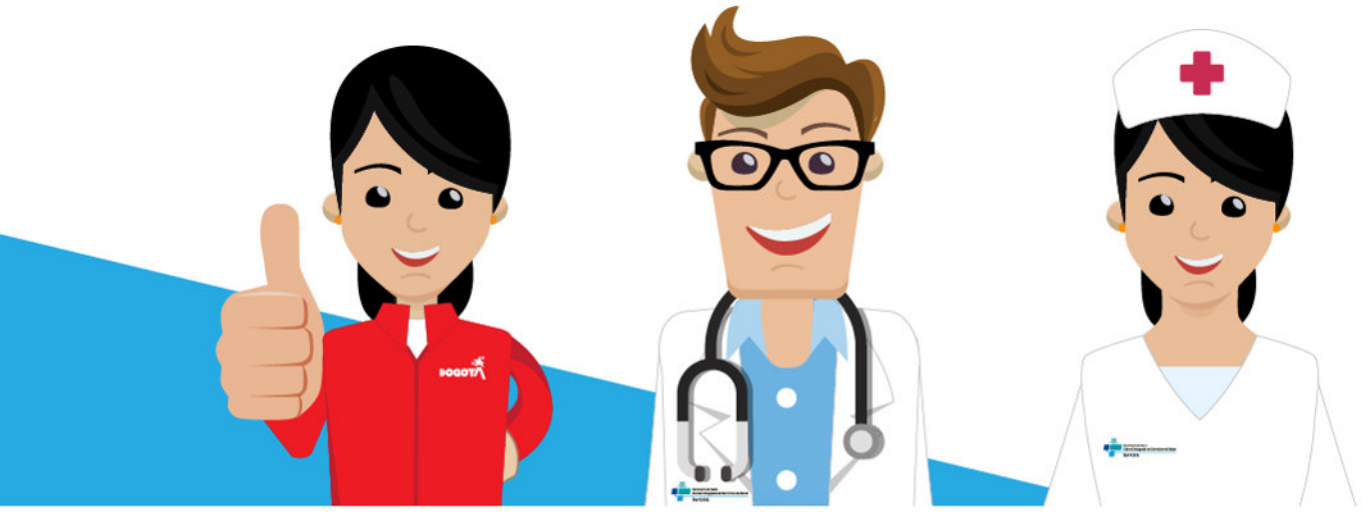
SUBRED INTEGRADA DE SERVICIOS DE SALUD SUR E.S.E

PLAN

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GI-TIC-PL-02 V10



Secretaría de Salud
Subred Integrada de Servicios de Salud
Sur E.S.E.

BOGOTÁ

Tabla de Contenido

1. INTRODUCCIÓN:

En la Subred integra de servicios de salud sur ese la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, la Subred Sur ESE implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los colaboradores, contratistas, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Subred Sur ESE, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La política general de seguridad de la información de la Subred Sur ESE se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la Subred Sur ESE. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del anexo A de la norma internacional ISO 27001:2022.

La política general de seguridad de la información en su enunciado reza: “La Subred Sur ESE se compromete a mantener la confidencialidad, integridad y disponibilidad de la información a través de la identificación y mitigación de los riesgos a los cuales está expuesta con el objeto de asegurar la misma y propender por el establecimiento de una cultura de seguridad informática”.

El Comité de seguridad de la información – CSI – tendrá la potestad de modificar la política general o las políticas específicas de seguridad de la información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad.

2. OBJETIVO:

El presente documento tiene como objetivo establecer las directrices en materia de seguridad de la información para la Subred Sur ESE, con el fin de regular, actualizar e implementar la gestión de la seguridad de la información dentro de la entidad.

3. ALCANCE:

Las directrices de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, colaboradores, contratistas y terceros que laboren o tengan relación con la Subred Sur ESE, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada. Este Plan de seguridad y privacidad de la información es elaborado de acuerdo con el análisis de riesgos y de vulnerabilidades en las dependencias de la Subred Sur ESE, por consiguiente, el alcance de estas políticas se encuentra sujeto a la Subred Sur ESE.

DESDE: Todos los directivos, funcionarios, contratistas, terceros y otros colaboradores de la Subred Sur ESE, incluyendo a todo el personal externo que cuenten con un equipo conectado a la red

HASTA: Todos los equipos propios y arrendados y servicios que de alguna manera tengan que utilizar local o remotamente el uso de la red o recursos tecnológicos de la Subred Sur ESE, así

como de los servicios e intercambio de archivos y programas.

4. DEFINICIONES:

ACCESO REMOTO: posibilidad de realizar ciertas tareas en una computadora (ordenador) sin estar físicamente en contacto con el equipo**.**

ACTIVO DE INFORMACIÓN: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Subred Sur ESE y, en consecuencia, debe ser protegido.

ACUERDO DE CONFIDENCIALIDAD: Es un documento en los que los colaboradores y contratistas de la Subred Sur ESE o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Subred Sur ESE, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

ATI - ADMINISTRADORES DE TECNOLOGÍAS DE INFORMACIÓN: Responsables de la administración de los equipos de cómputo, sistemas de información y redes de la Subred Sur ESE. Velan por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CAPACITY PLANNING: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

CENTROS DE CABLEADO: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

CENTRO DE CÓMPUTO: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

CIFRADO: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizad a los repositorios de información.

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

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido

CRIPTOGRAFÍA: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

CUSTODIO DEL ACTIVO DE INFORMACIÓN: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

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

DERECHOS DE AUTOR: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

DISPONIBILIDAD: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

DISPOSITIVOS IOT: consiste en un objeto al que se le ha dotado de conexión a Internet y cierta inteligencia software, sobre el que se pueden medir parámetros físicos o actuar remotamente y que por tanto permite generar un ecosistema de servicios alrededor del mismo.

EQUIPO DE CÓMPUTO: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

GUÍAS DE CLASIFICACIÓN DE LA INFORMACIÓN: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

HACKING ÉTICO: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

IDENTIFICACIÓN DEL RIESGO: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Subred Sur, que ponen en riesgo la Confidencialidad, Integridad y Disponibilidad de los Activos de Información, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

INCIDENTE DE SEGURIDAD: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

INGENIERÍA SOCIAL: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

INTEGRIDAD: Es la protección de la exactitud y estado completo de los activos.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: Es una lista ordenada y documentada de los activos de información pertenecientes a la Subred Sur ESE.

LICENCIA DE SOFTWARE: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MEDIO REMOVIBLE: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, cds, dvds y unidades de almacenamiento USB, entre otras.

PERFILES DE USUARIO: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/lec 27002:20005): intención y dirección general expresada formalmente por la Dirección.

PROPIEDAD INTELECTUAL: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

PROPIETARIO DE LA INFORMACIÓN: Es la unidad organizacional o proceso donde se crean los activos de información.

RECURSOS TECNOLÓGICOS: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de La Subred Sur ESE.

REGISTROS DE AUDITORÍA: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de La Subred Sur ESE. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

RESPONSABLE POR EL ACTIVO DE INFORMACIÓN: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

SGSI SEGÚN [ISO/LEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por La Subred Sur ESE o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SISTEMAS DE CONTROL AMBIENTAL: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

SOFTWARE MALICIOSO: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

TERCEROS: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

TRABAJO EN CASA: trabajo que se realiza en un lugar alejado de las oficinas centrales, de las instalaciones de producción o del cliente que lo contrata, mediante la utilización de las nuevas tecnologías de la información y la comunicación.

USUARIO: En el presente documento se emplea para referirse a directivos, colaboradores, contratistas, terceros y otros colaboradores de la Subred Sur ESE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Subred Sur ESE y a quienes se les otorga un nombre de usuario y una clave de acceso.

VULNERABILIDADES: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por La Subred Sur ESE (amenazas), las cuales se constituyen en fuentes de riesgo.

5. NORMATIVIDAD APLICABLE:

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Ley Estatutaria 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	Congreso de la Republica
Ley 1273	2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras Disposiciones.	Presidencia de la Republica
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.	Congreso de Colombia
Ley 1915	2018	Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.	Congreso de Colombia
Ley 1928	2019	Define nuevas reglas sobre el uso de información biométrica en Colombia y el almacenamiento seguro de datos sensibles.	Congreso de Colombia

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Ley de Protección de Datos de Salud (HIPAA - Estados Unidos)	Actualización 2021	Reglamentación que establece la seguridad y privacidad en el manejo de información de salud en sistemas electrónicos. Aplicable a empresas que manejen datos de salud internacionales.	Departamento de Salud y Servicios Humanos de EE.UU.
Ley 2300	2023	Regula el uso responsable de datos personales y establece nuevas reglas para el tratamiento de datos en Colombia, ampliando la Ley 1581 de 2012.	Congreso de Colombia
Decreto 1151	2008	Establecen los lineamientos generales de la estrategia de gobierno en línea de la república de Colombia, se reglamenta parcialmente la Ley 962 de 2005. Manual de implementación de la estrategia de gobierno en línea	Presidencia de la Republica
Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.	Ministro del Interior y de Justicia de la República de Colombia
Decreto 1377	2013	Reglamenta parcialmente la Ley 1581 de 2012 y establece los procedimientos para garantizar el derecho a la protección de datos personales. Este decreto es particularmente relevante para las entidades del sector salud que manejen información sensible.	Presidencia de la Republica
Decreto 1078	2015	Por medio del cual se expide el decreto único reglamentario del sector de tecnologías de la información y las comunicaciones	Presidencia de la Republica
Decreto 767	2022	Actualización del marco regulatorio para la seguridad digital en Colombia, promoviendo la adopción de estándares internacionales.	Presidencia de la República de Colombia
Resolución 1995	1999	Establece las normas técnicas y administrativas para el manejo de información en salud y define los principios y obligaciones para la protección de la confidencialidad de la información en el sector salud.	Ministerio de Salud
Directiva 005	2005	Por medio de la cual se adoptan las políticas generales de tecnología de información y comunicaciones aplicables al distrito capital.	Alcaldía Mayor de Bogotá, D.C.
ISO/IEC 27001	2013	Describe cómo gestionar la seguridad de la información en una empresa	Organización Internacional de Normalización (ISO)
ISO/IEC 27002	2013	Controles para seguridad de la información	Organización Internacional de Normalización (ISO)
ISO/IEC 27017	2015	Controles específicos para la seguridad en la computación en la nube, aplicables tanto a proveedores como a clientes.	Organización Internacional de Normalización (ISO)
ISO/IEC 27004	2016	Métricas Para la Medición de la Gestión de Seguridad de la Información.	Organización Internacional de Normalización (ISO)
ISO/IEC 27035	2016	Normativa que define las mejores prácticas para la gestión de incidentes de seguridad de la información.	Organización Internacional de Normalización (ISO)

