información, así como de la infraestructura tecnológica para su procesamiento.

13.3.13.2. El Director de Operaciones y el Líder de Infraestructura deben evitar la pérdida de datos realizando respaldos de la información de manera periódica, así como del software y los sistemas que la soportan. Si se trata de un servicio crítico se debe considerar respaldar la información, los sistemas y el software necesarios para recuperar el servicio completo en caso de desastre.

13.3.13.3. Los respaldos deben ser exactos y deben estar completos de acuerdo con lo definido por el propietario del activo de información, y deben ser con base en los mecanismos de control definidos en la política correspondiente.

13.3.13.4. El Director de Operaciones y el Líder de Infraestructura deben realizar los respaldos y ser probados trimestralmente, con el fin de identificar y corregir cualquier falla.

13.3.13.5. Debido a que los sistemas de **Tecnologías Eficientes de Villa** se encuentran en la nube, el proveedor de nube se encarga de la gestión de los medios de almacenamiento para hacer respaldos, por lo que se debe contar con una evidencia de que esto se realiza.

13.3.13.6. La periodicidad de los respaldos y el tiempo de retención de la información respaldada se deben determinar tomando en cuenta los requisitos del propietario del activo de información y la criticidad de la información.

13.3.13.7. Los respaldos no deben almacenarse en el mismo contenedor que la información que ha sido respaldada.

13.3.14. SOP-EDM-01-P07-08 Bitácora de eventos

13.3.14.1. El Director de Operaciones y el Líder de Infraestructura deben generar y mantener regularmente los registros de las actividades de los usuarios y administradores en la infraestructura tecnológica de **Tecnologías Eficientes de Villa,** así como de sus excepciones, fallas y eventos de seguridad. Estos registros deben contener información que incluya los identificadores de los usuarios y sus actividades en el sistema como:

- Fechas y horas de eventos clave como inicio y cierres de sesión, accesos fallidos y exitosos al sistema.
- Direcciones de red.

13.3.14.2. Los registros de los eventos deben ser analizados por el Director de Operaciones y el Líder de Infraestructura de manera periódica con el fin de identificar y reportar posibles incidentes de seguridad por los medios establecidos para este fin en cumplimiento con la Política de Incidentes de Seguridad de la Información.

13.3.15. SOP-EDM-01-P07-09 Protección de la información en bitácoras

13.3.15.1. El propietario del activo se encargará de realizar los registros de eventos y actividades de los usuarios deben ser resguardados y su acceso debe estar restringido, con el fin de que estén libres de modificaciones o eliminaciones.

13.3.15.2. El propietario del activo debe establecer el tiempo de retención de los registros de los eventos considerando la criticidad de la información y las leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa**.

13.3.16. SOP-EDM-01-P07-10 Sincronización de relojes

13.3.16.1. La infraestructura tecnológica debe contar con los protocolos necesarios para la sincronización de relojes, utilizando como referencia una única fuente confiable, con el fin de que los procesos en los sistemas se ejecuten en forma cronológica, respetando el orden de los eventos y verificando la exactitud de los registros.

13.3.17. SOP-EDM-01-P07-11 Instalación de software en sistemas operacionales

13.3.17.1. La instalación y la aplicación de cambios en el software de los sistemas

operacionales deben estar controladas y en cumplimiento con la Política de Gestión de Cambios, realizando un análisis de impacto hacia los procesos sustantivos de **Tecnologías Eficientes de Villa**.

13.3.17.2. La instalación y la aplicación de cambios en el software de los sistemas operacionales debe documentarse por el Área de Operaciones, el flujo de trabajo debe ser probado; la liberación a producción se debe realizar una vez que las pruebas aplicadas en su totalidad sean exitosas.

13.3.17.3. En el flujo de trabajo de la instalación de software en sistemas operacionales el Líder de Infraestructura debe incluir la realización de respaldos, siempre que sea un cambio de versión de la aplicación, en cumplimiento con la Política de Respaldos de Información y definir los pasos a seguir para realizar el retorno cuando la liberación a producción no sea exitosa o la versión estable anterior, y siempre se deben mantener las versiones anteriores del software como medida de contingencia.

13.3.18. SOP-EDM-01-P07-12 Gestión de vulnerabilidades técnicas

13.3.18.1. Cuando se desarrollan aplicativos institucionales el Área de área de área de Operaciones debe contemplar la realización de pruebas tendientes a detectar vulnerabilidades de los medios electrónicos, de telecomunicaciones y equipos automatizados, que prevengan el acceso y uso no autorizado.

13.3.18.2. El Director de Operaciones y el Oficial de Seguridad deben realizar una revisión por lo menos una vez al año, del análisis hecho para detectar las vulnerabilidades, a la infraestructura de los ambientes de nube, de tal forma que se revise el total de la infraestructura tecnológica crítica de **Tecnologías Eficientes de Villa** con el fin de identificar posibles debilidades y brechas de seguridad, tomando en cuenta los resultados de análisis previos. Los reportes de resultados de estos análisis deben contener las recomendaciones para el tratamiento de todos los hallazgos.

13.3.18.3. El Director de Operaciones y el Oficial de Seguridad deben identificar y asignar un responsable para cada hallazgo identificado en el análisis de vulnerabilidades, de tal forma que se dé seguimiento hasta que sea resuelto.

13.3.18.4. La aplicación de las recomendaciones debe ser analizada por el Área de Operaciones y el Oficial de Seguridad determinando la factibilidad de su aplicación, tomando en cuenta el costo beneficio y su impacto hacia **Tecnologías Eficientes de Villa**; se deben justificar y documentar las recomendaciones.

13.3.19. SOP-EDM-01-P07-13 Restricción en la instalación de software

13.3.19.1. El dueño del activo de los equipos de cómputo Institucionales y/o personales no deberán instalar software que se encuentren el catálogo de software no permitido en los equipos por parte del Líder de Soporte Técnico.

13.3.20. SOP-EDM-01-P07-14 Consideraciones para la revisión de mecanismos de control

13.3.20.1. El Área de Operaciones y el Coordinador de Soporte Técnico verificarán que las aplicaciones de operación de **Tecnologías Eficientes de Villa** mantengan los registros de eventos, incluyendo la información detallada de la operación o actividades efectuadas por los usuarios.

13.3.20.2. Los mecanismos de control para salvaguardar la integridad, confidencialidad y disponibilidad de la información crítica de **Tecnologías Eficientes de Villa** deben ser revisados por el Área de Operaciones para corroborar su eficiente y eficaz implementación.

13.3.20.3. Las revisiones deben ser programadas por el Director de Operaciones por lo menos una vez al año, acotando el alcance de las mismas y acordando con el propietario del activo las pruebas técnicas que se realizarán.

13.3.20.4. Previo a las revisiones de aplicaciones de operación crítica el Director de Operaciones debe analizar el impacto que podría causar a los servicios sustantivos de **Tecnologías Eficientes de Villa** y determinar las acciones que se deben tomar en caso de un incidente de servicio.

13.3.20.5. Las revisiones a las aplicaciones de operación crítica deben ser ejecutadas fuera de horarios en donde pudiera haber afectaciones de disponibilidad de los aplicativos Institucionales hacia los usuarios.

13.3.20.6. El Coordinador de Soporte Técnico debe brindar accesos temporales a responsables de revisión y deben ser proporcionando solo los privilegios necesarios para la realización de las auditorias, considerando el alcance de la revisión y en cumplimiento con la Política de Control de Accesos.

13.3.20.7. Derivado de la revisión se debe emitir un reporte por parte del Área de Operaciones con los hallazgos encontrados, de manera que se asignen responsables y tiempos compromiso para su atención.

13.3.20.8. Los registros de la infraestructura tecnológica que fue revisada deben ser

resguardados durante al menos 90 días.

14.SOP-EDM-08-P01 Seguridad de las comunicaciones

14.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para mantener un nivel adecuado de protección en el intercambio de información y flujo de datos hacia la nube de **Tecnologías Eficientes de Villa**.

14.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos; así como a las partes interesadas del SGI.

14.3. Responsabilidades

14.3.1. El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política de Seguridad en las Comunicaciones dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

14.3.2. El Líder de Infraestructura es responsable de establecer la gestión de la red, para la transferencia de la información.

14.3.3. El Oficial de Seguridad de la Información y el Auditor es responsable de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

14.3.4. El Director de Operaciones es responsable de hacer del conocimiento a las partes interesadas externas del SGI la Política de Seguridad de las Comunicaciones y exhortarlos a su cumplimiento.

14.3.5. Las partes interesadas externas del SGI son responsables de dar cumplimiento a la Política de Seguridad en las Comunicaciones dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial

cuidado en sus prohibiciones.

14.3.6. SOP-EDM-01-P08-02 Controles de red

14.3.6.1. El acceso a la red y los servicios de red deben estar basado en el perfil de acceso definido por el Coordinador de Soporte Técnico para cada uno de los activos de información

14.3.6.2. El Coordinador de Soporte Técnico debe habilitar el acceso a los usuarios y/o equipos, para acceder a los recursos de la red basado en el perfil de acceso definido y/o listas de acceso.

14.3.6.3. El personal interno de **Tecnologías Eficientes de Villa** para el uso de los aplicativos Institucionales, cuando se acceda a ellos a través de redes públicas, debe cuidar que la red pública sea segura; ya sea por dispositivos propiedad de **Tecnologías Eficientes De Villa** o personales.

14.3.6.4. Los permisos proporcionados por el Coordinador de Soporte Técnico de acceso a la red (tales como: cuentas de usuario y contraseñas) son personales e intransferibles, por lo tanto, queda prohibido hacer uso de recursos distintos a los asignados, así como el revelar, cambiar o duplicar los mismos.

14.3.6.5. Está prohibido que los usuarios de la red, equipos y dispositivos móviles modifiquen y/o adicionen la configuración, infraestructura y/o servicios de red proporcionados por **Tecnologías Eficientes de Villa**; cualquier requerimiento de modificación debe realizarse por el Coordinador de Soporte Técnico a través del procedimiento de control de cambios establecido.

14.3.6.6. La difusión no autorizada de configuración, diseño, esquemas e infraestructura de la red de **Tecnologías Eficientes de Villa** hacia entidades ajenas está prohibida.

14.3.6.7. Los controles de Autenticación de la red y sus servicios deben ser definidos por el Coordinador de Soporte Técnico y deben cumplir con la Política de Control de Accesos.

14.3.7. SOP-EDM-01-P08-03 Seguridad en los servicios de red

14.3.7.1. El Coordinador de Soporte Técnico debe definir e implementar los mecanismos de control que corroboren la confidencialidad, integridad, disponibilidad y confiabilidad de los servicios de red, así como el nivel de servicio de dichos servicios, ya sean proporcionados internamente por **Tecnologías Eficientes De Villa** o por un externo.

14.3.7.2. El Coordinador de Soporte Técnico debe monitorear la adecuada implementación de los mecanismos de control, operación y niveles de servicio para los servicios de red.

14.3.7.3. El Coordinador de Soporte Técnico debe limitar el acceso a redes alámbricas o inalámbricas con filtro de contenido. Estas redes deben contar con mecanismos de control que aseguren la integridad, confidencialidad y disponibilidad de la información de **Tecnologías Eficientes de Villa**, utilizando filtrado de tráfico entrante y saliente.

14.3.8. SOP-EDM-01-P08-04 Segregación en redes

14.3.8.1. La red de **Tecnologías Eficientes de Villa** debe estar segregada, considerando la criticidad de la información que se intercambia en las diferentes áreas de **Tecnologías Eficientes de Villa**, a manera de reducir el riesgo de acceso no autorizado.

14.3.8.2. El Coordinador de Soporte Técnico debe definir e implementar los perímetros de seguridad que sean convenientes para la operación de **Tecnologías Eficientes de Villa**; estos perímetros se implementan mediante la instalación de dispositivos de seguridad (routers, gateways, firewalls) o el uso de redes seguras, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

14.3.8.3. La segregación de la red debe permitir el uso de dominios independientes para el acceso al personal de **Tecnologías Eficientes de Villa** y para el acceso a partes interesadas externas del SGI.

14.3.8.4. Las excepciones en la segregación de la red deben estar debidamente justificadas, documentadas y aprobadas por el Coordinador de Soporte Técnico

14.3.9. SOP-EDM-01-P08-05 Mecanismos para la transferencia de la información

14.3.9.1. El Director de Operaciones debe establecer la normativa, así como definir e implementar los mecanismos de control para la transferencia de información transaccional dentro de la infraestructura de **Tecnologías Eficientes de Villa**.

14.3.9.2. La información altamente sensible no debe ser transmitida por herramientas de mensajería electrónica personal.

14.3.9.3. Está prohibida la transmisión de información por medio de servicios de almacenamiento personal en línea, es decir, aquellas unidades virtuales de almacenamiento por medio de Internet, las cuales incluyen, pero no se limitan a Google Drive, Dropbox, Rapidshare, MediaFire, WeTransfer, etcétera, a menos que se consideren de uso Institucional.

14.3.9.4. Está prohibido a las partes interesadas del SGI guardar y/o transferir, bajo la infraestructura de la red, material ajeno a **Tecnologías Eficientes de Villa**, tal como: material obsceno, racista, mensajes ofensivos, mensajes cadena, música, videos, mensajes multimedia, software, etcétera.

14.3.10. SOP-EDM-01-P08-06 Acuerdos en la transferencia de información

14.3.11. La Consejería Jurídica debe establecer acuerdos formales para el envío y recepción de información a personal externo, aliados estratégicos, contratistas y usuarios de terceras partes, los cuales deben cumplir la Política de Mecanismos para la Transferencia de la Información.

14.3.12. SOP-EDM-01-P08-07 Mensajería electrónica

14.3.12.1. El Coordinador de Soporte Técnico debe definir e implementar los mecanismos de control para la asignación, gestión, operación, resguardo y seguridad de la información de los sistemas de mensajería electrónica.

14.3.12.2. El acceso a los sistemas de mensajería electrónica debe cumplir con la Política de Control de Accesos.

14.3.12.3. Los usuarios de mensajería electrónica Institucional sólo se deben asignar al personal de **Tecnologías Eficientes de Villa**.

14.3.12.4. La mensajería electrónica debe ser utilizada sólo para fines de **Tecnologías Eficientes de Villa**, por lo que los mensajes enviados y recibidos a través de ésta, son considerados registros propiedad de **Tecnologías Eficientes de Villa**, por tanto, **Tecnologías Eficientes de Villa** se reserva el derecho de acceso y revisión de cualquier mensaje enviado a través de sus sistemas de mensajería electrónica.

14.3.12.5. El uso de correos o mensajería electrónica personal para desempeñar sus funciones dentro de **Tecnologías Eficientes de Villa** no está permitido.

14.3.12.6. Las herramientas de correo y mensajería electrónica Institucionales deben permitir verificar el correcto direccionamiento de la información hacia quien fue

enviada.

