"POR LA CUAL SE ACTUALIZA LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD DE LA EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA - E.S.E. ISABU"

EL GERENTE DE LA EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA ESE ISABU

En uso de sus facultades legales y reglamentarias y en especial las conferidas en el Acuerdo Municipal Nº 031 de 1997, Decreto No. 0097 del 24 de Marzo de 2020 y diligencia de posesión No. 0193 del 26 de Marzo del 2020

CONSIDERANDO

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

Que la Constitución Política de Colombia, en su artículo 209, establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley y, así mismo, en su artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que mediante la Ley 1273 de 2009 se creó un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos, tipificando penalmente las conductas contra la confidencialidad, la integridad, la disponibilidad de los datos y de los sistemas informáticos.

Que el Decreto número 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la seguridad y privacidad de la información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Dada la función establecida en el artículo 2.2.9.1.2.3 del Decreto número 1078 de 2015 para el representante legal de los sujetos obligados en relación con la coordinación de la implementación de la estrategia Gobierno en línea, la ESE ISABU creó en el año 2020 la Política de seguridad y privacidad de la información, la cual posteriormente fue actualizada mediante Resolución No.0565 del 12 de diciembre de 2022.

Con el objetivo de cumplir con las buenas prácticas corporativas de seguridad de la información emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en el Marco de Seguridad y Privacidad de la Información (MSPI), alineado con la norma NTC ISO 27001:2022 y su anexo A ISO 27002:2022 en su nueva actualización, se realizó la revisión anual de las políticas establecidas por la ESE ISABU concluyendo la necesidad de reestructurar las Políticas de seguridad de la Información de la Institución incorporando los marcos de referencia mencionados anteriormente, transformándolo con un enfoque centrado únicamente en seguridad de la información que abarque políticas de seguridad de la información, ciberseguridad y protección de la privacidad.

Que la ESE ISABU requiere actualizar la política de seguridad y privacidad de la información, con el propósito de garantizar coherencia con los retos y desafíos actuales en materia de seguridad de la información y protección de datos personales.

La ESE ISABU experimenta beneficios significativos al actualizar su política de seguridad de la información con la inclusión de nuevos apartados. Esta actualización no solo refuerza la base de la gestión de seguridad, sino que también aporta una mayor claridad y coherencia en la definición de objetivos, lineamientos y

responsabilidades. La adición de secciones como Declaración de compromiso, Principios de seguridad de la información y Roles y responsabilidades de la seguridad de la información proporciona un marco más completo y alineado con las mejores prácticas y estándares reconocidos. Además, la introducción de aspectos clave como la preservación digital, la gestión de riesgos y la concienciación refuerza la capacidad de la ESE ISABU para adaptarse a los desafíos contemporáneos en seguridad de la información, brindando así una mayor protección a los datos sensibles y mejorando la resiliencia ante posibles amenazas. En última instancia, estas adiciones contribuyen a una política más robusta y eficiente, respaldando la misión de la ESE ISABU de proporcionar servicios de salud de alta calidad de manera segura y confiable.

Que es necesario actualizar la politica de seguridad y privacidad de la información adoptando los apartados establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) consignando una "POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD ya que mediante este instrumento se determinaran los lineamientos que permiten proteger la Información de la ESE ISABU, a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos y de seguridad de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo, con el fin de asegurar el cumplimiento de la integridad, no repudio, disponibilidad, legalidad y confidencialidad de la información.

Por lo anteriormente expuesto,

RESUELVE

ARTÍCULO PRIMERO: Actualizar la politica de seguridad y privacidad de la información, para tal efecto, formará parte integral del presente acto administrativo y tendrá fuerza vinculante, el documento elaborado por la Oficina de Tecnologías de la información de la ESE ISABU denominado "POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD "

ARTICULO SEGUNDO: Incorporar en la politica de seguridad y privacidad de la información los apartados relevantes para la gestión de la seguridad de la información, los cuales incluyen adiciones en los siguientes capítulos: Objetivo, Lineamientos (5.2), Declaración de compromiso (5.3), Declaración de aprobación (5.4), Referencias y otros documentos (5.5), Principios de seguridad de la información (5.6), Privacidad de la información y protección de datos personales (5.7), Responsable (5.8), Contacto (5.9), Procedimiento para solicitar excepciones (5.10), Gestión de riesgos (5.11), Articulación de la preservación digital con la politica de seguridad de la información (5.13), Roles y responsabilidades de la seguridad de la información (5.14), Concienciación y formación (5.25), Monitorización y revisión (5.26), Mejora continua (5.27). Estas adiciones buscan fortalecer y actualizar el contenido del documento, abordando cada uno de los aspectos mencionados para garantizar una gestión integral y efectiva de la seguridad de la información.