NORMA	AÑO	DESCRIPCIÓN	EMITIDA POR
Reglamento General de Protección de Datos (GDPR - Europa)	2018	Marco regulador para la protección de datos personales en la Unión Europea, con impacto en organizaciones internacionales que manejan datos de ciudadanos europeos.	Parlamento Europeo y Consejo de la UE
ISO/IEC 27018	2019	Estándar para la protección de datos personales en entornos de computación en la nube.	Organización Internacional de Normalización (ISO)
ISO/IEC 27701	2019	Extensión de ISO/IEC 27001 para la gestión de la privacidad de la información y cumplimiento con regulaciones como la GDPR.	Organización Internacional de Normalización (ISO)
CONPES 3995	2020	Política nacional de confianza y seguridad digital.	Consejo Nacional de Política Económica y Social
Directiva NIST 800-207	2020	Establece los principios de Zero Trust Security, un modelo de ciberseguridad basado en verificación constante de identidad y permisos.	Instituto Nacional de Estándares y Tecnología (NIST, EE.UU.)
ISO/IEC 27001	2022	Nueva versión de la norma internacional que establece un marco para la gestión de seguridad de la información, con enfoque en resiliencia cibernética y gestión de riesgos en la nube.	Organización Internacional de Normalización (ISO)
ISO/IEC 23894	2023	Gestión de riesgos en inteligencia artificial (IA), proporcionando directrices para la evaluación y mitigación de riesgos en modelos de IA.	Organización Internacional de Normalización (ISO)
NIST Cybersecurity Framework (CSF)	2023	Marco actualizado para la gestión de riesgos de ciberseguridad, aplicable a entidades gubernamentales y privadas.	Instituto Nacional de Estándares y Tecnología (NIST, EE.UU.)

6. RESPONSABLES:

- Jefe oficina sistemas de información TIC.

7. CONTENIDO DEL PLAN:

7.1. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1.1. Lineamientos de estructura organizacional de seguridad de la información

La Subred Sur ESE establece un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

Normas que rigen para la estructura organizacional de seguridad de la información.

Normas dirigidas a: Alta dirección

- La alta dirección de la Subred Sur ESE debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- La alta dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La alta dirección debe revisar y aprobar las políticas específicas de seguridad de la información contenidas en este documento.
- La alta dirección debe promover activamente una cultura de seguridad de la información en la Subred Sur
- La alta dirección debe facilitar la divulgación de las políticas de seguridad de la información a todos los colaboradores de la entidad y al personal provisto por terceras partes.
- La alta dirección debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de La Subred Sur ESE.

Normas dirigidas a: Comité de seguridad de la información – CSI

- El comité de seguridad de la información debe actualizar y presentar ante la junta directiva las políticas de seguridad de la información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El comité de seguridad de la información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El comité de seguridad de la información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe liderar la generación de lineamientos para gestionar la seguridad de la información de la Subred Sur ESE y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- La oficina de control interno debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
- La oficina de control interno debe planear y ejecutar las auditorías internas al sistema de gestión de seguridad de la información de la Subred Sur ESE a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La oficina de control interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del sistema de gestión de seguridad de la información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- La oficina de control interno debe informar a las áreas responsables los hallazgos de las auditorías.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe asignar las funciones, roles y responsabilidades, a sus colaboradores para la operación y administración de la plataforma tecnológica de la Subred Sur ESE. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: Todos los usuarios

- Los directivos, colaboradores, contratistas, terceros y otros colaboradores de la Subred Sur ESE, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

7.1.2. Lineamientos para uso de dispositivos móviles

La Subred Sur ESE proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la Subred Sur ESE. Así mismo, velará porque los colaboradores hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

Normas para uso de dispositivos móviles.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la Subred Sur ESE.
- La oficina de sistemas de información TIC debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por La Subred Sur ESE.
- La oficina de sistemas de información TIC debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- La oficina de sistemas de información TIC debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- La oficina de sistemas de información TIC debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- La oficina de sistemas de información TIC debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de la Subred Sur ESE; dichas copias deben acogerse a la política de copias de respaldo de la información.
- La oficina de sistemas de información TIC debe instalar un software de antivirus tanto en los dispositivos móviles institucionales. Como en los personales que hagan uso de los servicios provistos por la Subred Sur ESE.
- La oficina de sistemas de información TIC debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: Todos los usuarios

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

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles, cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

7.1.3.Lineamientos para uso de conexiones remotas

La Subred Sur ESE establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Subred Sur ESE; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Normas para uso de conexiones remotas

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- La oficina de sistemas de información TIC debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la Subred Sur ESE de manera permanente.

Normas dirigidas a: Oficina de control interno

La oficina de control interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la Subred Sur ESE.

Normas dirigidas a: Todos los usuarios

Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Subred Sur ESE y deben acatar las condiciones de uso establecidas para dichas conexiones.

Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles, cafés internet, entre otros.

7.2. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información pretenden instituir y afianzar la cultura de seguridad de la información entre los colaboradores, contratistas, personal externo y proveedores de la Subred Sur ESE. Por tal razón, se hace necesario que las violaciones a las políticas seguridad de la información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7.2.1. Notificaciones de violaciones de seguridad:

Es de carácter obligatorio para todos los colaboradores de la Subred Sur ESE, la notificación inmediata de algún problema o violación de la seguridad, del cual fuere testigo; esta notificación debe realizarse por escrito vía correo electrónico a la gerencia y/o a los administradores de tecnologías de información - ATI y/o al líder de gestión de tecnologías de información y comunicaciones - TIC, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de todo colaborador que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a la Subred Sur ESE de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por tanto, se debe conocer y respetar las políticas de seguridad.

Está fundamentado como una exigencia que el personal de la organización conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta, escrita en las políticas de seguridad firmado por los colaboradores, contratistas, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Subred Sur ESE.

Por esta razón se entenderá que sólo una adecuada política de seguridad apoyará la concientización para obtener la colaboración de los colaboradores, haciéndoles conscientes de los riesgos que podemos correr y de la importancia del cumplimiento de las normas.

7.3. LINEAMIENTOS DE SEGURIDAD DEL PERSONAL

7.3.1. Lineamientos relacionada con la vinculación de colaboradores:

La Subred Sur ESE reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos colaboradores se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los colaboradores en sus cargos.

Normas relacionadas con la vinculación de colaboradores

<u>Normas dirigidas a: Las direcciones de contratación y talento humano</u>

- Las direcciones de contratación y talento humano deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la Subred Sur ESE, antes de su vinculación definitiva.
- Las direcciones de contratación y talento humano deben certificar que los colaboradores de la Subred Sur ESE firmen un acuerdo y/o cláusula de confidencialidad y un documento de aceptación de políticas de seguridad de la información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: supervisores de contrato, subgerentes, coordinadores, directores, líderes y jefes de oficina

- Cada supervisor de contrato, subgerente, coordinador, director, líder y jefe de oficina debe verificar la existencia de acuerdos y/o cláusulas de confidencialidad y de la documentación de aceptación de políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de la Subred Sur ESE.

Normas dirigidas a: Personal provistos por terceras partes

- El personal provisto por terceras partes que realicen labores en o para la Subred Sur ESE, deben firmar un acuerdo y/o cláusula de confidencialidad y un documento de aceptación de políticas de seguridad de la información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- El personal provisto por terceras partes, deben garantizar el cumplimiento de los acuerdos y/o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información de la Subred Sur ESE.

7.4. LINEAMIENTOS APLICABLES DURANTE LA VINCULACIÓN DE COLABORADORES Y PERSONAL PROVISTO POR TERCEROS

La Subred Sur ESE en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la alta dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las políticas de seguridad de la información de la Subred Sur ESE.

Todos los colaboradores de la Subred Sur ESE enmarcados en este aparte deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

Normas aplicables durante la vinculación de colaboradores y personal provisto por terceros.

Normas dirigidas a: Alta dirección

- La alta dirección debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer la Subred Sur ESE.
- La alta dirección debe promover la importancia de la seguridad de la información entre los colaboradores de la Subred Sur ESE y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
- La alta dirección debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente de la Subred Sur ESE, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe diseñar y ejecutar de manera permanente un programa de concientización en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
- La oficina de control interno debe capacitar y entrenar a los colaboradores de la Subred Sur ESE en el programa de concientización en seguridad de la información para evitar posibles riesgos de seguridad.

Normas dirigidas a: Oficina de control interno disciplinario

- La oficina de control interno disciplinario debe aplicar el proceso disciplinario de la Subred Sur ESE cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

Normas dirigidas a: las direcciones de contratación y talento humano

- Las direcciones de contratación y talento humano deben convocar a los colaboradores y personal provisto por terceras partes a las charlas y eventos programados como parte del programa de concientización en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Normas dirigidas a: Todos los usuarios

- Los colaboradores y personal provisto por terceras partes que por sus funciones hagan uso de la información de la Subred Sur ESE, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

7.5. LINEAMIENTOS DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS COLABORADORES Y PERSONAL PROVISTO POR TERCEROS

La Subred Sur ESE asegurará que sus colaboradores y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Normas para la desvinculación, licencias, vacaciones o cambios de labores de los colaboradores y personal provisto por terceros

Normas dirigidas a: Las direcciones de contratación y talento humano

- Las direcciones de contratación y talento humano deben realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los colaboradores de la Subred Sur ESE llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.
- Normas dirigidas a: supervisores de contrato, subgerentes, coordinadores, directores, líderes y jefes de oficina
- Cada supervisor de contrato, subgerente, coordinador, director, líder y jefe de oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los colaboradores o personal provistos por terceras partes a la oficina de control interno.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la oficina de sistemas de información TIC cuando haya lugar.

7.6. LINEAMIENTOS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN LINEAMIENTOS DE RESPONSABILIDAD POR LOS ACTIVOS

La Subred Sur ESE como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la Subred Sur ESE, son activos de la institución y se proporcionan a los colaboradores y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de la Subred Sur ESE, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la oficina de control interno. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

Normas de responsabilidad por los activos

Normas dirigidas a: Propietarios de los activos de información

- Las subgerencias, coordinaciones, direcciones y oficinas asesoras de la Subred Sur ESE, deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la Subred Sur ESE, se encuentran sujetos a auditorías por parte de la oficina de control interno y a revisiones de cumplimiento por parte de la oficina de control interno.