14.3.12.7. Está prohibido divulgar información sensible a través de redes sociales, Institucional o personal, las cuales incluyen, pero no se limitan a Facebook, Twitter, Youtube, LinkedIn

14.3.13. SOP-EDM-01-P08-08 Acuerdos de confidencialidad

14.3.14. La Consejería Jurídica debe definir las cláusulas del acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa**.

14.3.15. El propietario de activo debe definir el uso aceptable de los activos de información para el personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones así como del uso aceptable de los activos de información para las partes interesadas externas del SGI, mismas que deben estar alineadas a las políticas internas, requerimientos normativos, las leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa.**

14.3.16. La Consejería Jurídica es responsable de definir el mensaje de aviso de confidencialidad para el intercambio de información, por medio de mensajería electrónica Institucional.

14.3.17. El acuerdo de confidencialidad y no divulgación de información y el uso aceptable de los activos de información debe indicar las actividades de control y monitoreo que pueden ser realizadas para corroborar el adecuado uso de la información y sus activos a fin de no violar el derecho a la privacidad del personal de **Tecnologías Eficientes de Villa**, personal externo y usuarios de terceras partes.

14.3.18. Las cláusulas del acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa** deben de tener una vigencia de por lo menos un año al finalizar la relación laboral y/o la prestación de servicio con **Tecnologías Eficientes de Villa**.

14.3.19. Las cláusulas del acuerdo de confidencialidad y no divulgación de información y, el uso aceptable de los activos de información debe ser revisada por lo menos cada año para confirmar que sigan siendo actuales y apropiadas al entorno de **Tecnologías Eficientes de Villa.**

14.3.20. La violación de un acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa**, así como del uso aceptable de los activos de información debe ser tratada como un incidente de seguridad cumpliendo la Política

de Gestión de Incidentes de Seguridad de la Información.

15. SOP-EDM-01-P10 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas y Aplicaciones

15.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para corroborar que la adquisición, desarrollo y mantenimiento de los sistemas de información en propiedad de **Tecnologías Eficientes de Villa** se realiza de manera segura.

15.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones, cuando se adquieran, desarrollen o den mantenimiento a los sistemas y aplicaciones.

15.3. Responsabilidad

15.3.1. El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política de Adquisición, desarrollo y mantenimiento de sistemas y aplicaciones dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

15.3.2. El Director de Operaciones es responsable de gestionar los desarrollos y mantenimientos en las aplicaciones.

15.3.3. El Líder de Infraestructura en colaboración con el Coordinador de Soporte Técnico son responsables de diseñar la estructura de hardware, software y redes física y/o virtual.

15.3.4. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de manera correcta.

15.3.5. El Director de Operaciones es responsable de hacer del conocimiento a las partes interesadas externas del SGI la Política de Adquisición, Desarrollo y Mantenimiento de

Sistemas y exhortarlos a su cumplimiento.

15.3.6. Las partes interesadas externas del SGI son responsables de dar cumplimiento a la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

15.3.7. SOP-EDM-01-P10-01 Análisis y especificación de requerimientos de seguridad

15.3.7.1. Previo a la adquisición, desarrollo o mantenimiento de un aplicativo, el Área de Operaciones y el Coordinador de Soporte Técnico deben identificar los requerimientos de funcionalidad y los requerimientos técnicos relacionados con la seguridad de la información del aplicativo.

15.3.8. SOP-EDM-01-P10-02 Aseguramiento del uso de aplicativos Institucionales en redes seguras

15.3.8.1. Se deben de utilizar redes seguras (Para saber que es una red segura verifique el instructivo), para el uso de aplicativos Institucionales, ya sea por dispositivos propiedad de **Tecnologías Eficientes de Villa** o personales, de manera que se proteja de actividad fraudulenta la información utilizada durante el servicio, reduciendo el riesgo de consulta o modificación no autorizada.

15.3.9. SOP-EDM-01-P10-03 Protección de transacciones durante el uso de los aplicativos Institucionales

15.3.9.1. Se deben proteger las transacciones realizadas en los aplicativos Institucionales a fin de evitar comprometer la información sensible utilizada, evitando:

- Transmisión incompleta.
- Errores de enrutamiento.
- Alteración de mensajes no autorizados.
- Divulgación no autorizada.
- Duplicación del mensaje no autorizado o reproducción.

15.3.9.2. El Área de Operaciones y el Coordinador de Soporte Técnico deben definir e implementar los mecanismos de seguridad para asegurar la disponibilidad, confiabilidad e integridad de la información usada en las transacciones. Los mecanismos de seguridad deben reducir el riesgo de ataques como SQL injection, Cross Side Scripting, Inyección de archivos, Defacement, LDAP injection, entre otros.

15.3.9.3. En caso de identificar algún ataque de seguridad derivado de un hueco de seguridad en las aplicaciones, este se debe reportar al Líder de Soporte Técnico como un incidente de Seguridad de la Información.

15.3.10. SOP-EDM-01-P10-04 Desarrollo seguro

15.3.10.1. Se deben establecer reglas para el desarrollo seguro, considerando los siguientes aspectos:

- Mantener un entorno de desarrollo seguro.
- Usar una metodología de desarrollo del software estándar.
- Usar directrices de codificación.
- Usar repositorios seguros.
- Mantener un control de versiones durante la vida del proyecto.
- Tener conocimiento acerca de la seguridad en los aplicativos.
- Tener capacidad de identificación y corrección de vulnerabilidades por los desarrolladores.

15.3.10.2. Se deben usar técnicas de programación seguras tanto para los nuevos desarrollos como para casos de re-uso de escenarios anteriores. Las técnicas seguras deben incluir entre otras:

- Prevención de inyección de SQL (SQL Injection). Las consultas SQL de las aplicaciones deben realizarse mediante enunciados preparados (prepared statements) y evitar ensamblar consultas SQL con los parámetros enviados por el usuario (vía POST o GET).
- Prevención de inyección de código dinámico (Cross Side Scripting). El código que genera el contenido dinámico de las aplicaciones no debe hacer uso de los parámetros proporcionados por el usuario solo si ha sido pre-procesado.
- Prevención de inyección de archivos. Las aplicaciones que reciban archivos que estén expuestos en rutas públicas deben contar con mecanismos que evalúen si se trata de virus, troyanos o archivos para obtener acceso administrativo a las aplicaciones; una vez identificada la amenaza esta debe ser eliminada.

15.3.10.3. Se debe evitar crear copias de archivos de configuración con otra extensión en los servidores de producción; Los archivos de configuración, tales como web.config y php.ini, con extensión bak, old, 1, etcétera, pueden descargarse por internet y exponer información sensible de las aplicaciones (direcciones IP, contraseñas, bases de datos y otros elementos).

15.3.10.4. El Director de Operaciones debe contar con un registro de los ataques de seguridad derivados de un hueco en el desarrollo aplicativo, con el objeto de ser considerada su prevención tanto para los nuevos desarrollos como para casos de reúso de escenarios anteriores.

15.3.11. SOP-EDM-01-P10-05 Control de cambios en los aplicativos

15.3.11.1. El Director de Operaciones debe administrar y controlar los cambios durante el ciclo de vida de desarrollo de los aplicativos, a fin de minimizar el impacto de posibles incidentes, mediante un proceso de administración de cambios formalizado.

15.3.11.2. El Director de Operaciones deben verificar que previo a un cambio relacionado con aplicaciones, los componentes tales como instancias de base de datos o código fuente que son necesarios para la aplicación, sean respaldados, con la finalidad de permitir la restauración a un punto anterior en caso presentarse fallas al efectuar el cambio.

15.3.11.3. Se debe verificar el código publicado en los ambientes de pruebas y de ser posible en producción para detectar la existencia de huecos de seguridad, puertas traseras (backdoors) o código no autorizado.

15.3.12. SOP-EDM-01-P10-06 Revisión técnica de aplicaciones después de cambios en la plataforma operativa

15.3.12.1. Cuando se realice algún cambio de alto impacto a las plataformas operativas, como sistemas operativos, endurecimiento (hardening), bases de datos o plataformas que soporten aplicaciones, se deben revisar y probar dichos cambios, a fin de validar que no representen un impacto negativo en la seguridad y/o en las áreas de Operaciones de **Tecnologías Eficientes De Villa.**

15.3.13. SOP-EDM-01-P10-07 Principios de ingeniería para la seguridad de las aplicaciones

15.3.13.1. Se debe contar dentro de la arquitectura tecnológica, la estructura de hardware, software y redes requerida para el desarrollo e implementación de aplicaciones seguras.

15.3.13.2. Para las aplicaciones que actualmente no cumplen con la estructura de aplicaciones seguras, el Director de Operaciones debe evaluar el costo-beneficio de

la adopción de esta arquitectura tecnológica, y en su caso implementar esta estructura. (Verificar en el Manual/Instructivo de desarrollo seguro).

15.3.14. SOP-EDM-01-P10-08 Entorno de desarrollo seguro

15.3.14.1. Los Líder de área de Operaciones debe utilizar una metodología para el desarrollo de software que se adapte a las necesidades de **Tecnologías Eficientes de Villa** y que contemple dentro del ciclo de desarrollo la aplicación de buenas prácticas de desarrollo seguro, incluyendo a nivel código para la prevención de los ataques más comunes.

15.3.14.2. El Director de Operaciones debe gestionar los accesos y roles en los ambientes de desarrollo, pruebas y producción, de tal manera que no exista el conflicto de intereses y se mantenga una correcta segregación de tareas.

15.3.15. SOP-EDM-01-P10-09 Desarrollo tercerizado

15.3.15.1. Previo a la aceptación de un servicio de desarrollo tercerizado, se debe corroborar que la aplicación cuente con los requerimientos estipulados en el Contrato, que cuente con acuerdos de propiedad intelectual, que se hayan realizado pruebas de posibles vulnerabilidades, que no contenga código malicioso, y que cumpla con lo establecido en la arquitectura tecnológica, las buenas prácticas a nivel código para la prevención de los ataques más comunes, así como el cumplimiento de la Política de Requerimientos de Seguridad de Sistemas de Información.

15.3.16. SOP-EDM-01-P10-10 Pruebas de seguridad y aceptación del sistema

15.3.16.1. El Director de Operaciones ante la liberación al ambiente productivo de una aplicación, debe realizar un proceso de verificación de la adecuada implementación de la estructura de seguridad y de la adhesión a las reglas de desarrollo seguro, así como realizar un análisis de código malicioso y escáneres de vulnerabilidades; las excepciones identificadas de probabilidad y/o impacto alto deben ser corregidas durante el desarrollo para la aceptación del sistema.

15.3.17. SOP-EDM-01-P10-11 Protección de datos de prueba

15.3.17.1. El Líder de Proyecto es responsable de los datos para la realización de pruebas a las aplicaciones deben ser seleccionados, controlados y protegidos adecuadamente; los datos utilizados para las pruebas de las aplicaciones no deben tener relación con los datos originales del ambiente productivo.

15.3.17.2. Está prohibido el uso de datos operativos que contengan información sensible para la realización de pruebas en las aplicaciones.

15.3.17.3. En caso de que las pruebas requieran el uso de información real de operación para garantizar los niveles de servicio requeridos se requerirá que la información sea ofuscada o intercalada de tal manera que no se puedan construir registros originales completos de la información.

16.SOP-EDM-01-P11 Relación con contratistas

16.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para la gestión del personal externo, aliados estratégicos, contratistas y usuarios de terceras partes.

16.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones, cuando se solicitan, contratan y gestionan proyectos relacionados con la entrega o prestación de productos y servicios de partes interesadas externas del SGI que requieren acceso a la información de **Tecnologías Eficientes de Villa.**

16.3. Responsabilidades

16.3.1. El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política de Relación con Contratistas dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

16.3.2. El Director de Operaciones y el Gerente de Compras son responsables de establecer la gestión de los contratistas.

16.3.3. El Coordinador de Soporte Técnico es responsable de gestionar la seguridad física.

16.3.4. El Gerente de Recursos Humanos es responsable de establecer el programa de entrenamiento y conciencia en materia de Seguridad la Información.

16.3.5. El Director de Operaciones y el Coordinador de Soporte Técnico son responsables conforme su área de establecer y gestionar los accesos lógicos al personal externo y usuarios de terceras partes.

16.3.6. El Gerente de Recursos Humanos es responsable de establecer y gestionar los accesos físicos al personal externo y usuarios de terceras partes.

16.3.7. El Director de Operaciones y el Gerente de Compras son responsables de la supervisión y ejecución del contratista para definir las necesidades de los productos y servicios requeridos por **Tecnologías Eficientes de Villa**.

16.3.8. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

16.3.9. El Director de Operaciones y el Gerente de Compras son responsables de hacer del conocimiento a las partes interesadas externas del SGSI la Política de Relación con Contratistas y exhortarlos a su cumplimiento.

16.3.10. Las áreas participantes en la adquisición y arrendamiento de productos y contratación de servicios de **Tecnologías Eficientes De Villa** deben ser capacitadas en el proceso de gestión de proveedores por el Gerente de Compras.

16.3.11. La Consejería Jurídica debe definir las cláusulas del acuerdo de confidencialidad y no divulgación de información de **Tecnologías Eficientes De Villa** (empresarial e individual) y Gerencia de Compras es responsable de la socialización de la misma.

16.3.12. El Coordinador de Soporte Técnico debe definir e implementar los mecanismos de control necesarios para la protección de los activos de información a los que tendrán acceso las partes interesadas externas del SGI.

16.3.13. La Consejería Jurídica y el Coordinador de Soporte Técnico son responsables de la supervisión y ejecución del instrumento jurídico para identificar y determinar las especificaciones técnicas y de seguridad particulares de los productos y servicios requeridos por las áreas de **Tecnologías Eficientes De Villa**. La evaluación y contratación de productos y servicios se debe basar en la demostración del cumplimiento de las especificaciones solicitadas por áreas usuarias de **Tecnologías Eficientes de Villa**.

16.3.14. SOP-EDM-01-P11-01 Atención de tópicos de seguridad para los contratistas

16.3.14.1. La Consejería Jurídica en coordinación con la Gerencia de Compras deben establecer las cláusulas de seguridad de productos y servicios, éstas deben incluir la obligación de firmar acuerdos de confidencialidad y no divulgación de información de TECNOLOGÍAS EFICIENTES DE VILLA.

16.3.14.2. Las partes interesadas externas del SGI solo podrán reproducir o extraer información sensible de **Tecnologías Eficientes de Villa** cuando sea necesario para el cumplimiento de sus actividades con autorización previa y por escrito del responsable del Proyecto para la supervisión del contratista.

16.3.14.3. Las partes interesadas externas del SGI deben alinearse a la normativa interna establecida para la atención de los incidentes de seguridad, por lo que, de identificar algún posible evento de seguridad, debe notificarlo por los medios establecidos para este fin en cumplimiento con la Política de Incidentes de Seguridad de la Información.