ARTÍCULO CUARTO: La presente decisión rige a partir de la fecha de expedición y derogan las demás disposiciones que resulten contrarias.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bucaramanga, a los **veintiocho** (**28**) días del mes de noviembre de 2023.

GERMAN JESUS GOMEZ LIZARAZO
Gerente ESE ISABU

Elaboró: Jose Joaquin Salcedo Duran – Ingeniero de seguridad de la información

Revisó: William Figueroa Pineda – Coordinador Gestión de las TICS

Aprobó: William Figueroa Pineda – Coordinador Gestión de las TICS

POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** reconoce la importancia crítica de proteger la confidencialidad, integridad y disponibilidad de la información, tanto propia como de terceros, para garantizar la continuidad del negocio y la confianza de nuestros usuarios internos, externos y partes interesadas. Esta política de seguridad de la información, ciberseguridad y protección de la privacidad establece los principios, estándares y responsabilidades para proteger la información.

1. OBJETIVO

Establecer las políticas que regulan la seguridad de la información, ciberseguridad y protección de la privacidad en la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** y presentar en forma clara y coherente los elementos que deben conocer, acatar y cumplir todos los empleados, contratistas, proveedores y partes interesadas, con el fin de asegurar la confidencialidad, disponibilidad e integridad de la información de la entidad.

1.1. OBJETIVOS ESPECÍFICOS

- Realizar una adecuada gestión a los riesgos de seguridad de la información, ciberseguridad y protección de la privacidad, para garantizar la confidencialidad, integridad y disponibilidad de los activos de información, mediante la implementación de los lineamientos establecidos para ello.

- Garantizar la protección adecuada de todos los activos de información críticos de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** mediante la implementación de controles de seguridad efectivos, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información, minimizando así los riesgos asociados a su manipulación, acceso y divulgación no autorizados.

- Capacitar y sensibilizar al personal de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** en temas relacionados con seguridad de la información, ciberseguridad y protección de la privacidad buscando un aumento progresivo en la cultura de la seguridad de la información al interior de la compañía.

- Mejorar continuamente el desempeño del Sistema de Gestión de seguridad de la información mediante la implementación de acciones correctivas y de mejoras eficaces que se generen como resultado de las auditorías internas y externas.

- Gestionar de manera adecuada los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la posibilidad o el impacto de incidentes futuros.

- Dar cumplimiento a los requisitos legales, regulatorios, contractuales y otros suscritos y vigentes aplicables a las operaciones de Visión.

2. ALCANCE

La presente política contiene los lineamientos y las directrices de seguridad de la información que tienen como propósito garantizar la confidencialidad, integridad y disponibilidad de los activos de información gestionados por todos los procesos, razón por lo cual son de obligatorio cumplimiento por parte de todas los empleados, contratistas, proveedores y partes interesadas que generen, accedan o utilicen información de la Entidad.

3. RESPONSABLE

Proceso de Gestión de las Tics - en dirección de su Oficial de seguridad y protección de Datos personales. Así como sus colaboradores y toda persona que tenga acceso a la información de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA**