Normas dirigidas a: Oficina sistemas de información tic y área de activos fijos

- La oficina de sistemas de información TIC es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Subred Sur ESE y, en consecuencia, debe asegurar su apropiada operación y administración.
- La oficina de sistemas de información TIC en conjunto con el área de activos fijos, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de La Subred Sur ESE.

- la oficina de sistemas de información TIC debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La oficina de sistemas de información TIC es responsable de preparar los equipos de cómputo fijos y/o portátiles de los colaboradores y de hacer entrega de los mismos.
- La oficina de sistemas de información TIC en conjunto con el área de activos fijos son los responsables de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los colaboradores que se retiran o cambian de labores, cuando les es formalmente solicitado.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la Subred Sur ESE.
- La oficina de control interno debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.
- La oficina de control interno debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Subred Sur ESE.

Normas dirigidas a: Subgerentes, coordinadores, directores, líderes y jefes de oficina

- Los subgerentes, coordinadores, directores, líderes y jefes de oficina, o quien ellos designen, deben autorizar a sus colaboradores el uso de los recursos tecnológicos, previamente preparados por la oficina de sistemas de información TIC.
- Los subgerentes, coordinadores, directores, líderes y jefes de oficina, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la Subred Sur ESE o son trasladados de área.

Normas dirigidas a: Todos los usuarios

- Los recursos tecnológicos de la Subred Sur ESE, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Subred Sur ESE.
- Los recursos tecnológicos de la Subred Sur ESE provistos a colaboradores y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la Subred Sur ESE; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los colaboradores no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- Los colaboradores no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la Subred Sur ESE.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignadas a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los colaboradores deben realizar la entrega de su puesto de trabajo al Subgerente, Coordinador, Director, Líder o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

7.7. LINEAMIENTOS DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La Subred Sur ESE definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección. Toda la información de la Subred Sur ESE debe ser identificada, clasificada y documentada de acuerdo con las guías de clasificación de la información establecidas por el comité de seguridad de la información. Una vez clasificada, la Subred Sur ESE proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los colaboradores de la Subred Sur ESE y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

Normas para la clasificación y manejo de la información Normas dirigidas a: comité de seguridad de la información

- El comité de seguridad de la información debe recomendar los niveles de clasificación de la información propuestos por la oficina de control interno y la guía de clasificación de la Información de la Subred Sur ESE para que sean aprobados por la Junta Directiva.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe definir los niveles de clasificación de la información para la Subred Sur ESE y, posteriormente generar la guía de clasificación de la Información.
- La oficina de control interno debe socializar y divulgar la guía de clasificación de la Información a los colaboradores de La Subred Sur ESE.
- La oficina de control interno debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- La oficina de sistemas de información TIC debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: oficina sistemas de información tic y oficina de control interno

- La oficina de sistemas de información TIC junto con la oficina de control interno deben definir los métodos de cifrado de la información de la entidad de acuerdo al nivel de clasificación de los activos.

Normas dirigidas a: Coordinación gestión documental

- La coordinación de gestión documental debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- La Coordinación de Gestión Documental debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.
- La Coordinación de gestión documental debe administrar el contrato de almacenamiento y resguardo de las cintas de backup, otros medios de almacenamiento y documentos físicos de la Subred Sur ESE con el proveedor del servicio.

- La coordinación de gestión documental debe verificar el cumplimiento de los acuerdos de niveles de servicio y acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos de la Subred Sur ESE.

Normas dirigidas a: Propietarios de los activos de información

- Los propietarios de los activos de información deben clasificar su información de acuerdo con las guías de clasificación de la Información establecida.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su reclasificación.

Normas dirigidas a: Todos los usuarios

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

7.8. LINEAMIENTOS PARA USO DE TOKENS DE SEGURIDAD Y FIRMAS DIGITALES

La Subred Sur ESE proveerá las condiciones de manejo de los tokens de seguridad y firmas digitales para los procesos que los utilizan y velará porque los colaboradores hagan un uso responsable de estos.

Normas para uso de tokens de seguridad y Firmas Digitales

Normas dirigidas a: Áreas usuarias de tokens de seguridad y firmas digitales

- Cada área usuaria de tokens de seguridad y firmas digitales debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a: Administradores de los tokens de seguridad y firmas digitales

- Los Administradores de los tokens de seguridad y firmas digitales deben procesar las solicitudes de dichos tokens y Firmas según los requerimientos de cada entidad proveedora de éstos y adjuntar la documentación necesaria.

- Los Administradores de los tokens y firmas digitales deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Los administradores de los tokens y firmas digitales deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- Los administradores de los tokens y firmas digitales deben entregar a los colaboradores designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de los mismos.
- Los administradores de los tokens y firmas digitales deben dar avisos a las entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Los administradores de los tokens y firmas digitales deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: Usuarios de tokens de seguridad y firmas digitales

- Los usuarios que requieren utilizar los tokens de seguridad y firmas digitales deben contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens y firmas harán parte del inventario físico y Activos de Información de cada usuario a quien se haya asignado.
- Los usuarios deben devolver el token asignado y firma digital en estado operativo al administrador de los tokens y firmas digitales cuando el vínculo laboral con la subred sur ese se dé por terminado o haya cambio de cargo, para obtener paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la Subred Sur ESE.
- Cada usuario de los portales o sitios de uso de los tokens y firmas digitales debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso. El almacenamiento de los tokens y firmas digitales debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token y firma digital, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- Los usuarios deben notificar al Administrador de los tokens y firmas digitales en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comunique con las entidades emisoras de dichos tokens y firmas.
- Los usuarios no deben permitir que terceras personas observen la clave que genera el token y/o firma digital, así como no deben aceptar ayuda de terceros para la utilización del token y firma digital.
- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token y/o firma digital asignados, en el desarrollo de las actividades como colaboradores de la Subred Sur ESE. En caso de que suceda algún evento irregular con los tokens y firmas digitales los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
- Los usuarios deben mantener los tokens y firmas digitales asignados en un lugar seco y no introducirlos en agua u otros líquidos.
- Los usuarios deben evitar exponer los tokens y firmas digitales a campos magnéticos y a temperaturas extremas.

- Los usuarios deben evitar que los tokens y firmas digitales sean golpeados o sometidos a esfuerzo físico.
- Los usuarios no deben abrir los tokens y firmas digitales, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

Los usuarios no deben usar los tokens y firmas digitales fuera de las instalaciones de la Subred Sur ESE para evitar pérdida o robo de estos.

7.9. LINEAMIENTOS DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Subred Sur ESE será reglamentado por la oficina de sistemas de información TIC, junto con la oficina de control interno, considerando las labores realizadas por los colaboradores y su necesidad de uso.

Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Subred Sur ESE, de acuerdo con los lineamientos y condiciones establecidas.
- La oficina de sistemas de información TIC debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la Subred Sur ESE, ya sea cuando son dados de baja o reasignados a un nuevo usuario.
- La oficina de sistemas de información TIC debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la Subred Sur ESE de acuerdo con el perfil del cargo del funcionario solicitante.

Normas dirigidas a: Todos los usuarios

- Los colaboradores y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la oficina de sistemas de información TIC.
- Los colaboradores de la Subred Sur ESE y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la oficina de sistemas de información TIC.
- Los colaboradores y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.
- Los colaboradores y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Subred Sur ESE.

7.10. LINEAMIENTOS DE GESTIÓN Y CONTROL DE ACCESO LINEAMIENTOS DE ACCESO A REDES Y RECURSOS DE RED

La oficina de sistemas de información TIC de la Subred Sur ESE, como responsables de las redes de datos y los recursos tecnológicos de red de la Subred Sur ESE, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Normas de acceso a redes y recursos de red

Normas dirigidas a: La oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de La Subred Sur ESE.
- La oficina de sistemas de información TIC debe asegurar que las redes inalámbricas de la Subred Sur ESE cuenten con métodos de autenticación que evite accesos no autorizados.
- La oficina de sistemas de información TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la Subred Sur ESE, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.
- La oficina de sistemas de información TIC debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de La Subred Sur ESE.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: Todos los usuarios

- Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Subred Sur ESE, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Subred Sur ESE deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

7.11. LINEAMIENTOS DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

La Subred Sur ESE establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos, los sistemas de información y los aplicativos de la Subred Sur ESE. Así mismo, velará porque los colaboradores y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Normas de administración de acceso de usuarios normas dirigidas a: Oficina sistemas de información TIC.

- La oficina de sistemas de información TIC debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos, sistemas de información y aplicativos de la Subred Sur ESE, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- La oficina de sistemas de información TIC, previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- La oficina de sistemas de información TIC debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Subred Sur ESE; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros
- La oficina de sistemas de información TIC debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red, los sistemas de información y aplicativos de manera oportuna, cuando los colaboradores o el personal provisto por terceras partes se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- La oficina de sistemas de información TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
- La oficina de sistemas de información TIC debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la Subred Sur ESE.

Normas dirigidas a: Propietarios de los activos de información

- Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
- Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: Subgerentes, coordinadores, directores, líderes y jefes de oficina

- Los subgerentes, coordinadores, directores, líderes y jefes de oficina son los únicos que pueden solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los colaboradores que laboran en sus áreas, acogiéndose al procedimiento establecido para tal fin.

7.12. LINEAMIENTOS DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de la Subred Sur ESE realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: Todos los usuarios

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Subred Sur ESE deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los colaboradores no deben compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes.
- Los colaboradores y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la Subred Sur ESE deben acogerse a lineamientos para la configuración de contraseñas implantados por la Subred Sur ESE.

7.13. LINEAMIENTOS DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

La oficina de sistemas de información TIC de la Subred Sur ESE velará porque los recursos de la plataforma tecnológica y los servicios de red de La Subred Sur ESE sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: Oficina sistemas de información tic, administradores de los recursos tecnológicos y servicios de red

- La oficina de sistemas de información TIC debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos colaboradores designados para dichas funciones.
- La oficina de sistemas de información TIC debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- La oficina de sistemas de información TIC debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.
- La oficina de sistemas de información TIC debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- La oficina de sistemas de información TIC debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- La oficina de sistemas de información TIC debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, colaboradores de la Oficina de Sistemas de Información TIC, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de la Subred Sur ESE.

- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La oficina de sistemas de información TIC debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.
- La oficina de sistemas de información TIC debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoria de la plataforma tecnológica y los sistemas de información.