16.3.14.4. La Gerencia de Compras en coordinación con la Dirección de Calidad son responsables de capacitar a las partes interesadas externas del SGI sobre la normativa interna de seguridad a la que debe alinearse durante la prestación de los servicios contratados.

16.3.15. SOP-EDM-01-P11-02 Cadena de suministros en servicios de contratistas

16.3.15.1. Las partes interesadas externas del SGI no deben ceder, traspasar, enajenar, ni por cualquier otro motivo transmitir las obligaciones y derechos, sin la autorización previa y por escrito de **Tecnologías Eficientes de Villa**.

16.3.15.2. El usuario de terceras partes debe apegarse a los acuerdos de confidencialidad y no divulgación, así como los requerimientos y las cláusulas de seguridad que fueron acordados entre el contratista y **Tecnologías Eficientes de Villa**, lo cual debe establecerse expresamente.

16.3.15.3. En caso de incumplimientos de los instrumentos jurídicos por parte del usuario de terceras partes, el contratista responsable de este será el acreedor de la sanción correspondiente.

16.3.16. SOP-EDM-01-P11-03 Monitoreo y revisión de servicios del contratista

16.3.16.1. La Consejería Jurídica es responsable del cumplimiento del instrumento jurídico,

así como de los acuerdos de confidencialidad y no divulgación de información de **Tecnologías Eficientes de Villa** por parte del personal externo, aliados estratégicos, contratistas y usuarios de terceras partes deben ser revisados por lo menos una vez o en periodos regulares de acuerdo con la duración de su instrumento jurídico.

16.3.17. SOP-EDM-01-P11-04 Gestión de cambios a los servicios del contratista

16.3.17.1. Las áreas usuarias que requieran cambios en los productos o servicios provistos por las partes interesadas externas del SGI deben evaluar el impacto por la Consejería Jurídica antes de realizar la solicitud de manera oficial.

16.3.17.2. Si el impacto de los cambios de los servicios no requiere de modificaciones en las cláusulas del instrumento jurídico del contratista, se deben documentar y firmar los acuerdos entre ambas partes.

16.3.17.3. Si el impacto de los cambios de los servicios requiere de modificaciones en las cláusulas del instrumento jurídico del contratista, se deben solicitar las modificaciones a las cláusulas necesarias en los instrumentos jurídicos por medio del proceso formal a la Consejería Jurídica.

17. SOP-EDM-01-P12 Política de Gestión de Incidentes de Seguridad de la Información

17.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para la correcta gestión de los incidentes de seguridad de la Información a fin de reducir el impacto que estos podrían causar en las áreas de Operaciones de **Tecnologías Eficientes De Villa**.

17.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes De Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como las partes interesadas del SGSI vinculados a través de instrumentos jurídicos.

17.3. Responsabilidades

17.3.1. El personal de **Tecnologías Eficientes De Villa** es responsable de implementar y dar cumplimiento a la Política de Gestión de Incidentes de Seguridad de la Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones

a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad de la información cualquier omisión que se conozca sobre el cumplimiento de dicha política.

17.3.2. El Oficial de Seguridad de la información es responsable de establecer el esquema de gestión de los incidentes.

17.3.3. El Gerente de Recursos Humanos es responsable de definir e implementar el plan de entrenamiento y concienciación en materia de Seguridad la Información.

17.3.4. El Líder de Infraestructura es responsable de proporcionar y gestionar la tecnología necesaria para reportar los incidentes de seguridad.

17.3.5. El personal de **Tecnologías Eficientes De Villa** es responsable de informar a la Dirección de Calidad los incidentes de Seguridad Informática.

17.3.6. Las partes interesadas externas del SGI son responsables de reportar eventos y debilidades de seguridad a la Dirección de Calidad.

17.3.7. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de la manera correcta.

17.3.8. El Director de Operaciones es responsable de hacer del conocimiento las partes interesadas externas del SGI la Política de Gestión de Incidentes de Seguridad de la Información y exhortarlos a su cumplimiento.

17.3.9. Las partes interesadas externas del SGI son responsables de dar cumplimiento a la Política de Gestión de Incidentes de Seguridad de la Información dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

17.3.10. SOP-EDM-01-P12-01 Reporte de eventos de seguridad de la información

17.3.10.1. El Auditor Interno de **Tecnologías Eficientes de Villa** será el encargado de manejar los problemas relacionados con incidentes de seguridad, el cual debe contar con los conocimientos necesarios a nivel técnico sobre los diversos dominios de **Tecnologías Eficientes de Villa**, para la correcta contención y solución de los incidentes de seguridad.

17.3.10.2. Se debe establecer la normativa interna para la atención y respuesta a los incidentes de seguridad, incluyendo los de seguridad física y tecnológica; estos deben incluir los roles y responsabilidades de la gestión de los incidentes y su comunicación.

17.3.10.3. Los Líderes de Soporte Técnico e Infraestructura deben proveer y gestionar los mecanismos tecnológicos necesarios para que los incidentes de seguridad sean reportados y registrados.

17.3.11. SOP-EDM-01-P12-02 Reporte de debilidades de seguridad de la información

17.3.11.1. Las partes interesadas del SGI que utilicen los servicios y aplicativos Institucionales debe reportar al Coordinador de Soporte Técnico las posibles debilidades de control identificadas, a fin de prevenir algún incidente de seguridad de la información.

17.3.12. SOP-EDM-01-P12-03 Evaluación y decisión sobre eventos de seguridad de la información

17.3.12.1. El Líder de Soporte Técnico debe de realizar una evaluación a los eventos de seguridad reportados, con el fin de decidir oportunamente si el evento debe ser clasificado como un incidente de seguridad de la información, de manera que se atienda lo más rápido posible, reduciendo el impacto en la operación de **Tecnologías Eficientes de Villa**.

17.3.12.2. El Líder de Soporte Técnico debe definir y aplicar las medidas de contención necesarias a fin de evitar la propagación del incidente de seguridad de la información.

17.3.12.3. Los eventos y debilidades no clasificados como incidente de seguridad deben ser tratados y resueltos de acuerdo con su impacto en la operación de **Tecnologías Eficientes de Villa.**

17.3.13. SOP-EDM-01-P12-04 Respuesta a incidentes de seguridad de la información

17.3.13.1. El Líder del proyecto debe responder los incidentes de acuerdo con la normativa, identificando mejoras en el proceso, aplicando y notificando cambios en el mismo cuando sea necesario.

17.3.14. SOP-EDM-P12-05 Aprendizaje de los incidentes de seguridad de la información

17.3.14.1. El conocimiento obtenido del análisis y de la solución de los incidentes de seguridad se debe registrar en el SOP-BAI-08-F01 Registro de lecciones aprendidas (Registro de base de conocimiento), a fin de generar un antecedente para reducir los tiempos de atención, solución e impacto de futuros incidentes de seguridad.

17.3.14.2. El responsable de dar solución al incidente al momento de registrarlo en el SOP-BAI-08-F01 Registro de lecciones aprendidas (Registro de base de conocimiento), debiendo incluir cuando menos la siguiente información:

- Nombre de la persona que reporta.
- Información del incidente de seguridad.
- Fecha y hora del reporte.
- Actividades realizadas para la atención y solución.
- Causa del incidente.

17.3.14.3. El SMT debe informar y solicitar recursos en caso de ser requeridos para prevenir futuros incidentes derivado de las lecciones aprendidas documentadas.

17.3.15. SOP-EDM-P12-06 Recopilación de evidencia

17.3.15.1. El Coordinador de Soporte Técnico y el Líder de Soporte Técnico deben establecer la normativa para la identificación, recopilación y custodia de evidencias de los incidentes de Seguridad de la Información para propósitos disciplinarios o legales si es el caso.

17.3.15.2. El Coordinador de Soporte Técnico y el Líder de Soporte Técnico deben definir e implementar los mecanismos de control para la salvaguarda de la evidencia de los incidentes de seguridad.

18.SOP-EDM-01-P13 Seguridad de la información para la gestión de la continuidad.

18.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para conservar la Seguridad de la Información en los planes de continuidad y recuperación de las áreas de Operaciones que soportan los servicios críticos de **Tecnologías Eficientes De Villa**, diseñados para mantener la operación en un nivel aceptable durante un evento disruptivo.

18.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes De Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes De Villa** en el ejercicio de sus funciones.

18.3. Responsabilidades

18.3.1. El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política de Aspectos de seguridad de la información de la gestión de continuidad operativa dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad de la Información cualquier omisión que se conozca sobre el cumplimiento de dicha política.

18.3.2. El Director de Operaciones y el Líder de Infraestructura son los responsables de establecer el Plan de Continuidad del Negocio (BCP).

18.3.3. El Director de Operaciones y el Líder de Infraestructura son responsables concientizar sobre el Plan de Continuidad del Negocio (BCP), además de los procesos que deriven de estos.

18.3.4. El Oficial de Seguridad de la Información y el Auditor son responsables de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de manera correcta.

18.3.5. Las partes interesadas del SGI son responsables de dar cumplimiento a la Política de Seguridad de la Información para la Gestión de Continuidad del Negocio dentro de sus áreas de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

18.3.6. SOP-EDM-01-P13-01 Planeación de la continuidad de la seguridad de la información

18.3.6.1. El Director de Operaciones debe realizar un Análisis de Impacto al Negocio (BIA) a fin de identificar los servicios críticos de **Tecnologías Eficientes de Villa.**

18.3.6.2. El Director de Operaciones y el área de Órgano Interno de Control deben realizar un Análisis de Riesgos de Continuidad, con el fin de identificar los riesgos internos y externos de **Tecnologías Eficientes de Villa.**

18.3.6.3. De acuerdo con los resultados del Análisis de Impacto al Negocio y del Análisis de

Riesgo el Área de Operaciones debe establecer y documentar las estrategias de recuperación en el Plan de Continuidad de Negocio (BCP).

18.3.6.4. Los Planes de Continuidad del Negocio (BCP) debe considerar la continuidad de la Seguridad de la Información, de manera que se determinen los controles mínimos de seguridad que deben aplicarse en cada estrategia de recuperación y de continuidad de **Tecnologías Eficientes de Villa**.

18.3.6.5. La Dirección de Operaciones debe establecer las acciones y procesos necesarios para la recuperación y continuidad de **Tecnologías Eficientes de Villa**, incluyendo los procesos para la evaluación de los eventos que podrían afectar las área de Operaciones de **Tecnologías Eficientes de Villa** y la activación del Plan de Continuidad del Negocio (BCP).

18.3.7. SOP-EDM-01-P13-02 Implementación de la continuidad de la seguridad de la información

18.3.7.1. El Dirección de Operaciones debe implementar los controles de seguridad necesarios para la continuidad de la Seguridad de la Información en las estrategias de recuperación y continuidad del negocio, así como determinar los controles compensatorios para los controles que no se puedan mantener durante un evento que afecte la continuidad de **Tecnologías Eficientes de Villa**.

18.3.7.2. El Dirección de Operaciones debe asignar al personal de **Tecnologías Eficientes De Villa** con la autoridad y la competencia profesional necesaria para realizar las actividades establecidas en Plan Continuidad del Negocio (BCP), garantizando el nivel requerido de continuidad para la Seguridad de la Información durante una situación adversa.

18.3.7.3. El Plan Continuidad del Negocio (BCP) deben incluir el directorio del personal responsable de la recuperación y continuidad de **Tecnologías Eficientes de Villa**.

18.3.7.4. El Plan de Continuidad del Negocio (BCP) debe estar actualizados y accesibles en todo momento para consulta del personal de T**ecnologías Eficientes de Villa** con la autoridad y competencia profesional.

18.3.7.5. **SOP-EDM-01-P13-03 Verificación, revisión y evaluación de la continuidad de la seguridad de la información**

18.3.7.6. El Plan de Continuidad del Negocio (BCP) debe ser probado por lo menos una vez al año o cuando hayan sufrido modificaciones significativas por la Dirección de Operaciones.

18.3.7.7. Las pruebas al Plan de Continuidad del Negocio (BCP) deben incluir la verificación de los controles de continuidad de la seguridad de la información en cada escenario que será evaluado, para asegurarse que son consistentes con los objetivos de continuidad; estas pruebas son diferentes a las pruebas de seguridad de la información general.

18.3.7.8. La prueba al Plan de Continuidad del Negocio (BCP) debe realizarse de manera programada en horarios en donde el impacto a la operación de **Tecnologías Eficientes de Villa** sea controlado.

18.3.7.9. El Director de Operaciones debe documentar y analizar los resultados de las pruebas realizadas al Plan de Continuidad del Negocio (BCP).

18.3.7.10. Se debe informar al Director Generar y el área de Órgano Interno de Control sobre los resultados de las pruebas e investigarse aquellos que no hayan sido exitosos.

18.3.7.11. El Plan Continuidad del Negocio (BCP) debe ser revisado por el Área de Operaciones por lo menos una vez al año y actualizado cuando sea necesario, derivado de los resultados de las pruebas previas realizadas o de cambios significativos en la infraestructura, el entorno y/o en la operación de **Tecnologías Eficientes de Villa.**

18.3.8. SOP-EDM-01-P13-04 Disponibilidad de facilidades de procesamiento de información

18.3.8.1. El Líder de Infraestructura debe determinar de acuerdo con el Análisis de Impacto al Negocio (BIA), la infraestructura tecnológica clave que soporta servicios críticos de manera que se certifique su disponibilidad utilizando arquitecturas o componentes redundantes.

18.3.8.2. El Director de Operaciones y el Líder de Infraestructura deben incluir en las pruebas del Plan de Continuidad del Negocio (BCP) las pruebas a los sistemas y aplicaciones redundantes, de tal forma que se verifique su desempeño.

19.SOP-EDM-01-P14 Política de Cumplimiento

19.1. Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para definir y documentar los requisitos estatutarios, regulatorios y contractuales para la prevención del fraude, la protección de propiedad intelectual y la de datos personales que maneja **Tecnologías Eficientes de Villa**.

19.2. Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como a las partes interesadas del SGSI vinculados a través de instrumentos jurídicos.

19.3. Responsabilidades

19.3.1. El personal de **Tecnologías Eficientes de Villa** son responsables de implementar y dar cumplimiento a la Política de Cumplimiento dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

19.3.2. La Consejería Jurídica es responsable de:

- Establecer el esquema del uso de datos personales.
- Mantener los registros sobre acuerdos de voluntades de información confidencial que es transmitida por o a los contratistas.
- Establecer las cláusulas para el uso de software legal en los contratos con contratistas.
- Establecer los convenios con contratistas para otorgar la garantía especial de software.
- Establecer las cláusulas para la cesión de derechos de propiedad intelectual de los desarrollos técnicos y científicos derivados de la ejecución de los instrumentos jurídicos con el personal de **Tecnologías Eficientes de Villa** y contratistas.
- Establecer el mensaje de aviso de privacidad para el intercambio de información personal.
- El control, atención y seguimiento a todas las solicitudes que ejerzan alguno de los derechos ARCO

19.3.3. La Consejería Jurídica es responsable de concientizar sobre requisitos estatutarios, regulatorios y contractuales en materia de Seguridad la Información por lo menos una vez al año.