4. DEFINICIONES

- Acceso Autorizado: Obtener permisos o derechos adecuados para ver o utilizar información de acuerdo con las políticas establecidas.
- Auditoría: La revisión y evaluación sistemática de los procedimientos, controles y actividades para garantizar el cumplimiento de políticas y normas de seguridad.
- Biometría: La medición y análisis de características físicas o comportamentales únicas de individuos, como huellas dactilares o patrones faciales, utilizadas para autenticación.
- Ciberataque: Un intento malicioso de comprometer la seguridad informática, ya sea accediendo, dañando o robando información.
- Ciberseguridad: El conjunto de prácticas, procesos y tecnologías diseñadas para proteger sistemas, redes y datos contra amenazas digitales.
- Confidencialidad: Garantizar que la información sensible se mantenga privada y solo sea accesible por aquellos autorizados.
- Criptografía: El estudio y la aplicación de técnicas para asegurar la comunicación y la información mediante el uso de códigos y algoritmos.
- Datos Sensibles: Información que, si se divulga o se accede de manera no autorizada, podría causar daño significativo a los individuos o a la organización.
- Disponibilidad: Garantizar que la información y los recursos estén disponibles cuando se necesiten, evitando interrupciones no planificadas.
- Firewall: Una barrera de seguridad que monitorea y controla el tráfico de red para prevenir accesos no autorizados.
- Gestión de Identidad: El conjunto de políticas y tecnologías utilizadas para gestionar y garantizar la identificación segura de usuarios y dispositivos.
- Hackeo Ético: La práctica autorizada de pruebas de penetración y evaluación de seguridad para identificar y corregir vulnerabilidades en sistemas y redes.
- Incidente de Seguridad: Un evento que compromete la confidencialidad, integridad o disponibilidad de la información y que puede requerir una respuesta de seguridad.
- Inclusión: Garantizar que todas las personas tengan acceso equitativo y se beneficien de los recursos y oportunidades, sin importar sus diferencias.
- Ingeniería Social: El uso de tácticas psicológicas para engañar a las personas y obtener información confidencial o acceso no autorizado a sistemas.
- Malware: Software malicioso diseñado para dañar, infectar o tomar control de sistemas y dispositivos.
- Nube: Un entorno de almacenamiento y procesamiento de datos en línea, accesible a través de internet, que proporciona recursos informáticos según demanda.
- Phishing: Un tipo de ataque cibernético en el que se engaña a las personas para que revelen información confidencial, generalmente a través de correos electrónicos falsos.
- Privacidad: La protección de la información personal, garantizando que se maneje de manera ética y segura.
- Ransomware: Un tipo de malware que cifra archivos o sistemas, exigiendo un rescate para restaurar el acceso.
- Red Privada Virtual (VPN): Una conexión segura que permite a los usuarios acceder a una red privada a través de internet, protegiendo la comunicación contra amenazas.
- Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto no deseado.
- Seguridad de la Información: El conjunto de medidas y políticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información.

- Seguridad Informática: La práctica de proteger sistemas y datos contra amenazas cibernéticas, incluyendo el uso de medidas preventivas y correctivas.
- Seguridad Física: Medidas para proteger los recursos físicos de una organización, como servidores y centros de datos, contra daños o accesos no autorizados.
- Seguridad Operativa (OpSec): Prácticas y procesos para salvaguardar la información al controlar la exposición de datos y minimizar los riesgos operativos.
- Two-Factor Authentication (2FA): Un método de autenticación que requiere dos formas diferentes de verificación, como una contraseña y un código enviado a un dispositivo móvil.
- Usabilidad Segura: La integración de medidas de seguridad sin comprometer la facilidad de uso y accesibilidad del sistema.
- Vulnerabilidad: Una debilidad en un sistema que podría ser explotada para comprometer la seguridad.
- Whitelisting: Permitir solo el acceso a sistemas y aplicaciones a partir de una lista predefinida de elementos aprobados.
- Zero-Day: Una vulnerabilidad de seguridad que es explotada antes de que los desarrolladores tengan la oportunidad de solucionarla o emitir parches.
- Zero Trust: Un enfoque de seguridad que desconfía de cualquier entidad, incluso aquellas dentro del perímetro de la red, y requiere autenticación continua.

5. DESAROLLO

5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

5.2. LINEAMIENTOS

Las políticas y directrices contenidas en este documento se encuentran organizadas de acuerdo con las cláusulas de control presentadas en el documento GTC - ISO/IEC 27002:2022

5.3. DECLARACIÓN DE COMPROMISO

La alta dirección de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** está comprometida con la protección de la información de la organización contra la pérdida, el acceso no autorizado, la divulgación, la modificación o la destrucción. La organización ha implementado un sistema de gestión de seguridad de la información (SGSI) para cumplir con este compromiso.