7.14. LINEAMIENTOS DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Las subgerencias, coordinaciones, direcciones, áreas lideres o jefaturas de oficina como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La oficina de sistemas de información TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: Propietarios de los activos de información

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- La oficina de sistemas de información TIC debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

- La oficina de sistemas de información TIC debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La oficina de sistemas de información TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a: Desarrolladores (internos y externos)

- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla. (Codificación de errores para evitar despliegue de información sensible y/o susceptible de interpretación)
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.
- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
- Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

7.15. LINEAMIENTOS DE CRIPTOGRAFIA

7.15.1. Lineamientos de controles criptográficos:

La Subred Sur ESE velará porque la información de La Subred Sur ESE, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

Normas de controles criptográficos

Normas dirigidas a: Gestión de la información

- El área de gestión de la información debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información tic debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La oficina de sistemas de información tic debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- La oficina de sistemas de información tic, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la oficina de sistemas de información TIC.

7.16. LINEAMIENTOS DE SEGURIDAD FÍSICA Y MEDIO AMBIENTAL LINEAMIENTOS DE ÁREAS SEGURAS

La Subred Sur ESE proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

Normas de áreas seguras

Normas dirigidas a: Oficina sistemas de información TIC

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por colaboradores de la oficina de sistemas de información TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- La oficina de sistemas de información TIC debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

- La oficina de sistemas de información TIC debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado
- La oficina de sistemas de información TIC debe velar porque los recursos de la plataforma tecnológica de la Subred Sur ESE ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La oficina de sistemas de información TIC debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La oficina de sistemas de información TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: subgerentes, coordinadores, directores, líderes y jefes de oficina

- Subgerentes, coordinadores, directores, líderes y jefes de oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su área.
- Los subgerentes, coordinadores, directores, líderes y jefes de oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Los subgerentes, coordinadores, directores, líderes y jefes de oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los colaboradores autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros colaboradores de La Subred Sur ESE.

Normas dirigidas a: Área de recursos físicos

- El área de recursos físicos debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- El grupo de recursos físicos debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Subred Sur ESE.
- El grupo de recursos físicos debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la Subred Sur ESE.
- El grupo de recursos físicos debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Subred Sur ESE.
- El grupo de recursos físicos debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

- El grupo de recursos físicos debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.
- El grupo de recursos físicos debe cerciorarse de que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- El grupo de recursos físicos, con el acompañamiento de la oficina de sistemas de información TIC, debe verificar que el cableado de datos se encuentra protegido con el fin de disminuir las intercepciones o daños.
-

Normas dirigidas a: Todos los usuarios

- Los ingresos y egresos de personal a las instalaciones de la Subred Sur ESE deben ser registrados; por consiguiente, los colaboradores y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los colaboradores deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de La Subred Sur ESE; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos colaboradores o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los colaboradores de La Subred Sur ESE y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

7.17. LINEAMIENTOS DE SEGURIDAD PARA LOS EQUIPOS

7.17.1. Lineamientos de seguridad para los equipos institucionales

La Subred Sur ESE para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Subred Sur ESE que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Normas de seguridad para los equipos institucionales

Normas dirigidas a: OFICINA SISTEMAS DE INFORMACION TIC

- La oficina de sistemas de información TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los Activos de Información, dentro y fuera de las instalaciones de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de propiedad de la Subred Sur ESE.
- La Oficina de Sistemas de Información TIC, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
- La oficina de sistemas de información TIC debe generar estándares de configuración segura para los equipos de cómputo de los colaboradores de la Subred Sur ESE y configurar dichos equipos acogiendo los estándares generados.
- La oficina de sistemas de información TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran

conectarse a la red de datos de la Subred Sur ESE y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

- La oficina de sistemas de información TIC debe velar porque a los equipos de cómputo provistos por terceros realice los mantenimientos preventivos y correctivos de acuerdo al cronograma previamente establecido.
- La oficina de sistemas de Información TIC debe aislar los equipos de áreas sensibles, como el Área de Tesorería para proteger su acceso de los demás colaboradores de la red de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los colaboradores de la Subred Sur ESE, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.
- La oficina de control interno debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de La Subred Sur ESE, en particular de las áreas sensibles.

Normas dirigidas a: Grupo de recursos físicos

- El grupo de recursos físicos debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- El grupo de recursos físicos debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

Normas dirigidas a: Área de activos fijos

- El de activos fijos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la Subred Sur ESE cuente con la autorización documentada y aprobada previamente por el coordinador de recursos físicos.
- El área de activos fijos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la Subred Sur ESE, posean pólizas de seguro.

Normas dirigidas a: Todos los usuarios

- La oficina de sistemas de información TIC es la única área autorizada para realizar movimientos previa notificación al área de activos fijos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Subred Sur ESE.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los colaboradores y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la oficina de sistemas de información TIC.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico bien sea de propiedad de la Subred Sur ESE como de Terceros, el usuario responsable debe informar a la mesa de ayuda en donde se atenderá o escalará al interior de la oficina de sistemas de información TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Subred Sur ESE, solo puede ser realizado por los colaboradores de la oficina de sistemas de información TIC, o personal de terceras partes autorizado por la oficina de sistemas de información TIC.
- Los colaboradores de la Subred Sur ESE y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los colaboradores de La Subred Sur ESE y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo de la Subred Sur ESE, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

7.18. BLOQUEO DE ESCRITORIO, PANTALLA LIMPIA E IMPRESIÓN RETENIDA

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los colaboradores de la Subred Sur ESE deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDS, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata, para tal efecto.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla institucional, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

7.19. LINEAMIENTOS DE SEGURIDAD EN LAS OPERACIONES

7.19.1. Lineamientos de asignación de responsabilidades operativas:

La oficina de sistemas de información TIC, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la Subred Sur ESE, asignará funciones específicas a sus colaboradores, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La oficina de sistemas de información TIC proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Subred Sur ESE, efectuando

proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

Normas de asignación de responsabilidades operativas

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe efectuar, a través de sus colaboradores, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe proporcionar a sus colaboradores manuales de configuración y/u operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la Subred Sur ESE.

7.20. LINEAMIENTOS DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La Subred Sur ESE proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus colaboradores y personal provisto por terceras partes frente a los ataques de software malicioso.

Normas de protección frente a software malicioso.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Subred Sur ESE y los servicios que se ejecutan en la misma.
- La oficina de sistemas de información TIC debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- La oficina de sistemas de información TIC debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- la oficina de sistemas de información TIC, a través de sus colaboradores, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: Todos los usuarios

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Oficina de Sistemas de Información TIC; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la mesa de ayuda, para que, a través de ella, la oficina de sistemas de información TIC tome las medidas de control correspondientes.

7.21. LINEAMIENTOS DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Subred Sur ESE certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la oficina de sistemas de información TIC, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la Subred Sur ESE velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Normas de copias de respaldo de la información

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC, a través de sus colaboradores, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- La oficina de sistemas de información TIC debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

- La oficina de sistemas de información TIC debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La oficina de sistemas de información TIC debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Subred Sur ESE.

Normas dirigidas a: Propietarios de los activos de información

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la oficina de sistemas de información TIC, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: Todos los usuarios

- Es responsabilidad de los usuarios de la plataforma tecnológica de La Subred Sur ESE identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

7.22. LINEAMIENTOS DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

La Subred Sur ESE realizará monitoreo permanente del uso que dan los colaboradores y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la Subred Sur ESE. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

La oficina de sistemas de información TIC y la Oficina de Control Interno definirán la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Subred Sur ESE. Ambas áreas trimestralmente se reunirán a analizar los resultados del monitoreo efectuado.

Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información.

Normas dirigidas a: Oficina sistemas de información TIC y oficina de control interno

- La oficina de sistemas de información TIC, en conjunto con la Oficina de Control Interno, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de La Subred Sur ESE.
- La oficina de sistemas de información TIC y la Oficina de Control Interno, deben definir de manera trimestral cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Subred Sur ESE. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La oficina de sistemas de información TIC debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Subred Sur ESE. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe determinar los periodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información de la Subred Sur ESE.
- La oficina de control interno debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

Normas dirigidas a: Administradores de red

- Los administradores de red deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los administradores de red deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la oficina de sistemas de información TIC y la oficina de control interno.
- Los administradores de red deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

7.23. LINEAMIENTOS DE CONTROL AL SOFTWARE OPERATIVO

La Subred Sur ESE, a través de la Oficina de Sistemas de Información TIC, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Normas de control al software operativo

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Subred Sur ESE.
- La oficina de sistemas de información TIC debe asegurarse que el software operativo instalado en la plataforma tecnológica de la Subred Sur ESE cuenta con soporte de los proveedores en el caso de que este sea provisto por terceros.
- La oficina de sistemas de información TIC debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- La oficina de sistemas de información TIC debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- La oficina de sistemas de información TIC debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Subred Sur ESE.

7.24. LINEAMIENTOS DE GESTIÓN DE VULNERABILIDADES

La Subred Sur ESE, a través de la oficina de sistemas de información TIC y la oficina de control interno, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas dos áreas serán las encargadas de revisar, valorar y gestionar las vulnerabilidades encontradas.

Normas para la gestión de vulnerabilidades

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- La oficina de control interno debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- la oficina de sistemas de información TIC, a través de sus colaboradores, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Normas dirigidas a: Oficina sistemas de información TIC y oficina de control interno

- La oficina de sistemas de información TIC y la oficina de control interno, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

7.25. LINEAMIENTOS DE SEGURIDAD EN LAS COMUNICACIONES

7.25.1. Lineamientos de gestión y aseguramiento de las redes de datos

La Subred Sur ESE establecerá, a través de la oficina de sistemas de información TIC, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas, así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Subred Sur ESE.

Normas de gestión y aseguramiento de las redes de datos Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Subred Sur ESE.

- La oficina de sistemas de información TIC debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La oficina de sistemas de información TIC debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Subred Sur ESE.
- La oficina de sistemas de información TIC debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- La oficina de sistemas de información TIC debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Subred Sur ESE, acogiendo buenas prácticas de configuración segura.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Subred Sur ESE en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La oficina de sistemas de información TIC debe instalar protección entre las redes internas de la Subred Sur ESE y cualquier red externa, que este fuera de la capacidad de control y administración de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Subred Sur ESE.