19.3.4. El Director de Operaciones es responsable de definir e implementar los mecanismos de control para la adquisición o arrendamiento de software y sus licencias.

19.3.5. El Oficial de Seguridad de la Información y el Auditor son responsable de dar cumplimiento y seguimiento a todos los temas inherentes a la presente política, así como monitorear la implementación de los mecanismos de control para el acatamiento de manera correcta.

19.3.6. Las partes interesadas externas del SGSI son responsables de implementar y dar cumplimiento a la Política de Cumplimiento regulatorio, contractual y estatutario dentro de su área de responsabilidad y, de abstenerse de realizar incumplimientos o infracciones a la misma, manteniendo especial cuidado en sus prohibiciones.

19.3.7. SOP-EDM-01-P14-01 Identificación de legislación vigente y registros contractuales

19.3.7.1. La Consejería Jurídica debe identificar las leyes, regulaciones, normas, políticas internas e instrumentos jurídicos a los que debe dar cumplimiento TECNOLOGÍAS EFICIENTES DE VILLA, así como las áreas involucradas en su cumplimiento.

19.3.7.2. La Consejería Jurídica en coordinación con la Gerencia de Recursos Humanos deben identificar y asignar los roles, responsabilidades y los términos en que darán cumplimiento a las leyes, regulaciones, normas, políticas internas e instrumentos jurídicos identificados.

19.3.7.3. La Consejería Jurídica debe monitorear periódicamente el cumplimiento de las leyes, regulaciones, normas, políticas internas e instrumentos jurídicos identificados, de manera que cualquier desviación sea revisada y atendida.

19.3.8. SOP-EDM-01-P14-02 Uso controlado de software

19.3.8.1. El Dirección de Operaciones y el Líder de Soporte Técnico deben establecer la normativa para la instalación, desinstalación y cambio de equipo asignado del software adquirido o arrendado e infraestructura tecnológica de **Tecnologías Eficientes de Villa.**

19.3.8.2. El Dirección de Operaciones y el Líder de Soporte Técnico deben definir e implementar los mecanismos de control para la adquisición o arrendamiento de software, así como de sus licencias para el uso controlado del mismo por el personal de **Tecnologías Eficientes de Villa**, en cumplimiento con la Política de Relación con

Contratistas.

19.3.8.3. Los equipos de cómputo propiedad de **Tecnologías Eficientes de Villa** deben contener el software permitido instalado, de manera que, si el personal de **Tecnologías Eficientes de Villa** requiere software adicional a este, debe solicitarlo de manera formal por los medios establecidos al Coordinador y Líder de Soporte Técnico.

19.3.8.4. El software instalado en los equipos de cómputo propiedad de **Tecnologías Eficientes de Villa** no debe sufrir cambios en su configuración por personal no autorizado.

19.3.8.5. El Líder de Soporte Técnico en coordinación con el auditor deben establecer un procedimiento para la revisión periódica del software licenciado adquirido o arrendado por **Tecnologías Eficientes de Villa**, instalado en la infraestructura tecnológica.

19.3.8.6. El software licenciado adquirido o arrendado por **Tecnologías Eficientes de Villa** que tenga vigencia, deben ser monitoreado periódicamente por la Coordinación de Soporte Técnico, con el fin de realizar las renovaciones de manera oportuna.

19.3.8.7. Se debe contar con registros que acrediten las licencias de software instaladas en los equipos de cómputo e infraestructura tecnológica.

19.3.8.8. La Consejería Jurídica debe incluir en los instrumentos jurídicos de prestación de servicios por parte de contratistas las cláusulas para el uso de software legal como parte de la ejecución de los proyectos dentro de **Tecnologías Eficientes de Villa**.

19.3.9. SOP-EDM-01-P14-03 Avisos de derechos de autor en software

19.3.9.1. Todos los aplicativos o programas de cómputo desarrollados por las partes interesadas del SGI, y/o documentación de programación que sean propiedad de **Tecnologías Eficientes de Villa**, deben incluir avisos de derechos de autor.

19.3.10. SOP-EDM-01-P14-04 Protección aplicable del derecho de autor

19.3.10.1. El personal de **Tecnologías Eficientes de Villa** debe investigar la propiedad intelectual de todo el material que visualicen en Internet, antes de usarlo para cualquier propósito.

19.3.11. SOP-EDM-01-P14-05 Protección de registros

19.3.12 La consejería Jurídica debe identificar y resguardar los registros que sean la evidencia del cumplimiento de las leyes y regulaciones que son aplicables a **Tecnologías Eficientes de Villa.**

19.3.13 SOP-EDM-01-P14-06 Protección de datos y privacidad de la información personal

19.3..13.1 La Consejería Jurídica en coordinación con Gerencia de Recursos Humanos deben establecer un marco para la gestión de datos personales que incluya la normativa interna y los mecanismos de control administrativos, físicos y técnicos que garanticen la confidencialidad, integridad y disponibilidad de los datos personales previniendo su daño, pérdida, alteración, destrucción, mal uso, así como el acceso, su tratamiento no autorizado de datos personales que se encuentren bajo custodia de **Tecnologías Eficientes de Villa**, durante la gestión de dichos datos; mismos que deben estar alineados a leyes y regulaciones aplicables a **Tecnologías Eficientes de Villa.**

19.3.13.2 La transferencia de datos personales a personal externo y contratistas debe estar formalizada y autorizada por la Consejería Jurídica; dicha transferencia solamente debe realizarse cuando sea indispensable para las actividades de **Tecnologías Eficientes de Villa.**

19.3.13.3 La Consejería Jurídica en todos los instrumentos jurídicos de prestación de servicios que impliquen el tratamiento de datos personales y sensibles de los usuarios o personal de **Tecnologías Eficientes de Villa**, a nombre y por cuenta de **Tecnologías Eficientes de Villa** con personal externo y contratistas, se debe incluir una cláusula donde se indique, que se otorga el nivel de protección de datos personales previsto por las leyes y regulaciones actuales que le apliquen a **Tecnologías Eficientes de Villa**.

19.3.13.4 El personal de **Tecnologías Eficientes de Villa,** personal externo y contratistas involucrados con el uso, procesamiento, almacenamiento, transferencia y custodia de datos personales al interior y exterior de las instalaciones de **Tecnologías Eficientes De Villa** debe seguir los procesos contra acceso no autorizado, pérdida, alteración y mal uso de datos personales previamente aprobados y comunicados.

19.3.13.5 La Consejería Jurídica en coordinación con la Gerencia de Recursos Humanos deben establecer la normativa para acceder, rectificar y cancelar los datos

personales que se encuentren bajo custodia de **Tecnologías Eficientes De Villa**, así como de oponerse al tratamiento de los mismos o revocar el consentimiento que para tal fin sea otorgado a **Tecnologías Eficientes de Villa**.

19.3.13.6 El acceso a los registros de **Tecnologías Eficientes De Villa** que contengan información de datos personales debe solicitarse formalmente por escrito a la Gerencia de Recursos Humanos.

19.3.13.7 Los datos personales en custodia de **Tecnologías Eficientes de Villa**, en uso por personal externo o contratistas, solo deben ser utilizados para finalidades señaladas y por el tiempo acordado con el responsable del dato.

19.3.13.8 Se debe contar con consentimiento legal del Titular de los datos personales para la transferencia de datos personales a personal externo y contratistas cuando sea indispensable para las actividades de **Tecnologías Eficientes de Villa.**

19.3.13.9 El personal externo y contratistas deben apegarse al marco para la gestión de datos personales de **Tecnologías Eficientes de Villa**.

19.3.13.10 La consejería Jurídica debe definir el mensaje de aviso de privacidad para el intercambio de información personal.

19.3.13.11 No debe existir un sistema de registros personales en **Tecnologías Eficientes de Villa** cuya existencia sea desconocida para las personas descritas en el mismo, solo si **Tecnologías Eficientes De Villa** lo considera necesario para el cumplimiento de sus obligaciones legales.

19.3.14 SOP-EDM-01-P14-07 Divulgación de datos personales

19.3.14.2 La información personal incluyendo, sin limitantes, la agregada, resumida, anónima, los estudios de casos individuales, o la información que identifica personas, y que sea recopilada por **Tecnologías Eficientes de Villa**, no se debe vender, alquilar y/o transferir a terceras personas**.**

19.3.15 SOP-EDM-01-P14-08 Registros de divulgación de información privada

19.3.15.2 Toda divulgación de información privada a contratistas se debe registrada por el Consejero Jurídico, y dichos registros se deben mantener por un periodo mínimo de un año.

19.3.16 SOP-EDM-01-P14-09 Privacidad de la información del usuario y personal de TECNOLOGÍAS EFICIENTES DE VILLA

19.3.16.2 La información que pueda ser vinculada directamente a un usuario o personal de **Tecnologías Eficientes De Villa** en específico sólo se debe revelar cuando estos hayan dado previo consentimiento por escrito, o si **Tecnologías Eficientes de Villa** está legalmente obligado a divulgar información.

19.3.17 SOP-EDM-01-P14-10 Divulgación de Información privada a organizaciones contratadas

19.3.17.2 El personal externo y contratistas, que gestione datos personales, no debe vender o arrendar dichos datos a terceras personas en ninguna forma.

19.3.17.3 El personal externo y contratistas, que gestione datos personales, no debe transferir dichos datos en ninguna forma, excepto cuando éstas firmen un acuerdo de confidencialidad a través del cual se les prohíba diseminar y hacer uso de esta con fines no autorizados.

19.3.18 SOP-EDM-01-P14-11 Regulación de los controles criptográficos

19.3.18.2 El Consejero Jurídico debe monitorear la entrada en vigor de leyes o regulaciones que incluyan temas de cifrado a las que **Tecnologías Eficientes de Villa** pueda estar sujeto, con el fin de darles cumplimiento.

19.3.19 SOP-EDM-01-P14-12 Prevención del fraude

19.3.19.2 El Consejero Jurídico debe colaborar en la identificación de los riesgos de fraude en **Tecnologías Eficientes de Villa.**

19.3.19.3 El Consejero Jurídico debe identificar, analizar y evaluar en las áreas de **Tecnologías Eficientes de Villa,** las acciones que induzcan promuevan, inciten o desemboquen en fraude, corrupción, soborno cohecho, nepotismo, tráfico de influencias y el uso inadecuado de información privilegiada, de las partes interesadas del SGI.

19.3.19.4 El Consejero Jurídico debe definir e implementar los mecanismos de control contra acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno, de las partes interesadas del SGI.

19.3.19.5 Cuando sea requerido por la Dirección de General, el Consejero Jurídico se debe colaborar en la generación de información precisa relacionada a cualquier investigación relacionada con fraude, corrupción o soborno y determinar la información que pudo quedar comprometida, con el fin de mejorar la gestión y los mecanismos de control de la plataforma tecnológica y los aplicativos de **Tecnologías Eficientes de Villa**.

19.3.20 SOP-EDM-01-P14-13 Revisión de la seguridad de la información

19.3.20.2 El Director de Operaciones en coordinación con la Dirección de Calidad deben planificar una revisión por lo menos una vez al año sobre la situación que guarda la seguridad de la información en **Tecnologías Eficientes de Villa**.

19.3.20.3 Con base en los resultados obtenidos de la revisión sobre la situación que guarda la seguridad de la información en **Tecnologías Eficientes de Villa**, el área revisada debe identificar, planificar e implementar oportunamente las acciones de mejoras requeridas.

19.3.20.4 SOP-EDM-01-P14-14 Revisión de los controles de los aplicativos Institucionales

19.3.20.4.1 El alcance de las revisiones a los aplicativos Institucionales se debe establecer basándose en los riesgos identificados y el impacto hacia **Tecnologías Eficientes de Villa**.

19.3.20.5 SOP-EDM-01-P14-15 Verificación de cumplimiento de Seguridad de la Información

19.3.20.5.1 La Consejería Jurídica en coordinación con el área de Órgano Interno de Control deben llevar a cabo una verificación periódica del cumplimiento de la normativa interna relacionados con la seguridad de la información, por medio de personal con la competencia profesional.

19.3.20.6 SOP-EDM-01-P14-16 Revisión independiente de la seguridad de la información

19.3.20.6.1 Periódicamente debe llevarse a cabo una revisión externa e independiente de la seguridad de la información y los controles de los aplicativos Institucionales para determinar su calidad y cumplimiento, por medio de personal con la competencia profesional.

19.3.20.7 SOP-EDM-01-P14-17 Cumplimiento de las políticas y normas de seguridad

19.3.20.7.1 La Consejería Jurídica en coordinación con el área de Soporte Técnico deben establecer el proceso para corroborar el cumplimiento de las políticas y normas de seguridad y ciberseguridad de la información dentro de los procesos de **Tecnologías Eficientes de Villa**.

19.3.20.7.2 Todos los sistemas de control, políticas y normas de seguridad deben ser susceptibles de cumplimiento forzoso, antes de adoptarse como parte de algún proceso operativo dentro de **Tecnologías Eficientes de Villa**.

19.3.21 SOP-EDM-01-P14-18 Etiquetas de contenido en Internet

19.3.21.2.1 Toda la información publicada en los sitios de comercio y de red de **Tecnologías Eficientes de Villa,** es de carácter público y comercial, no siendo así para las aplicaciones y/o sistemas que la empresa proporciona, ya que estos son en su totalidad de carácter privado.

19.3.22 SOP-EDM-01-P14-19 Comentarios públicos en sistemas electrónicos

19.3.22.2 Los comentarios no oficiales que los trabajadores publiquen en un sistema de correo electrónico, en foros electrónicos o en otros sistemas electrónicos, no se deben entender como la posición oficial o declaraciones formales de **Tecnologías Eficientes de Villa**.

19.3.22.3 La información pública debe estar disponible en la página web de **Tecnologías Eficientes de Villa** y la información sólo para uso interno debe estar disponible en la red interna de **Tecnologías Eficientes de Villa**.

19.3.23 SOP-EDM-01-P14-20 Control de contenido

19.3.23.2 Los aplicativos y sistemas de comunicación de **Tecnologías Eficientes de Villa** no deben ser utilizados para ejercitar el derecho a la libre expresión del participante. Éstos, incluyendo la intranet, no deben utilizarse como foro abierto para discutir los cambios Institucionales, los asuntos relativos a las políticas operativas, ni otros tópicos similares de **Tecnologías Eficientes de Villa**.