7.26. LINEAMIENTOS DE USO DEL CORREO ELECTRÓNICO

La Subred Sur ESE, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre colaboradores y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Normas de uso del correo electrónico

Normas dirigidas a: oficina sistemas de información TIC y oficina de control interno

- La oficina de sistemas de información TIC estableció el procedimiento para la administración de cuentas de correo electrónico el cual se describe en el documento “GI-TICS-PR-05 creación modificación o actualización y eliminación correo institucional”, el cual se encuentra publicado en la intranet de la entidad.
- La Oficina de Sistemas de Información TIC debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- La oficina de sistemas de información TIC debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La oficina de sistemas de información TIC debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La oficina de sistemas de información TIC, con el apoyo de la Oficina de Control Interno, debe generar campañas para concientizar tanto a los colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

- La oficina de sistemas de información TIC estudiara las solicitudes de acceso web, autorizando las que realmente por su labor diaria requiera el acceso desde cualquier lugar de la subred sur.

Normas dirigidas a: Directores y jefes de oficina

- Los directores y Jefes de Oficina deberán solicitar la creación de las cuentas electrónicas de sus subprocesos a través del formato GI-TICS-FT-04 CREACION DE USUARIOS en el cual se registran los datos necesarios del usuario que hará uso de este servicio, el cual se encuentra disponible en la intranet de la institución. Así mismo debe solicitar la modificación o inactivación de ser necesaria de las cuentas electrónicas a la oficina de sistemas de información TIC.
- Los directores y jefes de oficina deberán solicitar el acceso Web al correo electrónico institucional con la debida justificación a la oficina de sistemas de información TIC.

Normas dirigidas a: Todos los usuarios

- La cuenta de correo electrónico asignada es por procesos y/o servicios; por consiguiente, ningún funcionario de la Subred Sur ESE o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos es propiedad de la Subred sur por lo que se debe usar únicamente para temas relacionados con el desarrollo de labores y funciones de cada usuario en apoyo al objetivo misional de la Subred Sur ESE y no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Subred Sur ESE, y cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los colaboradores de la Subred Sur ESE y el personal provisto por terceras partes.
- Los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información institucional.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Subred Sur, su cuenta de correo debe ser entregada por medio de acta a su superior.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Subred Sur ESE y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad. El único servicio de correo electrónico autorizado en la entidad es el asignado por la oficina de sistemas de información TIC.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos.

7.27. LINEAMIENTOS DE USO ADECUADO DE INTERNET

La Subred Sur ESE consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la Subred Sur ESE.

Normas de uso adecuado de internet

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.
- La oficina de sistemas de información TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La oficina de sistemas de información tic debe monitorear continuamente el canal o canales del servicio de internet.
- La oficina de sistemas de información TIC debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.
- La oficina de sistemas de información TIC debe generar registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe generar campañas para concientizar tanto a los colaboradores internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: Todos los usuarios

- Los usuarios del servicio de Internet de la Subred Sur ESE deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Hotmail, Gmail, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Subred Sur ESE.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Oficina de Sistemas de

Información TIC, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- No está permitido el intercambio no autorizado de información de propiedad de la Subred Sur ESE, de sus clientes y/o de sus colaboradores, con terceros.

7.28. LINEAMIENTOS DE INTERCAMBIO DE INFORMACIÓN

La Subred Sur ESE asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad y/o de intercambio de información con las terceras partes con quienes se realice dicho intercambio. La Subred Sur ESE propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Normas de intercambio de información

Normas dirigidas a: Área de contratación

- El área de contratación, en acompañamiento con la oficina de control interno, debe definir los modelos de acuerdos de confidencialidad y/o de Intercambio de Información entre la Subred Sur ESE y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Subred Sur ESE a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- El área de contratación debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la Subred Sur ESE que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la Subred Sur ESE.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Subred Sur ESE, reciben o envían información de los beneficiarios de la Subred Sur ESE, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- la oficina de control interno debe velar porque el intercambio de información de la Subred Sur ESE con entidades externas se realice en cumplimiento de las políticas de seguridad para el intercambio de información aquí descritas, los acuerdos de intercambio de Información y el procedimiento definido para dicho intercambio de información.
- La oficina de control interno debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Normas dirigidas a: Propietarios de los activos de información

- Los propietarios de los activos de información deben velar porque la información de la Subred Sur ESE o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las

cláusulas relacionadas en los contratos, acuerdos de confidencialidad o acuerdos de intercambio establecidos.

- Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la Subred Sur ESE por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la Subred Sur ESE así como del procedimiento de intercambio de información.
- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Normas dirigidas a: Coordinación de gestión documental

- La coordinación de gestión documental debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La coordinación de gestión documental debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la Subred Sur ESE, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Normas dirigidas a: Terceros con quienes se intercambia información de la Subred Sur Ese

- Los terceros con quienes se intercambia información de la Subred Sur ESE deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la Subred Sur ESE, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.
- Los terceros con quienes se intercambia información de la Subred Sur ESE deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: Todos los usuarios

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de La Subred Sur ESE o de sus beneficiarios.
- No está permitido el intercambio de información sensible de La Subred Sur ESE por vía telefónica.

7.29. LINEAMIENTOS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

7.29.1. Lineamientos para el establecimiento de requisitos de seguridad

La Subred Sur ESE asegurará que el software adquirido y desarrollado tanto al interior de La Subred Sur ESE, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él.

Las áreas propietarias de sistemas de información, la oficina de sistemas de información TIC y la Oficina de Control Interno incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: propietarios de los sistemas de información, oficina sistemas de información tic y oficina de control interno

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de La Subred Sur ESE formalmente asignada.
- La oficina de sistemas de información TIC debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera. Las áreas propietarias de los sistemas de información, en acompañamiento con La oficina de sistemas de información TIC y la oficina de control interno deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.
- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La oficina de control interno debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores deben utilizar usar los protocolos sugeridos por la oficina de sistemas de información TIC y la oficina de control interno en los aplicativos desarrollados.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

7.30. LINEAMIENTOS DE DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La Subred Sur ESE velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Subred Sur ESE.

Normas de desarrollo seguro, realización de pruebas y soporte de los propietarios de los sistemas de información

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y Aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La oficina de sistemas de información TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La oficina de sistemas de información TIC debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La oficina de sistemas de información TIC, a través de sus colaboradores, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada

sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- La oficina de sistemas de información TIC debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la Subred Sur ESE.

Normas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la Subred Sur ESE; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar

privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

7.31. LINEAMIENTOS PARA LA PROTECCIÓN DE LOS DATOS DE PRUEBA

La oficina de sistemas de información TIC de La Subred Sur ESE protegerá los datos de prueba que se entregarán a los d desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

Normas para la protección de los datos de prueba

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- La oficina de sistemas de información TIC debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

7.32. LINEAMIENTOS QUE RIGEN LA RELACIÓN CON TERCERAS PARTES

7.32.1. Lineamientos de inclusión de condiciones de seguridad en la relación con terceras partes

La Subred Sur ESE establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los colaboradores responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: Oficina sistemas de información TIC, oficina asesora jurídica y oficina de control interno

- La oficina de sistemas de información TIC, la oficina asesora jurídica y la oficina de control interno deben generar un modelo base para los acuerdos de niveles de servicio y requisitos de seguridad de la información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- La oficina de sistemas de información TIC, la oficina asesora jurídica y la oficina de control interno deben elaborar modelos de acuerdos de confidencialidad y acuerdos de intercambio de información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Subred Sur ESE.
- La oficina de sistemas de información TIC debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- La oficina de sistemas de información TIC debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la Subred Sur ESE.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe evaluar y aprobar los accesos a la información de La Subred Sur ESE requeridos por terceras partes.
- la oficina de control interno debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Normas dirigidas a: Supervisores de contratos con terceros

- Los supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Subred Sur ESE a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

7.33. LINEAMIENTOS DE GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

La Subred Sur ESE propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: oficina sistemas de información TIC y oficina de control interno

- La oficina de sistemas de información TIC debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Subred Sur ESE.
- La oficina de sistemas de información TIC y la oficina de control interno deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: Oficina de control interno y supervisores de contratos con terceros

- La oficina de control interno y los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los acuerdos de niveles de servicio, acuerdos de confidencialidad, acuerdos de intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

- Los Supervisores de contratos con terceros, con el apoyo de la oficina de control interno, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

7.34. LINEAMIENTOS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

7.34.1. Lineamientos para el reporte y tratamiento de incidentes de seguridad

La Subred Sur ESE promoverá entre los colaboradores y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La alta dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: Propietarios de los activos de información

- Los propietarios de los activos de información deben informar a la Oficina de Control Interno, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La oficina de control interno debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.
- La oficina de control interno debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
- La oficina de control interno debe, con el apoyo con La Oficina de Sistemas de Información TIC, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a: Comité de seguridad de la información

- El comité de seguridad de la información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: Todos los usuarios

- Es responsabilidad de los colaboradores de La Subred Sur ESE y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los colaboradores deben notificarlo a la Oficina de Control Interno para que se registre y se le dé el trámite necesario.

7.35. LINEAMIENTOS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

7.35.1. Lineamientos de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

La Subred Sur ESE proporcionará los recursos suficientes para proporcionar una respuesta efectiva de colaboradores y procesos en caso de contingencia o eventos catastróficos que se presenten en la Subred Sur ESE y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La Subred Sur ESE mantendrá canales de comunicación adecuados hacia colaboradores, proveedores y terceras partes interesadas.

Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: Comité se seguridad de la información y oficina de control interno

- El comité de seguridad de la información, junto con la oficina de control interno, deben reconocer las situaciones que serán identificadas como emergencia o desastre para la Subred Sur ESE, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- El comité de seguridad de la información, junto con la oficina de control interno, deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres.
- La oficina de control interno debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar. El Comité de Seguridad de la Información, junto con la oficina de control interno, producto del análisis de impacto al negocio (BIA) deben seleccionar las estrategias de recuperación más convenientes para la Subred Sur ESE.
- La oficina de control interno debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El comité de seguridad de la información, junto con la oficina de control interno, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

Normas dirigidas a: Oficina sistemas de información TIC Y oficina de control interno

- La oficina de control interno, en conjunto con La oficina de sistemas de información TIC, deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- La oficina de sistemas de información TIC y la oficina de control interno deben participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al comité de seguridad de la información.

Normas dirigidas a: subgerentes, coordinadores, directores, líderes y jefes de oficina

- los subgerentes, coordinadores, directores, líderes y jefes de oficina deben identificar, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. estos documentos deben ser probados para certificar su efectividad.

7.36. LINEAMIENTOS DE REDUNDANCIA

La Subred Sur ESE propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Subred Sur ESE.

Normas de redundancia

Normas dirigidas a: Oficina sistemas de información TIC y oficina de control interno

- La oficina de sistemas de información TIC y la oficina de control interno deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la Subred Sur ESE y la plataforma tecnológica que los apoya.
- La oficina de sistemas de información TIC y debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Subred Sur ESE.
- La oficina de sistemas de información TIC, a través de sus colaboradores, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Subred Sur ESE.