19.3.24 SOP-EDM-01-P14-22 Tipo de publicaciones

19.3.24.2 El contenido publicado en la Intranet de **Tecnologías Eficientes de Villa** debe ser

identificado, o bien como público o sólo para uso interno. Nunca se debe incluir información sensible en la intranet de **Tecnologías Eficientes de Villa.**

19.3.25 SOP-EDM-01-P14-23 Propiedad legal del material publicado

19.3.25.2 A menos que sea aprobado con anticipación, y explícitamente notificado en la página de Intranet, todo contenido incluido en la intranet de **Tecnologías Eficientes de Villa** es propiedad de **Tecnologías Eficientes de Villa**.

19.3.26 SOP-EDM-01-P14-24 Designación del propietario de la información

19.3.26.2 Todo contenido publicado en la Intranet de **Tecnologías Eficientes de Villa** debe tener un propietario designado. La información de contacto de este propietario debe estar claramente indicada en la página donde aparece el contenido.

20 SOP-EDM-01-P15 Política de Auditorías externas a Tecnologías Eficientes de Villa

20.1 Objetivo

Establecer las medidas de control para llevar a cabo auditorias de externos a **Tecnologías Eficientes de Villa** para conservar la Seguridad de la Información, diseñadas para mantener la operación en un nivel aceptable durante un evento disruptivo.

20.2 Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones.

20.3 Responsabilidades

20.3.1 El personal de **Tecnologías Eficientes de Villa**.es responsable de implementar y dar cumplimiento a la Política de Aspectos de seguridad de la información de la gestión de auditorías de externos dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar al Oficial de Seguridad de la Información cualquier omisión que se conozca sobre el cumplimiento de dicha política.

20.3.2 El Director de General y el Director de Operaciones son responsables de establecer el vínculo entre la empresa (Cliente) que auditará a **Tecnologías Eficientes de Vill**a.

20.3.4 El Oficial de seguridad es responsable de estar presente ante la auditoría externa (cliente) hacia **Tecnologías Eficientes de Villa**.

20.4 SOP-EDM-01-P15-01 Auditorías externas

20.4.1 Para el caso de auditorías de externos a **Tecnologías Eficientes de Villa** solo podrán ser llevadas a cabo por las partes interesadas externas que tengan un contrato con la misma.

20.4.2 Se entenderán como auditorías externas todo proceso que un agente externo someta a **Tecnologías Eficientes de Villa** con el único interés de confirmar la seguridad de la información que tiene la empresa hacia la posesión de los datos de la empresa que lo solicite.

20.4.3 En ninguna circunstancia se le dará acceso a información clasificada como confidencial y/o privada a ninguna empresa que no tenga vínculo directo con **Tecnologías Eficientes de Villa**.

20.4.4 Para el caso de las auditorías externas la información proporcionada de la empresa será únicamente concerniente contrato estipulado por el cual esté solicitando la auditoria

20.4.5 Toda auditoria de externos hacia **Tecnologías Eficientes de Villa** deberá ser solicitada de manera formal hacia la dirección General y/o Dirección de Operaciones

20.4.6 En ninguna circunstancia ningún colaborador deberá dar respuesta ni información de carácter sensible sin aprobación del superior inmediato o Dirección General.

21.SOP-EDM-01-P16 Política de Ambiental de TECNOLOGÍAS EFICIENTES DE VILLA

21.1 Objetivo

Establecer las medidas de control para dar cumplimiento de las leyes, las normas y los reglamentos aplicables en materia de medioambiente.

21.2 Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones.

21.3 Responsabilidades

21.3.1 El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política de Aspectos Ambientales dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar cualquier omisión que se conozca sobre el cumplimiento de dicha política.

21.4 SOP-EDM-01-P16-01 Adopción de medidas adecuadas para proteger el medioambiente

21.4.1 El personal de **Tecnologías Eficientes de Villa**.es responsable de establecer y operar un sistema de gestión ambiental diseñado para mejorar continuamente ambiental.

21.4.2 El Director de Operaciones es responsable de aumentar la conciencia medioambiental de nuestros empleados y, al mismo tiempo, los empoderar y animar a minimizar la huella ambiental.

21.4.3 El área de compras es responsable en la toma de decisiones de compra y subcontratación, cuando sea posible, especificar productos y servicios con menor impacto ambiental.

21.4.4 El área legal es responsable de identificar todas las regulaciones ambientales relevantes y obligaciones de cumplimiento relevantes con los requisitos ambientales de Tecnologías Eficientes de Villa.

21.4.5 El personal de **Tecnologías Eficientes de Villa** es responsable y debe estar comprometidos a proteger el medio ambiente, buscar activamente medidas de prevención de la contaminación y conservación de recursos.

21.4.6 El personal de **Tecnologías Eficientes de Villa** es responsable de reintroducir productos y materiales de fin de uso, extender su ciclo de vida y reciclar materiales para promover una economía circular.

21.4.7 El Director general es responsable de establecer la estrategia de sostenibilidad y que esta esté diseñada para comprender y satisfacer las expectativas de nuestros clientes, partes interesadas y la sociedad en general.

21.4.8 El personal de **Tecnologías Eficientes de Villa** es responsable de mantener relaciones estrechas con socios, comunidades, gobiernos, grupos industriales y otras partes, y

divulgamos activamente nuestros desempeños ambientales.

21.5 SOP-EDM-01-P16-02 Toma de conciencia para el cumplimiento con las leyes, normas, reglamentos y reglamentos aplicables en materia de medio ambiente, salud y seguridad.

21.5.1 La alta dirección es responsable de:

- Tomar las medidas adecuadas para proteger el medio ambiente y la salud y seguridad de los colaboradores, clientes, proveedores y vecinos de riesgos inaceptables.
- Tomar las medidas adecuadas para prevenir lesiones y enfermedades en el lugar de trabajo; proporcionar empleados con un ambiente de trabajo seguro y saludable.
- Realizar de manera proactiva la debida diligencia para identificar, evaluar y mitigar el medio ambiente, salud y seguridad antes de iniciar una nueva actividad o proyecto, diseño y adquisición de productos/servicios, y fusiones y adquisiciones.
- Adoptar las medidas apropiadas para eliminar los riesgos inaceptables de instalaciones, productos, servicios y procesos.

- Esforzarse por la mejora continua de su sistema de gestión ambiental a través de priorización, establecimiento de objetivos y metas, e implementación de procesos para conservar agua y otros recursos naturales, preservar la biodiversidad y prevenir la deforestación, eliminar el uso de materiales tóxicos y peligrosos, prevenir la contaminación y recuperar, reutilizar y reciclar productos y materiales.

- Esforzarse por mejorar continuamente su sistema de gestión de la seguridad establecer prioridades, establecer objetivos y metas, e implementar procesos y programas preventivos para reducir el riesgo de lesiones, enfermedades, muertes y pérdidas de activo.

- Ayudar a los empleados, clientes, proveedores y socios a reconocer los impactos de sus actividades de trabajo en materia de medio ambiente y su papel y responsabilidad en la lucha por para prácticas de trabajo más sostenibles.

- Exigir a los proveedores y contratistas que se adhieran a las normas aplicables en materia de medio ambiente, salud y leyes, normas, reglamentos y normas de seguridad de **Tecnologías Eficientes de Villa**.

- Tener una reunión al menos una vez al año para abordar temas relacionados con la Responsabilidad Social Corporativa de Tecnologías Eficientes de Villa.

- Liderar las evaluaciones de riesgos requeridas, involucrando a las Unidades Operativas

aplicables y expertos apropiados en la materia.

- Proporcionar fondos y recursos para garantizar que las instalaciones/lugares de trabajo de **Tecnologías Eficientes de Villa** cumplan con los requisitos con las leyes, normas, reglamentos aplicables en materia de medio ambiente, salud y seguridad, estándares y códigos reconocidos internacionalmente y los estándares de Tecnologías Eficientes de Villa.

21.6 SOP-EDM-01-P16-03 Responsabilidades de las áreas operativas en materia ambiental.

21.6.1 Es responsabilidad de todas las áreas:

- Comprender y cumplir con las leyes, normas y normas de medio ambiente, salud y seguridad, reglamentos, normas y códigos reconocidos internacionalmente y los estándares de Tecnologías Eficientes de Villa.que se aplican a sus área de Operaciones .
- Remediar los lugares de trabajo y los bienes raíces contaminados ambientalmente.
- Desarrollar y mantener un programa de preparación para emergencias.
- Esforzarse por mejorar continuamente su sistema de gestión de la seguridad y desarrollar/implementar programas preventivos para reducir el riesgo de lesiones, enfermedades, fatalidad, y pérdida de bienes.
- Esforzarse por la mejora continua de su sistema de gestión ambiental a través del establecimiento de objetivos y metas y la implementación de procesos para conservar el agua y otros recursos naturales, preservar la biodiversidad, eliminar el uso de materiales tóxicos y peligrosos, prevenir la contaminación y recuperar, reutilizar, y reciclar productos y materiales y gestionar la sostenibilidad ambiental.
- Mantener cualquier sistema de certificación ambiental y de seguridad de terceros, como ISO 14001 o ISO 45001.
- Informar a la alta dirección antes de interactuar o involucrar a las autoridades gubernamentales u organismos responsables del medio ambiente, la salud y/o la seguridad o cuando se contacte con ellos directamente por estas agencias.
- Desarrollar y/o adquirir Productos y Materiales que cumplan con las leyes aplicables, normas, reglamentos y estándares de Tecnologías Eficientes de Villa.
- Obtener la aprobación antes de finalizar la formulación de un material y un producto, diseño o adquisición.
- Asegurarse de que todos los Productos y Materiales se prueben y, cuando corresponda, se certifiquen o aprobado según las normas y reglamentos aplicables.
- Gestionar los aspectos medioambientales, de seguridad y salud de todos los productos y materiales a lo largo de su ciclo de vida.
- Notificar al Director de Operaciones ante un incidente relacionado con el producto;

- Mantener los estándares de medio ambiente, salud y seguridad que comprenden la modelo de negocio y reflejar los requisitos reglamentarios actuales y previstos, y proporcionar orientación a las Unidades Operativas para lograr el cumplimiento y las aprobaciones
- Realizar auditorías ambientales, de salud y seguridad.
- Gestionar la remediación de todos los sitios contaminados.
- Establecer límites de exposición para productos químicos y físicos.
- Proporcionar orientación sobre el apoyo adecuado a la salud y el bienestar en el trabajo servicios para Unidades Operativas.
- Validar que todos los productos y materiales estén probados y, en su caso, certificados o aprobado según las normas y reglamentos aplicables.

22.SOP-EDM-01-P17 Políticas y lineamentos anticorrupción

22.1 Objetivo

Establecer las medidas de control para dar cumplimiento de las leyes, las normas y los reglamentos aplicables en materia y lineamientos anticorrupción.

22.2 Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos, así como al personal de **Tecnologías Eficientes de Villa** en el ejercicio de sus funciones.

22.3 Responsabilidades

22.3.1 El personal de **Tecnologías Eficientes de Villa** es responsable de implementar y dar cumplimiento a la Política y lineamientos anticorrupción dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar cualquier omisión que se conozca sobre el cumplimiento de dicha política.

22.4 SOP-EDM-01-P17-01 De la corrupción

I. El Personal deberá evitar anteponer algún interés diverso al de Tecnologías Eficientes de Villa, y deberá evitar incurrir en Conflicto de Intereses y en Hechos de Corrupción. Asimismo, deberá rechazar cualquier solicitud u ofrecimiento que haga un Tercero, que se considere un Hecho de Corrupción.

II. Para efectos de las presentes Políticas y Lineamientos, los Hechos de Corrupción se pueden clasificar en los tipos de Corrupción:

a. Abuso del cargo: El Personal que con su conducta u omisión pretenda impedir la ejecución de una norma o el cumplimiento de una resolución de autoridad competente; quien retarde o niegue la ejecución de las funciones de su cargo; se apropie o disponga indebidamente de los bienes o valores bajo su cuidado; entregue u otorgue un servicio, cargo, comisión o contrato a sabiendas que no será ejecutado o sin tener facultades para ello, autorice o contrate a quien se encuentre inhabilitado, a sabiendas de esta situación; que otorgue una identificación o acreditación para desempeñar una función a quien realmente no lo desempeña o dilate injustificadamente poner a un detenido a disposición de la autoridad correspondiente.

b. Abuso de funciones: El Personal que ejerza funciones que no tenga conferidas o se valga de las que tenga, pararealizar o inducir actos u omisiones arbitrarios, para generar un beneficio para sí o para terceros o para causar perjuicio a alguna persona o a Tecnologías Eficientes de Villa.

c. Cohecho: El Personal que solicite, exija, acepte, ofrezca, obtenga o pretenda obtener, por sí o a través de terceros, cualquier beneficio no comprendido en su remuneración, con independencia de que consista en dinero; valores; bienes muebles o inmuebles, incluso mediante enajenación en precio notoriamente inferior al que se tenga en el mercado; donaciones; servicios; empleos y demás beneficios indebidos para sí o para sus parientes consanguíneos, civiles o para terceros con los que tenga relaciones profesionales, laborales o de negocios, o para socios o sociedades de las que los sujetos antes referidos formen parte.

d. Colusión: El Tercero que ejecute con uno o más sujetos, acciones que impliquen o tengan por objeto o efecto obtener un beneficio o ventaja indebidos de Tecnologías Eficientes de Villa.con motivo de un proceso de contratación. También se considerará colusión cuando los Terceros acuerden o celebren contratos, convenios, arreglos o combinaciones entre competidores, cuyo objeto o efecto sea obtener un beneficio indebido u ocasionar un daño o perjuicio al patrimonio de Tecnologías Eficientes de Villa.

e. Concusión: El Personal que exija, por sí o por medio de otro, dinero, valores, servicios o cualquiera otra cosa que sepa no ser debida, o en mayor cantidad que la señalada por las regulaciones aplicables.

f. Conflicto de intereses: La posible afectación del desempeño imparcial y objetivo de las funciones del Personal debido a intereses personales, familiares o de negocios. Se presenta cuando en las decisiones o acciones del Personal prevalece un interés distinto al de Tecnologías Eficientes de Villa.

g. Extorsión: El Personal que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro de su interés o causando a alguien un perjuicio patrimonial.

h. Fraude: El Personal que engañe a otro o a un Tercero o aprovechándose del error en que éste se

halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido de Tecnologías Eficientes de Villa.

i. Intimidación: El Personal que inhiba o intimide a cualquier persona para evitar que ésta o un tercero denuncie, formule querella, o aporte información relativa a la presunta comisión de una conducta sancionada por la normatividad interna o cualquier otra regulación; o realice una conducta ilícita u omita una lícita que lesione los intereses de las personas que las presenten o aporten, o de algún tercero con quien dichas personas guarden algún vínculo familiar, de negocios o afectivo.

j. Lavado de Dinero: proceso por el cual se borra el rastro ilícito de los bienes (tanto dinero en efectivo, como cualquier otro tipo de activos) que se han integrado en el sistema económico con una apariencia de legitimidad.

k. Peculado: El Personal que autorice, solicite o realice actos para el uso o apropiación para sí o para las personas con las que guarden algún vínculo familiar, de negocios o afectivo, recursos de Tecnologías Eficientes de Villa, sean materiales, humanos o financieros, sin fundamento jurídico o en contraposición a las normas aplicables.

l. Soborno: pagos o beneficios ilegales que se ofrecen o entregan a una persona con poder o influencia, con el fin de obtener un tratamiento preferencial, una decisión favorable o una ventaja indebida

m. Pago o recepción de remuneraciones indebidas o superiores a las autorizadas por la ley o norma que las prevea.

n. Tráfico de influencias: El personal que utilice su posición, cargo o empleo ante un servidor público para la tramitación o resolución ilícita de un asunto para el beneficio propio o de alguna otra persona de su interés.

o. Uso indebido o revelación de información privilegiada o sensible: El Personal que por sí o por interpósita persona, sustraiga, destruya, oculte, utilice, o inutilice ilícitamente información o documentación que se encuentre bajo su custodia o a la que tenga acceso, o de la que tenga conocimiento por su cargo.

así como también los definidos por las Leyes y Obligaciones Anticorrupción, que los prohíban o sancionen.

22.5 SOP-EDM-01-P17-02 Del soborno

22.5.1 En Tecnologías Eficientes de Villa, están prohibidos todos los Tipos de Soborno. El Soborno es un Hecho de Corrupción en el que incurre quien por sí mismo o a través de otro ofrezca, solicite, exija a través de su influencia real o supuesta, acepte, entregue, reciba, prometa o autorice un beneficio económico o de otro tipo, actual, futuro o en expectativa, que no se encuentre debidamente regulado o

autorizado por una norma, con la intención de:

a. Obtener un negocio o cargo, mantenerlo o conseguir una ventaja en el mismo;
b. Efectuar una presentación errónea u ocultación en los registros contables con respecto de Sobornos y otros actos indebidos;
c. Incentivar o recompensar un desempeño inapropiado en la actividad o función encomendada;
d. Evadir una regulación formal o implícita.
e. Inducir, modificar o inhibir la toma de decisiones relativa a un negocio, asociación o alianza;
f. Modificar el sentido de la resolución u opinión en algún asunto;
g. Ejercer el cargo o funciones conferidas de manera diversa a la legítimamente esperada;
h. Evadir, ocultar o manipular información para obtener u otorgar una ventaja o beneficio indebido;
i. Usar agentes externos, consultores y otros intermediarios en posibles esquemas de Soborno, y

22.5.1 El Personal, en cumplimiento a las Políticas Internas de Tecnologías Eficientes de Villa, en ninguna circunstancia deberá efectuar pago, regalo o promesa alguna a ningún funcionario o servidor público de alguna entidad gubernamental nacional o extranjera, o a Terceros, con el fin de que sus decisiones, acciones u omisiones beneficien a Tecnologías Eficientes de Villa.o al propio Personal.

22.6 SOP-EDM-01-P17-03 Manifiesto anticorrupción

22.6.1 El Personal manifestará de forma expresa, su rechazo absoluto a cualquier Hecho de Corrupción y su compromiso con el cumplimiento de las Leyes y Obligaciones Anticorrupción, las Políticas Internas Anticorrupción y las disposiciones jurídicas y administrativas que regulan sus funciones. Esta manifestación incluye la adhesión al Código de Ética y al Código de Conducta y el compromiso con el cumplimiento de las presentes Políticas y Lineamientos.

22.6.2 La manifestación podrá hacerse de la manera siguiente:

a) Al momento de la firma del Contrato de Trabajo, como parte integral de sus obligaciones, cuando éstosincluyan dicha manifestación;
b) Por escrito, mediante la suscripción del documento denominado Manifiesto Anticorrupción, sólo en el supuesto de que no se encuentre disponible la opción señalada en el contrato;
c) Tratándose de particulares que actúen en nombre y representación de Tecnologías Eficientes de Villa, deberán hacerlo por escrito mediante la suscripción del Manifiesto Anticorrupción y será integrado al expediente del contrato de representación o mandato.

22.6.3 El Manifiesto Anticorrupción a que se refiere la literal c anterior, será renovado bajo responsabilidad de quien lo suscribe al menos una vez cada cinco años.

22.6.3.1 El Manifiesto Anticorrupción original con firma autógrafa del Personal a que se refiere la literal a anterior, deberá conservarse por el área a cargo de los expedientes laborales del Personal que lo suscribe por el periodo descrito.

22.6.4 El Personal que ejerce funciones o actividades expuestas a un Riesgo de Corrupción deberá contar con la capacitación requerida en materia de Ética e Integridad Corporativa, así como en Anticorrupción

22.6.5 Tecnologías Eficientes de Villa, a través de medios electrónicos, aplicarán anualmente a los Terceros que interactúan con el Personal, una encuesta para conocer la percepción de Corrupción

22.7 SOP-EDM-01-P17-04 Identificación de Riesgos de Corrupción

22.7.1 Es responsabilidad del área legal la identificación de Riesgos de Corrupción de los Procesos Institucionales de las funciones y cargos potencialmente expuestos.

22.7.2 La Alta Dirección y el Personal puede estar expuesto a realizar Hechos de Corrupción en virtud del tipo de funciones o actividades que desempeñe, sin que ello necesariamente implique que vaya a incurrir en Hechos de Corrupción.

22.7.3 El área legal es responsable en el ámbito de su competencia de:

- Identificar dentro de su Proceso Institucional, las actividades que sean potencialmente expuestas o vulnerables al Riesgo de Corrupción, así como al Personal que las ejecuta;
- Evaluar los Riesgos de Corrupción, declararlos y llevar a cabo un inventario de éstos, manteniéndolo actualizado, y
- Establecer los controles internos necesarios para mitigar o eliminar los Riesgos de Corrupción, en términos de las Normas Internas de Administración de Riesgos.

22.7.4 Para llevar a cabo esta identificación, también podrán consultar si las funciones y/o actividades que se realizan, reúnen alguno o varios Factores de Riesgo de Corrupción.

22.7.5 El área legal establecerá los medios y periodicidades para la aplicación o en su caso, renovación de los Cuestionario de Autoevaluación para la Identificación y Prevención de Riesgos de Corrupción.

22.7.6 El personal que participe en los Procesos Institucionales será responsable de coadyuvar en la identificación de Riesgos de Corrupción, en cualquier actividad que desarrolle y se encuentre

expuesta a alguno o varios de los Factores de Riesgo de corrupción.

22.8 SOP-EDM-01-P17-05 Actividades relacionadas a las funciones estatutarias potencialmente expuestas o vulnerables a los Riesgos de Corrupción.

22.8.1 Para la identificación de funciones estatutarias y/o actividades potencialmente expuestas o vulnerables al Riesgo de Corrupción de cada Proceso Institucional, deberá considerarse el siguiente listado de actividades que, de manera enunciativa, más no limitativa, relaciona aquellas que por su naturaleza pudieran estar potencialmente expuestas o vulnerables al Riesgo de Corrupción para su identificación inicial, incluyendo el Alcance de las Actividades o funciones expuestas o vulnerables al Riesgo de Corrupción, mismas que deberán ser evaluadas conforme a los mecanismos establecidos normativamente por Tecnologías Eficientes de Villa:

1. Contratación de Terceros y administración de contratos;
2. Administración de bienes muebles e inmuebles;
3. Participación en los grupos de abastecimiento estratégico y de autorización de la excepción al concurso abierto;
4. Procedimientos contenciosos, de arbitraje y cualquier otro de resolución de controversias;
5. Gestión de pagos.
6. Procedimientos de comercialización de productos;
7. Control y administración de inventarios;
8. Definición, administración y operación de estrategias de transporte, almacenamiento y abastecimiento de hidrocarburos y sus productos derivados o subproductos;
9. Participación en esquemas de negocios, incluyendo los procedimientos de gestión, intervención o selección de acuerdos de negocios con socios, asociados, inversionistas, actuales o potenciales;
10. Selección y contratación de Personal;
11. Procedimientos de planeación, autorización, operación y/o supervisión de sistemas de seguridad, vigilancia, monitoreo y control de accesos y salidas de las instalaciones de productos, personas y bienes muebles;
12. Procedimientos relativos al registro y revelación de información financiera a partes interesadas;
13. Otorgamiento o revocación de franquicias, licencias de uso u otros derechos relacionados con las marcas propiedad de Tecnologías Eficientes de Villa;
14. Administración, operación, contratación, diseño, monitoreo o control de tecnologías de ciberseguridad;
15. Procedimientos deliberativos que otorguen, revoquen, restituyan o resuelvan sobre

peticiones, solicitudes, derechos, beneficios o afectaciones a particulares;

16. Procedimientos financieros de control, administración o acceso a bancos;
17. Trámite y gestión hasta la resolución de quejas y denuncias e inconformidades y auditorías, y
18. Aprobación de inversiones asociadas a la cadena de valor.

22.8.2 Los responsables deberán evaluar todos los alcances de las actividades relacionadas a las funciones estatutarias y/o actividades potencialmente expuestas o vulnerables a los Riesgos de Corrupción, y considerar si en el ámbito de su competencia intervienen en alguna de ellas con independencia del Proceso Institucional al que pertenezca.

22.9 SOP-EDM-01-P17-06 Riesgos de corrupción.

22.9.1 Los responsables de identificar que una actividad, cargo o función es vulnerable a Hechos de Corrupción, deberán considerar si éstas tienen alguno o varios factores que incidan en la materialización del Riesgo de Corrupción.

22.9.2 Algunos de estos factores de Riesgo de Corrupción:

- Acceso a información sensible.
- Autonomía / amplio margen en la discrecionalidad / unilateralidad en la toma de decisiones.
- Contacto con Terceros
- Área de Operaciones /registros/controles manuales
- Bajo nivel de implementación de la norma.
- Marco normativo deficiente
- Sobrerregulación.
- Supervisión deficiente.
- Insuficiencia en el aseguramiento de la base de datos.
- Respaldos de información no verificados, dañados o incompletos.
- Inexistencia de criterios para acceso a la información.
- Deficiente seguridad de información.
- Sistemas deficientes.

, los cuales son enunciativos más no limitativos y complementan a aquellas que en su caso se enuncien en las Normas Internas de Administración de Riesgos.

22.9.3 Para identificar Factores de Riesgo de Corrupción en los Procesos Institucionales, los

responsables deberán considerar:

a. Las recomendaciones que, en su caso, emitan los consejos de Tecnologías Eficientes de Villa.y/o el área de calidad ámbito de su competencia;
b. El resultado de verificaciones, auditorías o investigaciones practicadas por entes fiscalizadores o revisores;
c. La información que obre en sus registros que indique la existencia de antecedentes de Hechos de Corrupción detectados;
d. El resultado de investigaciones internas realizadas;
e. Las actividades expuestas al Riesgo de Corrupción previamente definidas, y
f. Las recomendaciones emitidas por la Gerencia de Recursos Humanos a través de sus áreas competentes.

22.9.4 Actualización del inventario de Riesgos de Corrupción y del Personal que ejerce las actividades o funciones expuestas al Riesgo de Corrupción en los Procesos Institucionales.

22.9.5 El inventario de Riesgos de Corrupción y el registro del Personal que desempeñe las funciones y cargos expuestos a Riesgos de Corrupción, deberá mantenerse vigente y actualizado por el Personal responsable y su contenido deberá actualizarse cuando:

a. Existan modificaciones estatutarias, de organización o de estructura.
b. El Personal identifique nuevos Riesgos de Corrupción no declarados previamente.
c. Se incluyan o modifiquen los Procesos Institucionales.
d. Se emitan recomendaciones por cualquier autoridad competente o bien, por el responsable legal de la organización.
e. Amerite dar de baja algún registro por causas justificadas.
f. Surjan situaciones en el entorno que impacten en las funciones o actividades, aun cuando éstas sean de carácter temporal.

g. El Personal que desarrolla las actividades en las que se identificaron los riesgos sea reemplazado por cualquier motivo.

Lo anterior de manera complementaria a lo dispuesto en las Normas Internas de Administración de Riesgos.

22.9.6 Así también, cada vez que el inventario de Riesgos de Corrupción sea modificado, deberá de ser enviado al responsable legal, para que pueda realizar las observaciones, comentarios y/o recomendaciones a los mismos.

22.10 SOP-EDM-01-P17-07 Relaciones con terceros

22.10.1 El Personal que intervenga en actividades y funciones en las que se interactúa con Terceros, deberá observar el cumplimiento de las Leyes y Obligaciones Anticorrupción y conducirse de conformidad con los principios y valores éticos establecidos en el Código de Ética y de manera transparente para el interés y beneficio de Tecnologías Eficientes de Villa; por lo que deberá aplicar en su contacto con Terceros, el contenido de la presente sección.

22.10.2 Los Terceros que interactúen con el Personal, deberán abstenerse de proponer o sugerir cualquier Hecho de Corrupción que se aparte del cumplimiento de las Leyes y Políticas Internas Anticorrupción de Tecnologías Eficientes de Villa.

22.10.3 Se considera que el Personal interviene e interactúa con Terceros, cuando participa en la atención, planeación, tramitación, resolución, otorgamiento, revisión, desarrollo, aprobación o autorización y ejecución de las actividades y funciones en las que mantiene contacto con personas físicas o morales ajenas a Tecnologías Eficientes de Villa. Entre ellas seconsiderarán al menos las reguladas en el lineamiento II.4.2, incluyendo el Alcance de las Actividades o funciones expuestas o vulnerables al Riesgo de Corrupción.

22.10.4 El Personal deberá dejar registro de la celebración de reuniones presenciales y visitas con Terceros.

22.10.5 El Personal deberá informar siempre a los Terceros, durante la reunión, que les asiste el derecho de formular un reporte, o presentar una queja o denuncia ante las instancias competentes, por el incumplimiento de las Leyes y Obligaciones Anticorrupción y las Políticas de Tecnologías Eficientes de Villa.que en su caso adviertan en el contacto con el Personal.

22.10.6 Tratándose de reuniones remotas efectuadas a través de medios electrónicos las mismas se celebrarán acorde a la normatividad y de igual forma se podrá realizar algún reporte, queja o denuncia en caso de que se amerite. Y compartirlo con la instancia correspondiente.
22.10.7 Se llevarán a cabo auditorías a proveedores de manera aleatoria sin alguna periodicidad para tener certeza del debido cumplimiento en temas de corrupción.

22.10.7 Todo proveedor que no cuente con controles antisoborno se les hará la invitación a gestionarlos dentro de su organización, en caso de no aplicarlos se les solicitará acatarse a nuestros controles y políticas anticorrupción.