7.37. LINEAMIENTOS DE CUMPLIMIENTO

7.37.1. Lineamientos de cumplimiento con requisitos legales y contractuales

La Subred Sur ESE velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: Oficina asesora jurídica y oficina de control interno

- La oficina asesora jurídica y la oficina de control interno deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Subred Sur ESE y relacionados con seguridad de la información.

Normas dirigidas a: Oficina sistemas de información TIC

- la oficina de sistemas de información TIC debe certificar que todo el software que se ejecuta en la Subred Sur ESE esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La oficina de sistemas de información TIC debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Subred Sur ESE para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Normas dirigidas a: Todos los usuarios

- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

7.38. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, ANONIMIZACION Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Subred Sur ESE a través de la oficina de control interno, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Subred Sur ESE, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la Subred Sur ESE, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Subred Sur ESE exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus colaboradores, estableciendo los controles necesarios para preservar aquella información que la Subred Sur ESE conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la Subred Sur ESE y no sea publicada, revelada o entregada a colaboradores o terceras partes sin autorización.

En cuanto al proceso de anonimización de datos personales es controlar el riesgo asociado de las personas naturales y jurídicas que brindan su información para fines estadísticos a las diferentes instituciones o personas naturales. De ahí surge el proceso o la implementación adecuada de la anonimización que busca controlar que dichos microdatos no sean utilizados para fines netamente estadísticos. Para lograr lo anterior, se debe tener en cuenta que el fin último de este es la utilidad de la información para los usuarios. Así, se procura mantener el aprovechamiento de los datos, intentando introducir el menor ruido posible en los resultados y de igual manera, protegiendo la privacidad de las fuentes de información de los pacientes.

El proceso de anonimización para poner a disposición de los usuarios las bases de datos anonimizadas de las operaciones estadísticas y de información de la Sub Red Sur ESE, a través de la oficina de Sistemas de Información – Tics, es necesario realizar procedimientos con el fin

de no ser detectadas las fuentes de información. Es por ello que el equipo de Sistemas de Información – Tics, realiza distintas técnicas bajo unos parámetros planteados para así, asegurar que la información difundida de los microdatos sea de calidad, optimizando los riesgos y la utilidad de los datos.

En tanto, que el objetivo es presentar los datos anonimizados en algunos informes institucionales, base de datos estadísticos y algunos documentos externos, y existe una baja probabilidad de detectar al informante y a su vez se preserva la calidad en los datos, asegurando ciertas propiedades estadísticas como el promedio y los totales.

Por medio de unas etapas definidas en la Sub Red Sur ESE:

a. Viabilidad: En esta etapa se determina la necesidad de proteger la confidencialidad, mediante la interpretación de una normativa que justifique las disposiciones de la privacidad de las fuentes. Se debe analizar las unidades estadísticas y variables. Se analizan las principales características y el uso de los datos, mediante la observación de la metodología de la encuesta y del formulario de recolección; como resultado se identifica la estructura de los datos y se examina la coherencia y consistencia de los microdatos. Además, se revisa la información sobre las necesidades de los usuarios y se priorizan. Al igual se decide el tipo de publicación a realizar de los microdatos, de acuerdo a las políticas de difusión establecidas y de las necesidades de los usuarios.

b. Riesgo: Se establecen las necesidades de riesgo de difusión que deben ser protegidos, el cual se realiza mediante una apreciación del método para identificar situaciones donde se presenten inseguridad. Se debe considerar una serie de escenarios potenciales que permitan detectar a determinada fuente y tomar medidas de prevención. Los escenarios describen la información disponible para el intruso y como este podría utilizar la información para identificar a un individuo o empresa, y define criterios realistas acerca de lo que el hacker puede saber sobre los encuestados. En este paso se determinan los cuasi-identificadores (variables disponibles a los usuarios que permitan la identificación indirecta de las unidades estadísticas) y la forma como se pueden usar dichas variables. Una fuente se encuentra insegura cuando se es capaz de diferenciarla del resto. El riesgo puede ser individual o global.

c. Ejecución de métodos: De acuerdo con la evaluación de los riesgos se determina si es necesario realizar la anonimización de los datos.

d. En esta etapa se realiza la aplicación de los métodos necesarios para la anonimización, obteniendo una nueva base de datos o informes con los microdatos protegidos.

e. Entrega del archivo o base de datos anonimizada: Es preciso describir los métodos utilizados de protección y de pérdida de información, con el fin de entender lo que ha cambiado o las limitaciones que se pueden presentar debido a la confidencialidad de los datos; además como buena práctica y para procesos futuros en la misma operación estadística y de otras. Este documento debe ser de uso interno, ya que, si el intruso conoce las técnicas realizadas, puede reversar la programación y encontrar determinadas fuentes de información de su interés.

Normas de privacidad y protección de datos personales

<u>Normas dirigidas a: Áreas que procesan datos personales</u>

- Las áreas que procesan datos personales de beneficiarios, colaboradores, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Subred Sur ESE.

- Las áreas que procesan datos personales de beneficiarios, colaboradores, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, colaboradores, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, colaboradores, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamientoo de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: Oficina de control interno

- La oficina de control interno debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, colaboradores, proveedores y demás terceros de la Subred Sur ESE de los cuales reciban y administre información.

Normas dirigidas a: Oficina sistemas de información TIC

- La oficina de sistemas de información TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, colaboradores, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a: Todos los usuarios

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la Subred Sur ESE o de sus colaboradores de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Normas dirigidas a: usuarios de los portales de la Subred Sur Ese

- Los usuarios de los portales de la Subred Sur ESE deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.
- Los usuarios de los portales de la Subred Sur ESE deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de La Subred Sur ESE.
- Los usuarios de los portales de la Subred Sur ESE deben aceptar el suministro de datos personales que pueda hacer la Subred Sur ESE a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.

7.39. ACTIVIDADES

Como respuesta a los requerimientos de la política digital y a lo establecido el decreto 1008 del 14 de junio de 2018 de MinTIC : "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" la ESE Subred Sur, utilizando la metodología definida por el MinTIC en las guías para la implementación del modelo de seguridad y privacidad de la información-MSPI que establece cinco fases a través de un ciclo de operación con objetivos, metas y actividades que a continuación se describen

Fuente. Guía Modelo de Seguridad y Privacidad de la Información – MinTIC

A. Crear el documento de autodiagnóstico de la entidad en la implementación de seguridad y privacidad de la información: La ESE Subred Sur realizara el diagnostico respectivo a partir de los lineamientos sugeridos por el MinTIC para su aplicación en todas las entidades públicas para el subsistema de Seguridad de la Información.

Producto a entregar: Documento Diagnostico y autoevaluación de la seguridad y privacidad de la información en la ESE Subred Sur.

B. Análisis de vulnerabilidades (Ethical Hacking) de la plataforma tecnológica de la entidad: Las pruebas de vulnerabilidades son importante para las organizaciones para poder proteger su seguridad de posibles ataques que perjudiquen dicha identidad. El proceso de localizar e informar las vulnerabilidades, proporcionan una forma de detectar y resolver el problema de seguridad clasificando las vulnerabilidades antes de que alguien o algo pueda explotarlas, ahorrándole a la entidad dueña del software tener una gran pérdida de dinero o de clientes.

Las pruebas de vulnerabilidad son técnicas empleadas para comprobar la seguridad de una entidad. Para obtener un resultado objetivo, las pruebas de vulnerabilidad se realizan por medio de servicios de consultoría especializados que utilizan metodologías y herramientas informáticas a través de las cuales se concretan de manera controlada pruebas de hacking, ingeniería social, identificación de vulnerabilidades de aplicaciones, servicios web, pruebas de acceso, entre otros con el fin de sustentar qué tan robusto es un control o tan informada y capacitados está el recurso humano con relación a la información a su cargo.

Es importante tener en cuenta que estas pruebas no tienen como objetivo identificar solamente una vulnerabilidad sobre un sistema específico o algún sistema desactualizado, sino que la meta principal es identificar los riesgos de seguridad de la información a través de los controles evaluados a través de las pruebas, para así tomar las medidas proactivas/preventivas para mitigar los riesgos encontrados.

Producto a entregar: Informe de los resultados del proceso y las recomendaciones a implementar.

C. Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación: Se realizara el seguimiento a cada uno de los indicadores establecidos para medir el porcentaje de cumplimiento de la política de seguridad de la información y el plan de continuidad del negocio, Se alimentara la herramienta con la información de las diferentes fuentes de información con que cuenta la oficina de informática.

Producto a entregar: Documento seguimiento cumplimiento política de seguridad de la información y BCP.

D. Formular, Implementar y actualizar los indicadores del SGSI: Esta acción contempla la construcción de indicadores que permitan tener una medición de la efectividad de los controles vigentes frente a la presencia de incidentes de seguridad, el conocimiento de los funcionarios, contratistas y terceros de las políticas y lineamientos de TI.

Producto a entregar: Matriz de indicadores de gestión de seguridad y privacidad de la información

E. Actualizar la matriz de activos de información: Esta actividad implica identificar e incluir en el inventario de activos de información todos aquellos elementos que aportan información y tienen valor para la institución, La ESE Subred Sur posee un inventario de información oficial cuya información fue recaudada en el año 2020. Se hará un proceso de identificación de nuevos elementos, la clasificación de los activos críticos y sensibles para la entidad, la valoración cuantitativa y cualitativa de los mismos. Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.

Producto a entregar: Inventario de Activos de Información Actualizado y aprobado

F. Actualizar el plan de continuidad de la operación de la Entidad (Plan de contingencia): Se revisará los documentos actuales del plan y se actualizarán de acuerdo a las disposiciones de bioseguridad que están impactando las labores misionales de la entidad, así como la creación de los nuevos procedimientos que sean necesarios para garantizar la continuidad del negocio en el evento que se materialice una amenaza planteada en el mapa de riesgos de la entidad.

Producto a entregar: Documento Plan de continuidad de la operación actualizado, procedimientos de recuperación, matriz de actores y sus responsabilidades actualizadas.

G. Seguimiento al cumplimiento de la ley 1712 de 2014 de Transparencia: Se realizará la revisión de los procedimientos establecidos por la ESE Subred Sur para tal el cumplimiento de la ley 1712 y se actualizara aquellos que han quedado obsoletos o ya no aplican, garantizando la transparencia del acceso a los datos públicos por parte de terceros

Producto a entregar: Documentos de procedimientos de seguridad y privacidad de la información creados y/o actualizados.

H. Solicitar la recolección de bases de datos personales de acuerdo a los estándares emitidos por la Superintendencia de Industria y Comercio: Se debe realizar un levantamiento de información de las bases de datos personales existentes en la Subred Sur E.S.E.

Entregable: Listado de bases de datos personales por área.

I. Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos: Se realizará el análisis de la información suministrada por las áreas de la Subred Sur E.S.E. y se depuraran aquellas que no cumplan con los requerimientos de la ley 1582 de 2012.

Entregable: Listado de bases de datos personales depurado.

J. Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de la información: Se procederá al registro ante la superintendencia de industria y comercio de las bases de datos personales de la Subred Sur E.S.E.

Entregable: Confirmación de registro de las bases de datos personales en la Superintendencia de Industria y Comercio.

7.40. SEGUIMIENTO Y CONTROL

Para el seguimiento y control de los planes de trabajo se realizará un informe de cumplimiento por cada una de las vigencias de los cronogramas planteados para cada uno de los planes y el análisis de las fichas de los indicadores propuestos.

7.5 LINEAMIENTOS DE SEGURIDAD EN LA NUBE

La Subred Sur ESE garantizará la protección de los datos e infraestructura alojada en servicios de computación en la nube, estableciendo controles y buenas prácticas para su administración segura. Se adoptarán políticas para la selección de proveedores, configuración segura de entornos cloud, cifrado de datos, gestión de accesos y monitoreo continuo de la seguridad en la nube.

Normas dirigidas a: Propietarios de los sistemas de información

- Los propietarios de los sistemas de información deben asegurarse de que cualquier implementación en la nube cumpla con las normativas de seguridad de la Subred Sur ESE y con estándares como **ISO/IEC 27017** (controles de seguridad para la nube) e **ISO/IEC 27018** (protección de datos personales en la nube).
- Los propietarios de los sistemas de información deben aprobar las configuraciones de seguridad en la nube antes de la puesta en producción, verificando que incluyan controles de acceso adecuados y cifrado de datos.
- Los propietarios de los sistemas de información deben validar que los servicios en la nube cuenten con un **Acuerdo de Nivel de Servicio (SLA)** que garantice disponibilidad, integridad y confidencialidad de la información.
- Los propietarios de los sistemas de información deben asegurarse de que los datos sensibles almacenados en la nube estén cifrados y protegidos contra accesos no autorizados.

Normas dirigidas a: Oficina de Sistemas de Información TIC

- La oficina de sistemas de información TIC debe seleccionar proveedores de servicios en la nube que cumplan con estándares internacionales de seguridad, como **ISO 27001, NIST CSF** o **SOC 2 Type II**.
- La oficina de sistemas de información TIC debe garantizar que toda comunicación entre sistemas locales y en la nube se realice a través de **canales seguros y cifrados** (TLS 1.2 o superior).

- La oficina de sistemas de información TIC debe implementar controles de **gestión de identidad y accesos (IAM)** para restringir el acceso a los recursos en la nube según el principio de **privilegios mínimos**.
- La oficina de sistemas de información TIC debe configurar mecanismos de **monitoreo y auditoría** en **los** servicios en la nube para detectar accesos indebidos o actividades sospechosas.
- La oficina de sistemas de información TIC debe establecer procedimientos para la **eliminación segura de datos en la nube**, asegurando que no queden accesibles tras la finalización del servicio con un proveedor.
- La oficina de sistemas de información TIC debe definir una política de **respaldo y recuperación de datos** en entornos cloud, garantizando la redundancia y disponibilidad de la información crítica.
- La oficina de sistemas de información TIC debe configurar alertas automáticas para notificar intentos de acceso no autorizado a recursos alojados en la nube.
- La oficina de sistemas de información TIC debe aplicar herramientas de **Prevención de Pérdida de Datos (DLP)** para evitar la fuga de información sensible en servicios cloud.

Normas dirigidas a: Usuarios finales y colaboradores

- Los usuarios deben utilizar únicamente servicios en la nube autorizados por la Subred Sur ESE y evitar el uso de plataformas no aprobadas para el almacenamiento de información corporativa.
- Los usuarios deben evitar el acceso a servicios en la nube desde redes públicas o dispositivos no autorizados.
- Los usuarios deben reportar de inmediato cualquier actividad sospechosa detectada en cuentas o sistemas en la nube de la Subred Sur ESE.
- Los usuarios deben cumplir con las políticas de uso de credenciales seguras y autenticación multifactor (MFA) al acceder a los servicios en la nube.

Normas dirigidas a: Oficina de Control Interno

- La oficina de control interno debe realizar auditorías periódicas sobre los servicios en la nube utilizados por la Subred Sur ESE, verificando su cumplimiento con las políticas de seguridad.
- La oficina de control interno debe supervisar la correcta aplicación de los controles de acceso, cifrado y monitoreo en las plataformas cloud.
- La oficina de control interno debe validar que los proveedores de servicios en la nube cumplan con los requisitos de seguridad establecidos en los contratos con la Subred Sur ESE.
- La oficina de control interno debe realizar evaluaciones de riesgo en la nube para identificar vulnerabilidades y proponer mejoras en la protección de los datos.

7.6 LINEAMIENTOS PARA EL USO SEGURO DE INTELIGENCIA ARTIFICIAL EN SEGURIDAD DE LA INFORMACIÓN

La Subred Sur ESE promoverá el uso seguro y responsable de la **Inteligencia Artificial (IA)** en la protección de la información, garantizando que las tecnologías emergentes no comprometan la confidencialidad, integridad y disponibilidad de los datos. Se establecerán políticas para la detección de amenazas mediante IA, automatización de respuestas a incidentes, análisis predictivo de riesgos y auditoría de decisiones automatizadas.

Normas dirigidas a: Propietarios de los sistemas de información

- Los propietarios de los sistemas de información deben asegurar que cualquier herramienta de IA implementada en la Subred Sur ESE cumpla con estándares de seguridad y privacidad, como los definidos en ISO/IEC 23894 (gestión de riesgos de IA).
- Los propietarios de los sistemas de información deben validar que los modelos de IA utilizados para la detección de amenazas o análisis de datos sean explicables, auditables y libres de sesgos discriminatorios.
- Los propietarios de los sistemas de información deben evaluar los riesgos asociados al uso de IA en la toma de decisiones, asegurando que existan mecanismos de validación humana cuando sea necesario.
- Los propietarios de los sistemas de información deben aprobar cualquier integración de IA en los sistemas de la Subred Sur ESE, verificando que no genere vulnerabilidades en la seguridad.

Normas dirigidas a: Oficina de Sistemas de Información TIC

- La oficina de sistemas de información TIC debe utilizar sistemas de IA para la detección de amenazas, tales como herramientas de análisis de comportamiento para la identificación de accesos no autorizados y ataques cibernéticos.
- La oficina de sistemas de información TIC debe implementar IA en la automatización de respuesta a incidentes, permitiendo bloquear actividades maliciosas en tiempo real sin intervención humana.
- La oficina de sistemas de información TIC debe garantizar que los datos utilizados para el entrenamiento de modelos de IA en seguridad sean anonimizados y protegidos contra accesos indebidos.
- La oficina de sistemas de información TIC debe utilizar algoritmos de IA para predecir **vulnerabilidades** y anticipar posibles ciberataques basándose en patrones históricos.
- La oficina de sistemas de información TIC debe verificar que los sistemas de IA aplicados en ciberseguridad se actualicen regularmente para evitar falsos positivos o negativos en la detección de amenazas.
- La oficina de sistemas de información TIC debe integrar auditorías en los sistemas de IA para garantizar la trazabilidad de sus decisiones y reducir el riesgo de automatización errónea.

Normas dirigidas a: Usuarios finales y colaboradores

- Los usuarios deben utilizar herramientas basadas en IA de acuerdo con las políticas definidas por la Subred Sur ESE y evitar el uso de aplicaciones de IA externas que no estén aprobadas.
- Los usuarios deben reportar cualquier decisión automatizada tomada por IA que genere dudas sobre su precisión o posible impacto negativo en la seguridad de la información.
- Los usuarios no deben compartir información confidencial con asistentes virtuales o herramientas de IA sin previa validación de seguridad.
- Los usuarios deben recibir capacitación sobre el **uso ético y seguro de la inteligencia artificial** en el manejo de la información institucional.

Normas dirigidas a: Oficina de Control Interno

- La oficina de control interno debe realizar auditorías regulares sobre los modelos de IA utilizados en seguridad, verificando su precisión y cumplimiento con normativas de privacidad.
- La oficina de control interno debe evaluar el impacto de la IA en la toma de decisiones dentro de la Subred Sur ESE, asegurando que no afecte los derechos de los usuarios.
- La oficina de control interno debe establecer mecanismos de revisión manual para las decisiones críticas generadas por IA, garantizando que no se produzcan errores por automatización.
- La oficina de control interno debe supervisar la transparencia y explicabilidad de los modelos de IA, verificando que puedan ser auditados en caso de incidentes de seguridad.

7.7 LINEAMIENTO DE USO DE APLICATIVOS NO INSTITUCIONALES

La Subred Sur E.S.E. promoverá el uso seguro y responsable de la información y de los recursos tecnológicos, incluyendo el acceso excepcional a aplicativos no institucionales (p. ej., WhatsApp Web, YouTube, Facebook, Instagram, X/Twitter, Telegram, páginas de IA u otros), cuando exista una necesidad del servicio debidamente justificada. Para estos casos, la habilitación solo procederá con el Formato de Solicitud y Responsabilidad de Uso de Aplicaciones No Institucionales diligenciado y firmado por el usuario y el Director del proceso, dejando explícitas las condiciones de uso, la vigencia y la aceptación de responsabilidades. El incumplimiento de estas condiciones podrá dar lugar a la revocatoria inmediata del permiso y a la aplicación de las medidas administrativas que correspondan, conforme a la Política de Seguridad y Privacidad de la Información y la normatividad aplicable.