22.11 SOP-EDM-01-P17-08 Conflicto de Interés

22.11.1 El Conflicto de Intereses es la posible afectación del desempeño imparcial y objetivo de las funciones del Personal debido a intereses personales, familiares o de negocios. Se presenta cuando en las decisiones o acciones del Personal prevalece un interés distinto al de Tecnologías Eficientes de Villa.

22.11.2 El Conflicto de Intereses debe ser informado por el Personal en cuanto tenga conocimiento o indicios de su existencia. La existencia de vínculos y relaciones que pudieran causar Conflicto de Intereses no constituye una irregularidad administrativa o delito por sí mismo, pero la omisión, negativa o falseamiento en su revelación por parte del Personal, así como la intervención o conocimiento en asuntos en los que debieron excusarse, pueden constituir delitos o Faltas administrativas o laborales, lo cual, en su caso, será informado a las autoridades correspondientes, para los efectos legales procedentes.

22.11.3 El Conflicto de Intereses puede ser Real, Potencial o Aparente y todos deben de ser declarados por el Personal, por escrito o de manera electrónica y solicitar instrucciones para solicitar su tratamiento o atención.

22.11.4 El Personal que requiera orientación para determinar si se encuentra ante un Conflicto de Intereses podrá determinarlo mediante el empleo de la “Guía para identificar posibles Conflictos de Intereses, o bien, formular la consulta correspondiente en la Línea Ética.

22.11.5 El Personal que se encuentre en una posible situación de Conflicto de Intereses deberá comunicarlo de inmediato a su superior jerárquico.

22.11.6 Los superiores jerárquicos que tomen conocimiento del Conflicto de Intereses del Personal a su cargo, deberán adoptar medidas preventivas, tales como:

a. Excluir al Personal en cuestión, del proceso, función o actividad, a menos que exista alguna causa justificada, debidamente motivada, que lo impida;

b. Hacer acompañar al Personal en Conflicto de Intereses con otras personas que no lo tengan y puedan atestiguar sobre la transparencia del desarrollo de la actividad o función. En este supuesto, el Personal designado deberá rendir un informe pormenorizado al superior jerárquico en el que se deje constancia de lo actuado, o

c. De no resultar posible ninguna de las opciones anteriores, dejar constancia fundada y motivada de los argumentos por los que, en su caso, se tomaron decisiones distintas sobre el asunto materia del Conflicto de Intereses.

22.11.7 En los casos anteriores, los superiores jerárquicos deberán dejar constancia de lo actuado y de las decisiones adoptadas en el expediente correspondiente del asunto que se trate. Esta constancia también podrá registrarse en los medios electrónicos que para tales efectos dispongan Tecnologías Eficientes de Villa.

22.11.8 Las constancias escritas de lo actuado deberán de conservarse como parte del expediente del asunto que se esté tratando.

22.11.9 El Personal que tome conocimiento de relaciones de Terceros con Personas Políticamente Expuestas, que pudiera constituir un Conflicto de Intereses Real, Potencial o Aparente, deberá informarlo a su superior jerárquico, a fin de que se adopten las medidas de prevención citadas en el lineamiento anterior.

22.12 SOP-EDM-01-P17-09 Debida diligencia

22.12.1 La información que se proporcione durante la Debida Diligencia será custodiada, controlada y proporcionada por las áreas y a través de los medios que se designen en la normatividad que para tales efectos se emita.

22.12.2 Tecnologías Eficientes de Villa.a través de las áreas que sean designadas en la normatividad específica, mantendrán vigentes los registros con la información actualizada y confiable de Terceros con los que mantenga o pretenda llevar a cabo Acuerdos comerciales, que resulte estrictamente necesaria para brindar confianza a sus inversionistas, socios y aliados comerciales.

22.12.2 Tecnologías Eficientes de Villa, atendiendo a la naturaleza y características del negocio, practicarán procesos de Debida Diligencia a Terceros, para lo cual solicitarán la información necesaria para conocer el riesgo implícito en Ética e Integridad Corporativa en términos de los lineamientos que la regulen, estableciendo, en

su caso, medidas de mitigación para la prevención de Riesgos de Corrupción.

22.12.4 Las áreas responsables de practicar la Debida Diligencia en Ética e Integridad Corporativa, tratándose de fusiones y adquisiciones accionarias, deberán poner especial énfasis en los antecedentes reputacionales del Tercero,sus accionistas, directivos y sus Beneficiarios Finales.

22.12.5 Tratándose de plazas del personal del área jurídica responsables de establecer las estrategias que permitan que la estructura organizacional cuente con Perfiles éticos, de manera conjunta con las áreas usuarias, a fin de prevenir y mitigar Riesgos de corrupción, deberán desarrollar e integrar la descripción del Perfil ético necesario entre los requerimientos a cumplirse para la ocupación de las plazas de confianza que deberán cubrir los candidatos para su contratación en las mismas, sin importar su carácter de transitorio o de planta, o si se trata de Personal adscrito o de nuevo ingreso.

22.12.6 En la Debida Diligencia de Perfiles éticos del candidato que aspire a incorporarse a la empresa se deberá verificar al menos lo siguiente:

- Que no haya sido sancionado por autoridad competente en México o el extranjero por Hechos de Corrupción, soborno, Lavado de Dinero, fraude o sus similares en el extranjero;
- Que declare sus Relaciones de los Terceros con Funcionarios y Servidores Públicos de gobiernos (Personas Políticamente Expuestas) aún y cuando no exista un posible Conflicto de Intereses;
- Que informe la existencia de demandas y/o denuncias interpuestas contra Tecnologías Eficientes de Villa;
- Que declare la existencia de posible Conflicto de Intereses, y
- Que declare que se ha separado legalmente de los activos e intereses económicos de Terceros que estén relacionados con la materia o afecten de manera directa el ejercicio de las funciones y responsabilidades que asumirá, y que signifiquen un Conflicto de Intereses o que lo hará previo a su contratación.

22.12.7 Respecto al tema de Función de cumplimento y órgano de gobierno sesionará de en la última semana del mes de junio y la segunda del mes diciembre.

22.13 SOP-EDM-01-P17-010 Regalos e invitaciones

22.13.1 El Personal deberá conducirse con rectitud sin utilizar su empleo, cargo o comisión para obtener o pretender obtener algún beneficio, provecho o ventaja personal o a favor de Terceros, ni buscar o aceptar compensaciones, prestaciones, dádivas, obsequios o regalos de cualquier persona u organización.

22.13.2 El Personal está obligado a dar a las personas en general el mismo trato, por lo que no concederán privilegios opreferencias a organizaciones o personas, ni permitirán que influencias, intereses o prejuicios indebidos afecten su compromiso para tomar decisiones o ejercer sus funciones de manera objetiva.

22.13.3 El Personal que exija, acepte, o realice cualquier acción para la obtención de un Regalo o Invitación en el ejercicio de su cargo, y el Tercero que lo ofrezca o entregue serán denunciados ante las autoridades

competentes.

22.13.4 En el caso de que se presente cualquier dilema ético respecto de Regalos o Invitaciones, el Personal podrá solicitar apoyo al área legal a fin de asegurarse que la decisión que adopte se apegue a los principios éticos de Tecnologías Eficientes de Villa.

22.13.5 En caso de que permanezcan dudas, el Personal como regla general, primero debe comentar el asunto con la persona que ocupe el nivel superior inmediato. Si eso no fuera posible, o si el superior no puede ayudarlo a resolver el tema, debe continuar buscando hasta encontrar una respuesta o solución. Para efectos de lo anterior, el Personal puede dirigirse con el siguiente nivel jerárquico en el escalafón o contactar a la Línea Ética para solicitar asesoría y orientación o denunciar Hechos de Corrupción.

22.13.6 El Personal que reciba de manera gratuita la transmisión de la propiedad o el ofrecimiento para el uso de cualquier bien, con motivo del ejercicio de sus funciones, deberá informarlo inmediatamente a su inmediato superior, en caso de transmisión de la propiedad de bienes, ponerlos a disposición de las autoridades competentes.

22.13.7 El Personal únicamente podrá aceptar invitaciones para asistir a eventos, entendiéndose como tales talleres, exposiciones, ferias, congresos, cursos, simposios, cocteles, presentaciones, o actividades similares, organizados y patrocinados por Terceros y que con la aceptación de la invitación no se configure un Conflicto de Intereses o se contravengan disposiciones jurídicas o administrativa, cuando resulte aplicable, además deberán concurrir las circunstancias siguientes:

a. Que exista una clara razón de negocios para Tecnologías Eficientes de Villa;
b. Que los gastos generados por concepto de transporte, hospedaje y otros gastos individuales sean cubiertos por Tecnologías Eficientes de Villa, y
c. Se cuente con la autorización previa y por escrito de un superior jerárquico.

22.13.8 El Personal deberá solicitar la autorización para la asistencia a los eventos motivo de las invitaciones que reciba a que se refiere el lineamiento anterior, mediante correo electrónico o escrito libre al superior jerárquico o en su defecto al jefe del superior jerárquico, que al menos contenga: El nombre, ficha o número de empleado, fecha de evento, nombre de la organización que lo patrocina, nombre del contacto de dicha organización, motivo del evento, duración aproximada del mismo, beneficios que obtendrá Tecnologías Eficientes de Villa.con la asistencia, así como la manifestación expresa de no encontrarse bajo un Conflicto de Intereses en caso de asistir al evento.

22.13.9 Quedan exceptuados de este lineamiento:

i) el Personal designado para acudir a eventos corporativos en representación de Tecnologías Eficientes de Villa, y
ii) ii) el Personal que haya sido designado a desempeñar funciones o ejecutar parte de

las actividades previstas en cumplimiento de un Acuerdo comercial celebrado entre Tecnologías Eficientes de Villa con Terceros.

22.14 SOP-EDM-01-P17-011 Prevención de lavado de dinero

22.14.1 En términos de las Normas Internas, en el ámbito de su competencia, los responsables de los Procesos Institucionales, identificarán las área de Operaciones que realizan en las que se lleven a cabo Actividades Vulnerables y determinarán los requisitos necesarios para tener una certeza razonable de la procedenciay destino de los recursos, valores, acuerdos, alianzas y negocios en general.

22.14.2 Para determinar las Actividades Vulnerables, los responsables deberán de tomar en consideración la existencia de antecedentes en los que se hayan presentado situaciones de indicios de riesgo de Lavado de Dinero

22.14.3 Tecnologías Eficientes de Villa llevarán a cabo la identificación de los Terceros a efecto de otorgar mayor seguridad a sus áreas de operaciones y prevenir riesgos de operación, legales o reputacionales a los que pudieran estar expuestos.

22.14.4 La información y documentación que deberá ser proporcionada por los Terceros dependerá de su propia naturaleza. Es decir, la información y documentación que deberá entregar el Tercero será diferente dependiendo del tipo de Tercero y de su nacionalidad. Sin embargo, en los procedimientos de identificación, a manera de control preventivo,en todo caso se establecerán datos obligatorios para todos los Terceros, tales como: el nombre, profesión, domicilio,identificaciones personales con fotografía y firma, estatus migratorio (tratándose de extranjeros), así como identificación de los representantes legales. Estos datos deberán ser revelados a Tecnologías Eficientes de Villa.en los formularios respectivos durante el desarrollo de la Debida Diligencia en términos de la normatividad que la regule.

22.15 SOP-EDM-01-P17-012 Regulación y reporte de actividades sospechosas

22.15.1 Tecnologías Eficientes de Villa, en su esfuerzo por detectar y prevenir la realización de área de Operaciones con recursos de procedencia ilícita, combatir el mercado ilícito de combustibles, afectaciones a su patrimonio y el financiamiento al terrorismo, ejecutan Acciones Antilavado, mediante la identificación de las Actividades

Vulnerables, por lo que no celebrarán Acuerdos comerciales con Terceros cuyos recursos sean de procedencia o cuyo destino sea para fines ilícitos.

22.15.2 En caso de detectarse algún Acuerdo comercial que incluya recursos de procedencia ilícita o para cuya obtención se hayan contravenido las Leyes Antilavado, se procederá a analizar con las áreas competentes, la conveniencia de rescindir la relación comercial y se llevarán a cabo las actividades necesarias para investigar y denunciar las conductas y omisiones descritas en la presente sección ante las autoridades competentes.

22.15.3 Tecnologías Eficientes de Villa establecerán y mantendrán un marco normativo para que los Procesos Institucionales que celebren Acuerdos comerciales prevengan el Lavado de Dinero. Esta regulación también establecerá los controles operacionales, mecanismos de reporte y atención de los asuntos en los que existan indicios de Lavado de Dinero, así como los medios de remisión a las autoridades cuando resulte procedente, seguimiento e informes que se generen al respecto y su forma de conservación.

22.15.4 Tecnologías Eficientes de Villa atenderán los reportes del área de Operaciones sospechosas que involucren Actividades Vulnerables de los Terceros, que realice el Personal responsable de los Procesos Institucionales, que celebren Acuerdos comerciales, a través del área legal que dará seguimiento a los asuntos y determinará las medidas preventivas que deberán adoptarse para prevenir la materialización de Riesgos de Corrupción, operacionales, reputacionales o legales. Este grupo también será responsable del seguimiento de los asuntos hasta su conclusión.

22.15.5 Tecnologías Eficientes de Villa podrán celebrar Acuerdos de colaboración con autoridades fiscales o financieras, nacionales oextranjeras, para llevar a cabo intercambio de información que fortalezca la prevención de Lavado de Dinero, el combate al mercado ilícito de combustibles y la prevención del financiamiento al terrorismo.

22.16 SOP-EDM-01-P17-013 Alteración de libros y/o registros

22.16.1 El Personal o Terceros no realizarán hechos irregulares o ilícitos que impliquen la alteración de libros o que impacten en los estados financieros de Tecnologías Eficientes de Villa. Tecnologías Eficientes de Villa no tolerarán estas conductas.

22.16.2 Tecnologías Eficientes de Villa, se obligan a dar cumplimiento, con el objetivo de fortalecer la responsabilidad corporativa, combatir el fraude corporativo y contable, así como certificar que la información financiera es confiable, por lo cual exige el establecimiento y mantenimiento de

una adecuada implementación del sistema de control interno, así como una evaluación de la efectividad de los controles.

22.16.3 El Personal o Terceros cometerá una alteración de libros y registros, cuando con su actuación u omisión se propicie lo siguiente:

1. Una declaración o registro falso, omiso o alterado que implique sobreestimar activos o subestimar pasivos que impacte en los reportes financieros;
2. La distorsión o falseamiento del registro o documento que sustente las área de Operaciones y/o la información financiera, o
3. Cualquier acto intencional llevado a cabo, con la finalidad de sustraer activos u ocultar obligaciones que tienen o puedan tener un impacto en los estados financieros.

22.16.4 El Personal es responsable de proveer información operacional y financiera precisa en la que no se omita información que impacte en los libros o registros financieros.

22.16.5 En términos de las Normas los titulares de las áreas de Tecnologías Eficientes de Villa, identificarán la exposición que tienen para la ocurrencia de la alteración de libros o registros a fin de establecer las medidas de control que se consideren convenientes para prevenir los riesgos. En todo caso tomarán en cuenta si el Personal que realiza las actividades encomendadas presenta alguna de las características siguientes:

a. Existencia de un incentivo para obtener un beneficio directo o indirecto.
b. Apremio por cumplir alguna meta.
c. Intención de ocultar otro ilícito o irregularidad.
d. Oportunidad de cometerlo por deficientes o inexistentes controles internos.
e. Inadecuada supervisión de las actividades.
f. Concentración de funciones.

22.17 SOP-EDM-01-P17-014 Tratamiento de donativos y donaciones

22.17.1 Tecnologías Eficientes de Villa prohíben el otorgamiento de donativos o donaciones en dinero o especie, incluyendo bienes, servicios, valores u otros recursos, a cualquier persona física o moral.

22.17.2 El Personal que tenga conocimiento de la asignación de bienes o recursos en dinero o especie, que se hayan otorgado o se vayan a otorgar a personas físicas o morales como donativo o donación, que no hayan sido tratados de acuerdo con la regulación en la materia, deberá de informarlo a sus superiores o reportarlo a través de la Línea Ética

22.18 SOP-EDM-01-P17-015 No represalias

22.18.1 Tecnologías Eficientes de Villa, conforme al Código de Ética tienen una política de No Represalias. No son toleradas las represalias directas o indirectas contra el Personal o Terceros que hayan presentado de buena fe un reporte o facilitado información a los responsables de la investigación de posibles Hechos de Corrupción.

22.18.2 Tecnologías Eficientes de Villa garantizarán la continuidad laboral o contractual de quien reporte, cuando con motivo de la información que aporte se pretenda su separación o terminación contractual. El Personal que tome represalias será objeto de medidas disciplinarias.

22.18.3 Tecnologías Eficientes de Villa protegerán al Personal y Terceros que denuncien un Hecho de Corrupción emitiendo, en su caso, las medidas cautelares suficientes para proteger la identidad e integridad de los informantes que soliciten el resguardo de su anonimato.

22.18.4 Tecnologías Eficientes de Villa designa el correo gobierno@tecnologiaseficientesdevilla.com , para tratar todo tipo de denuncia, el área de Recursos Humanos será la encargada de administrar dicho correo y informar al área legal para la investigación correspondiente.

22.18.5 El área legal es responsable para investigar los Hechos de Corrupción, en la imposición de medidas disciplinarias cuando existan, podrán considerar las atenuantes y/o excluyentes siguientes:

Atenuantes

- Si de manera espontánea el infractor, sin existencia previa de denuncia o investigación de cualquier autoridad que tenga competencia en materia de Anticorrupción, confiesa ante la instancia competente los hechos constitutivos de infracción, siempre y cuando no exista afectación económica o, en su defecto, la haya restituido, o
- Habiendo participado de manera colectiva en una infracción a las presentes Políticas y Lineamientos, sin existencia previa de denuncia o investigación de cualquier autoridad que tenga competencia en materia de Anticorrupción, denuncie al resto de los infractores y colabore en el desarrollo de la investigación con cualquier instancia que lo requiera.

Excluyente

- Cuando el Personal haya actuado en situación de extrema gravedad, o en la prevención de daños irreparablesa las personas, siempre que existan las denuncias ante la Fiscalía General de la República o su similar en el extranjero, y así se acredite.

22.18.5 El área legal, en su ámbito de competencia, procurarán la conformación de instancias internas o grupos de trabajo especializados para la adecuada atención de los reportes de Hechos de Corrupción, incluyendo el Lavado de Dinero y la alteración de libros o registros presentados para, de ser el caso, su posterior remisión a las autoridades competentes.

22.18.6 Con independencia de las sanciones que pudieran ser impuestas por autoridades competentes que conozcan de los Hechos de Corrupción, Lavado de Dinero y fraude corporativo, Tecnologías Eficientes de Villa podrán imponer medidas disciplinarias en el marco de su competencia conforme a los Estatutos Orgánicos, mediante los procedimientos internos que tengan instaurados.

22.18.7 Tecnologías Eficientes de Villa conforme a sus facultades estatutarias a través del área legal en coadyuvancia con las áreas competentes, investigarán los hechos reportados y darán parte de Recursos Humanos para la aplicación de las medidas disciplinarias a que haya lugar, las cuales podrán incluir la rescisión laboral. Adicionalmente se dará vista a las autoridades facultadas de conocer aquellas conductas que pudieran ser constitutivas de un Hecho de Corrupción.

22.18.8 Las instancias competentes para aplicar medidas disciplinarias en Tecnologías Eficientes de Villa podrán tomar en cuenta lasatenuantes y excluyentes incluidas en los resultados de la investigación.

23 SOP-EDM-01-P18 Políticas en materia de derechos humanos, igualdad de género y no discriminación.

23.1 Objetivo

Establecer las directrices internas para garantizar el cumplimiento de la legislación nacional vigente y principios internacionales en materia de derechos humanos, igualdad de género y no discriminación.

23.2 Alcance

Aplica en todos los ámbitos de **Tecnologías Eficientes de Villa**; el personal en el ejercicio de sus funciones, sus recursos, información, sus procesos internos o externos vinculados a través de instrumentos jurídicos de **Tecnologías Eficientes de Villa.**

23.3 Responsabilidades

El Comité de Igualdad y no discriminación de **Tecnologías Eficientes de Villa** es responsable de implementar, evaluar y dar cumplimiento a la Política de materia de derechos humanos, igualdad de género y no discriminación así como comunicar a todo el personal de no realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones, así como notificar a la Defensora de Derechos humanos e igualdad laboral así como al Comité de Igualdad cualquier omisión que se conozca sobre el cumplimiento de dicha política.

23.4 SOP-EDM-01-P18-01 Política de igualdad de oportunidades

Esta Política de Igualdad Laboral y No Discriminación se armoniza con la Constitución Política de los Estados Unidos Mexicanos, en particular con lo establecido en la fracción III del artículo 1º, comprometiéndose la organización a promover, respetar, proteger y garantizar los derechos humanos en el ámbito laboral, bajo los principios de universalidad, interdependencia, indivisibilidad y progresividad.

La organización garantiza el acceso equitativo a oportunidades de empleo, desarrollo profesional y condiciones laborales para todas las personas, sin distinción de sexo, género, edad, orientación sexual, estado civil, origen étnico, discapacidad u otra condición. Se prohíben expresamente prácticas de discriminación directa o indirecta.

a) El área de Recursos Humanos es la responsable de realizar los procesos de reclutamiento y promoción con igualdad de condiciones y sin sesgos de género o de cualquier otra índole.
b) El personal mantendrá una cultura organizacional basada en el respeto a la diversidad y al reconocimiento del talento sin distinción.
c) La alta dirección es el responsable de eliminar barreras estructurales que impidan el acceso igualitario a posiciones de liderazgo, dirección o toma de decisiones.
d) El área de Recursos Humanos es el responsable de mantener el acceso igualitario a la capacitación, formación profesional y programas de desarrollo del talento.
e) Las evaluaciones de desempeño se realizarán bajo criterios objetivos, con

perspectiva de equidad y enfoque de competencias.

23.5 SOP- EDM-01-P18-02 Política de inclusión y no discriminación

a) **Cero tolerancia a la discriminación y acoso**

- Se prohíben expresamente todo acto de acoso laboral, acoso sexual, maltrato, violencia, segregación, violencia de género y cualquier forma de discriminación en materia de: apariencia física, cultura, discapacidad, idioma, sexo, género, edad, condición social/económica/de salud o jurídica, embarazo, estado civil o conyugal, religión, opiniones, origen étnico o nacional, preferencias sexuales y situación migratoria.
- Se aplicarán sanciones conforme a los protocolos internos y leyes aplicables.

b) **Entorno laboral respetuoso**

- Se fomentará el respeto mutuo, la equidad y la inclusión como principios esenciales de convivencia laboral.

c) **Denuncia y atención de quejas**

- Toda persona podrá denunciar de forma segura y confidencial cualquier acto discriminatorio, sin temor a represalias.

23.6 Política de Reclutamiento y Selección Igualitario

a) **Igualdad de acceso al empleo**

- Ningún proceso de reclutamiento podrá restringirse por edad, género, estado civil, discapacidad, orientación sexual, religión, origen étnico, etc.

b) **Vacantes inclusivas**

- Las convocatorias y descripciones de puestos deberán utilizar lenguaje no sexista y promover activamente la inclusión.

c) **Entrevistas sin sesgos**

- Se capacitará al personal de reclutamiento para identificar y evitar sesgos conscientes e inconscientes.

23.7 Política de Conciliación Vida-Personal-Laboral

La organización promoverá medidas de conciliación entre la vida laboral, familiar y personal, incluyendo horarios flexibles, licencias y otras prácticas que favorezcan el equilibrio de las responsabilidades, fomentando la corresponsabilidad.

a) **Flexibilidad de horarios**

- Se fomentarán jornadas laborales flexibles y modalidades como el teletrabajo cuando las funciones lo permitan.

b) **Licencias equitativas**

- Se otorgarán permisos de maternidad, paternidad, cuidados familiares, lactancia y emergencias personales conforme a la ley y con perspectiva de género.

c) **No discriminación por responsabilidades familiares**

- Se prohíbe cualquier trato desigual hacia personas que ejercen roles de cuidado.

23.7 Política de Conciliación Vida-Personal-Laboral

Todo el personal recibirá capacitación periódica sobre igualdad de género, no discriminación, derechos humanos y prevención del acoso, como parte del fortalecimiento de la cultura organizacional en igualdad.

a) **Capacitación obligatoria y periódica**

- Todo el personal deberá recibir formación continua en temas de igualdad de género, derechos humanos, acoso y diversidad.

b) **Sensibilización de mandos medios y altos**

- Las personas en puestos directivos recibirán formación específica sobre liderazgo inclusivo y prevención de violencia.

c) **Evaluación de impacto**

- Se medirán los resultados de las capacitaciones para evaluar cambios en prácticas y actitudes.

23.8 Política de Igualdad Salarial

La organización se compromete a garantizar la igualdad de remuneración por trabajo de igual valor, independientemente del sexo u otras condiciones personales. Se revisarán periódicamente las estructuras salariales para eliminar posibles brechas salariales de género.

a) **Auditoría salarial periódica**

- Se realizarán diagnósticos para identificar posibles brechas salariales por género y aplicar medidas correctivas.

b) **Criterios objetivos de remuneración**

- El salario se definirá con base en el puesto, responsabilidades, competencias y desempeño, nunca por factores personales.

c) **Transparencia en compensaciones**

- Se promoverá la claridad en los criterios de pago y ascensos para fomentar la confianza y equidad interna.

23.8 Política de Igualdad Salarial

El Comité de Igualdad Laboral y No Discriminación, responsable de promover, coordinar y supervisar la implementación efectiva de estas políticas, así como proponer medidas de mejora.

a) **Integración plural**

- El Comité estará integrado por representantes de distintas áreas y niveles jerárquicos, incluyendo paridad de género.

b) **Funciones del Comité de Igualdad**

I. **Diseñar e implementar el Plan de Igualdad Laboral y No Discriminación**

- Proponer y ejecutar acciones, metas e indicadores para promover la igualdad en el centro de trabajo.
- Asegurar que el plan esté alineado con las políticas institucionales y normas vigentes.

II. **Diagnosticar y evaluar condiciones de igualdad**

- Realizar diagnósticos internos de manera anual para identificar brechas de género, discriminación o desigualdad.
- Analizar estadísticas desagregadas por sexo y otros factores relevantes.

III. **Supervisar el cumplimiento de políticas institucionales**

- Vigilar que se apliquen correctamente las políticas de inclusión, igualdad salarial, conciliación vida-trabajo, entre otras.

IV. **Atender y dar seguimiento a quejas o denuncias por discriminación**

- Recibir, canalizar, dar seguimiento y resolver de manera confidencial e imparcial las quejas relacionadas con discriminación, acoso, hostigamiento o trato desigual.
- Coordinar con el área jurídica o de recursos humanos para la aplicación de sanciones cuando corresponda.

V. **Promover la participación igualitaria**

- Impulsar mecanismos que aseguren la participación activa y equitativa de mujeres, personas con discapacidad y grupos vulnerables en todos los niveles jerárquicos.

VI. **Capacitar y sensibilizar**

- Coordinar o gestionar la formación continua en temas de género, igualdad, diversidad, derechos humanos y prevención del acoso para todo el personal.

VII. **Impulsar acciones afirmativas**

- Diseñar y proponer medidas especiales para corregir desequilibrios estructurales (por ejemplo, establecer metas de representación femenina en puestos de liderazgo o contratación de personas con discapacidad).

VIII. **Revisar procesos organizacionales con perspectiva de igualdad**

- Evaluar y hacer recomendaciones para que procesos como reclutamiento, ascensos, compensaciones o despidos sean objetivos y libres de sesgos.

IX. **Elaborar informes de seguimiento**

- Presentar reportes trimestrales o anuales sobre el cumplimiento de acciones, indicadores y avances en igualdad laboral.

X. **Actualizar protocolos internos**

- Revisar y actualizar periódicamente los protocolos de atención a la violencia laboral, acoso y discriminación, asegurando que estén alineados con cambios normativos o buenas prácticas.

XI. **Fomentar la cultura organizacional incluyente**

- Promover campañas de comunicación interna para visibilizar la importancia de la igualdad, la diversidad y el respeto.

XII. **Acompañar auditorías o procesos de certificación**

- Coordinar y documentar los procesos requeridos para la certificación o mantenimiento de la Norma Mexicana NMX-R-025-SCFI-2015 u otras similares.

XIII. **Garantizar la confidencialidad y protección de las personas denunciantes**

- Velar por que ningún integrante del personal sufra represalias por presentar una queja o colaborar en un procedimiento.

c) **Sesiones y reportes**

- Se reunirá de forma regular (mínimo cada trimestre) y presentará informes de avances y propuestas a la alta dirección.

23.9 Compromiso de la Alta Dirección

La Alta Dirección se compromete formalmente a cumplir, promover y hacer cumplir esta Política de Igualdad Laboral y No Discriminación, y a garantizar los recursos necesarios para su aplicación efectiva. Esta política será difundida, revisada de manera anual y actualizada en función de las necesidades institucionales y el marco normativo vigente.

Revisado el 02 de febrero de 2025.

Firmas:

Presidente  **Manuel de Jesús González Arredondo**	Secretario  **Ivette Jacqueline López Cortes**
Vocal  Andrea Ramírez Méndez	Vocal  **Mario Emilio Carrillo Gallegos**
	Vocal  **Carmen Araceli Villavicencio Sandoval**