Normas dirigidas a: directores de los procesos

- ✓ **Autorizar solo por excepción y necesidad del servicio**: El uso de aplicativos no institucionales no constituye un canal institucional; su autorización debe ser excepcional, justificada y limitada al propósito operativo declarado.
- ✓ **Diligenciamiento completo del formato**: El propietario del sistema/proceso debe garantizar que el formato incluya, como mínimo: proceso/área, tipo de vinculación, justificación, aplicativo, URL/detalle, tipo de permiso, vigencia (inicio/fin), equipo/activo (hostname/IP/ubicación) y tipo de información a gestionar, incluyendo si involucra datos personales y si requiere cargas/descargas.
- ✓ **Definición de alcance y restricciones:** Debe establecer por escrito las restricciones aplicables (p. ej., “solo consulta”, “sin descargas”, “sin envío de archivos”, “solo mensajería informativa”), y el alcance mínimo necesario para cumplir la actividad.
- ✓ **Prohibición de información no autorizada:** Debe impedirse la gestión de información clasificada, sensible, reservada o datos personales mediante aplicativos no institucionales, salvo que exista evaluación previa del riesgo, controles definidos por Seguridad Informática y autorización expresa en el formato.
- ✓ **Vigencia obligatoria y revisión periódica:** Toda autorización debe tener fecha de vencimiento; las renovaciones deben tramitarse mediante nuevo formato o actualización formal del existente, según el procedimiento definido.
- ✓ **Responsabilidad de proceso y aceptación del riesgo:** Al avalar la solicitud, el Director(a)/Líder del proceso reconoce el riesgo asociado y se compromete a aplicar medidas de control dentro del proceso (instrucciones al personal, supervisión del uso, verificación de cumplimiento).

- ✓ **Cambios de personal o función:** Ante cambio de usuario, traslado, vacaciones prolongadas o finalización del vínculo, el propietario del proceso debe solicitar revocatoria inmediata del acceso autorizado.
- ✓ **Gestión de incidentes**: Si se presenta un incidente (fuga, suplantación, exposición de datos, malware, contenido sospechoso), el propietario del proceso debe apoyar la contención (bloqueo, trazabilidad, entrega de evidencias) y liderar acciones correctivas en su área.

Normas dirigidas a: Oficina de Sistemas de Información TIC

- ✓ **Habilitación condicionada al formato firmado:** La habilitación técnica solo se realizará si el formato está completo, vigente y firmado por el usuario y el Director(a)/Líder del proceso, y si existe un ticket/caso asociado para trazabilidad.
- ✓ **Evaluación de riesgo previa (uso interno – Seguridad Informática):** Antes de habilitar, se debe clasificar el nivel de riesgo (bajo/medio/alto) considerando: tipo de aplicativo, exposición a Internet, necesidad de descargas/cargas, si incluye datos personales, y el activo desde el cual se usará.
- ✓ **Decisión y condiciones documentadas:** Se debe registrar la decisión (aprobar/denegar/aprobar con controles) y consignar condiciones/controles explícitos (p. ej., “solo URL específica”, “solo desde red institucional”, “sin adjuntos”, “MFA obligatorio”).
- ✓ **Principio de mínimo privilegio: Otorgar** únicamente el acceso estrictamente necesario: por URL, categoría, perfil, horario o ubicación, según sea viable técnica y operativamente.
- ✓ **Control de cargas/descargas:** Cuando el formato indique que requiere cargas/descargas, TIC deberá definir controles compensatorios (p. ej., bloqueo de descargas, restricciones por tipo de archivo, análisis antimalware, repositorio institucional para almacenamiento) o denegar si el riesgo es inaceptable.
- ✓ **Monitoreo y registros:** Mantener registros de navegación/acceso relacionados con la excepción (cuando sea posible) para fines de investigación y auditoría, conforme a los lineamientos de seguridad y privacidad.
- ✓ **Caducidad automática del permiso:** Implementar mecanismos para que el permiso expire en la fecha “vence el” definida, y asegurar la revocatoria al vencimiento o por instrucción de Seguridad Informática/Control Interno.
- ✓ **Configuración segura del endpoint:** Validar que el equipo/activo indicado cumpla condiciones mínimas (antimalware activo, parches vigentes, navegación segura, bloqueo de extensiones no autorizadas, etc.), de acuerdo con el estándar interno.
- ✓ **Restricción de bypass:** Está prohibido habilitar mecanismos que evadan controles institucionales (proxies no autorizados, VPNs no aprobadas, extensiones de evasión, webproxys).
- ✓ **Soporte y acompañamiento: TIC** debe orientar al usuario sobre las condiciones técnicas del permiso (qué está habilitado y qué no) y dejar evidencia en el caso/ticket.
- ✓ **Gestión de incidentes:** Ante eventos de seguridad asociados, TIC debe ejecutar acciones de contención (bloqueo, aislamiento, recolección de logs), en coordinación con Seguridad Informática.

Normas dirigidas a: Usuarios finales y colaboradores

- ✓ **Uso exclusivo para el fin autorizado**: El aplicativo no institucional solo podrá utilizarse para la finalidad aprobada en el formato. Cualquier uso diferente se considera no autorizado.
- ✓ **Uso únicamente en el activo aprobado**: El acceso se realizará únicamente desde el equipo/activo registrado (hostname/IP/ubicación). No se permite trasladar el uso a equipos personales o no inventariados.

- ✓ **Prohibición de compartir credenciales:** El usuario no debe compartir credenciales, sesiones, enlaces de acceso, códigos MFA o dispositivos asociados. Es responsable de toda acción realizada con su cuenta.
- ✓ **No gestionar información no permitida:** Está prohibido divulgar, transmitir, almacenar o procesar información institucional no autorizada por estos medios. En especial: datos personales, información clínica, información reservada/confidencial o documentación interna, salvo autorización expresa y controles definidos.
- ✓ **Condiciones sobre cargas/descargas:** Si el permiso no lo autoriza, el usuario no debe descargar ni cargar archivos. Si está autorizado, debe seguir los controles definidos (análisis antimalware, uso de repositorios institucionales, no almacenamiento local permanente, etc.).
- ✓ **Uso de cuentas institucionales cuando aplique:** Cuando sea viable, se deberá usar correo/cuentas institucionales; no se deben asociar cuentas personales para fines laborales sin autorización expresa.
- ✓ **No instalar complementos o software**: El usuario no debe instalar extensiones, clientes, complementos, "plugins" o aplicaciones asociadas sin aprobación de TIC.
- ✓ **Cuidado con enlaces y suplantación:** El usuario debe verificar dominios oficiales y evitar enlaces sospechosos. En mensajería/redes, está prohibido abrir adjuntos/enlaces dudosos o de origen desconocido.
- ✓ **Protección de la sesión:** Bloquear el equipo al ausentarse; no dejar sesiones abiertas; no permitir el acceso de terceros al puesto de trabajo.
- ✓ **Reporte inmediato de incidentes:** Cualquier sospecha de phishing, fuga, acceso no reconocido, malware o uso indebido debe reportarse de inmediato a Seguridad Informática y a la Mesa de Servicio.
- ✓ **Aceptación de consecuencias:** El usuario reconoce que el incumplimiento puede generar revocatoria del permiso y medidas administrativas conforme a la Política de Seguridad y Privacidad de la Información y la normatividad aplicable.

Normas dirigidas a: Oficina de Control Interno

- ✓ **Verificación de cumplimiento:** Incluir en auditorías y seguimientos la verificación del cumplimiento del lineamiento y del soporte documental: formato firmado, ticket asociado, vigencia, decisión de riesgo y controles definidos.
- ✓ **Revisión de trazabilidad de excepciones**: Validar que las excepciones (aplicativos no institucionales habilitados) cuenten con: justificación, responsables, activo autorizado, fecha de habilitación, fecha de vencimiento y evidencia de revocatoria cuando aplique.
- ✓ **Muestreo y pruebas de efectividad**: Realizar muestreos periódicos para confirmar que los accesos habilitados correspondan a permisos vigentes y que los controles definidos (restricciones, registros, caducidad) estén funcionando.
- ✓ **Gestión de hallazgos y planes de mejora:** En caso de incumplimientos, emitir hallazgos y solicitar planes de mejora con responsables, fechas y evidencia de cierre.
- ✓ **Seguimiento a incidentes relacionados:** Verificar que incidentes asociados a aplicativos no institucionales tengan gestión completa (contención, análisis, acciones correctivas y preventivas, lecciones aprendidas).
- ✓ **Recomendaciones de control:** Proponer ajustes a criterios de autorización (por ejemplo, restringir por tipo de información, prohibir descargas, limitar vigencias, exigir MFA, etc.) y elevar riesgos recurrentes a instancias de gobierno cuando corresponda.

8. BIBLIOGRAFÍA:

1. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional De Confianza Y Seguridad Digital, CONPES 3995 (01 de julio 2020)
2. INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES. Instrumento de identificación de la línea base de seguridad (09 de junio 2017)
3. ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI) (2013)

9. ANEXOS (Opcional):

- ANEXO 1. PLAN DE TRABAJO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN -2026

10. CONTROL DE CAMBIOS:

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
2017-08-08	1	Creación del documento para la Subred integrada de Servicios de Salud Sur E.S.E.
2018-07-27	2	Cambia de plantilla de Manual a Plan (Código anterior: GI-MA-01), de acuerdo a los requerimientos normativos.
2021-01-25	3	Actualización de normativa vigente y generación actividades para 2021.
2021-05-14	4	Actualización proceso de administración correo electrónico y formato de creación de usuarios
2021-11-29	5	Actualización de código (Anterior: GI-TICS-PP-02). Actualización de los lineamientos de seguridad de la información, anonimización y protección de datos personales.
2022-01-28	6	Inclusión de normatividad, objetivo, política Seguridad Digital
2023-01-30	7	Cambia de plantilla del Plan (Código anterior: MI-SIG-CDO-FT-7 V1), de acuerdo a los requerimientos normativos y se realiza actualización al documento.
2024-01-31	8	Se realiza ajuste general del documento.
2025-01-31	9	Actualización Normativa, lineamientos de seguridad en la nube y seguridad con inteligencia artificial
2026-01-30	10	Actualización de lineamiento de uso de aplicativos no institucionales

De conformidad con lo establecido en la Resolución 0295 de 13 de marzo de 2019, en sesión del Comité de Institucional Gestión y Desempeño de la Subred Integrada de Servicios de Salud Sur E.S.E. realizado el **28 de enero de 2026** se aprobó el presente Plan.

ELABORADO / MODIFCADO	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrés Felipe Cubillos García	**Nombre:** Julio Andrés Sánchez Sánchez	**Nombre**: Sandra Patricia Alba Calderón	**Nombre:** Viviana Marcela Clavijo / Julio Andrés Sánchez Sánchez
Cargo: Profesional Especializado Seguridad Informática	**Cargo** jefe Oficina Gestión de la Información - TIC	**Cargo:** Referente Control Documental – Oficina de Calidad	**Cargo**: Gerente / Jefe Oficina Gestión de la Información – TIC
Fecha: 2026-01-21	**Fecha:** 2026-01-21	**Fecha:** 2026-01-30	**Fech**a: 2026-01-30