5.4. DECLARACIÓN DE APROBACIÓN

La alta Dirección, declara que las políticas de seguridad de la información, ciberseguridad y protección de la privacidad buscan la disminución, a un nivel aceptable de los riesgos a los que está expuesta la información de la organización y que están alineadas con la misión y visión que tiene la entidad para con sus clientes.

Declara además, que el documento de políticas de seguridad de la información, ciberseguridad y protección de la privacidad entra en vigor a partir del 25 de noviembre de 2020 y que es de obligatorio cumplimiento para todos los funcionarios de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA**, contratistas, proveedores, consultores y cualquier otro tipo de terceros que desempeñen funciones en las oficinas de la entidad o en cualquier modalidad y/o que el desempeño de sus labores esté relacionado con activos de información de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA.**

Esta política se divulgará y/o dará a conocer a empleados, contratistas, proveedores y consultores y se contraerán acuerdos que obliguen al cumplimiento de ésta.

5.5. REFERENCIAS Y OTROS DOCUMENTOS

MARCO NORMATIVO	VERSION	TITULO	RESPONSABLE DEL ANALISIS	FRECUENCIA DE REVISION
NTC – ISO/IEC 27001	2022	Seguridad de la información, ciberseguridad y protección de la privacidad	Oficial de Seguridad de la información	Cuando se generen cambios en el estándar
GTC – ISO/IEC 27002	2022	Controles de seguridad de la Información	Oficial de Seguridad de la información	Cuando se generen cambios en el estándar
Ley 1581 de 2012	2012	Ley de protección de datos personales	Oficial de Seguridad de la información	Cuando se generen cambios en la ley
Guía de responsabilidad demostrada	2013	Guía de responsabilidad demostrada	Oficial de Seguridad de la información	Cuando se generen cambios en guía
Decreto 1377	2013	reglamentar parcialmente la Ley 1581 de 2012,	Oficial de Seguridad de la información	Cuando se generen cambios
Ley 1273	2009	Ley de delito informático	Oficial de Seguridad de la información	Cuando se generen cambios en la ley
LEY 23	1982	Ley de Derechos de Autor	Oficial de Seguridad de la información	Cuando se generen cambios en la ley
DECRETO 2693. Disponible en Línea:	2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones	Oficial de Seguridad de la información	Cuando se generen cambios en la ley

5.6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA.** se compromete a:

- Confidencialidad: Proteger la información de divulgaciones no autorizadas o no intencionadas.
- Integridad: Mantener la precisión y confiabilidad de la información.
- Disponibilidad: Garantizar que la información y los sistemas de información estén disponibles cuando sea necesario.
- Cumplimiento Legal y Regulatorio: Cumplir con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información.

5.7. PRIVACIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

Dando cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a sus Decreto Reglamentarios, La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** adopta una política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de las actividades comerciales o laborales.

De esta manera, La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** manifiesta que garantiza los derechos de la disponibilidad, privacidad, la intimidad, el buen nombre y la autonomía organizacional, en el tratamiento de los datos personales, y en consecuencia todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Todas las personas que en desarrollo de diferentes actividades contractuales, comerciales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar a La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.

5.8. RESPONSABLE

El Oficial de seguridad de la información y la alta dirección la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA**, vela por el cumplimiento del Sistema de Gestión de Seguridad de la Información; y sus políticas de seguridad de la información, así como de su vigencia, pertinencia, mantenimiento y divulgación dentro de la organización.

5.9. CONTACTO

En caso de tener alguna duda u observación con respecto al presente documento debe comunicarse con el responsable del Sistema de Gestión de Seguridad de la Información al E-mail: seguridad.informatica@isabu.gov.co.

5.10. PROCEDIMIENTO PARA SOLICITAR EXCEPCIONES

Si usted es un funcionario de la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** o tiene alguna relación con la entidad y encuentra alguna excepción o situación particular en la cual se dificulte o se imposibilite el cumplimiento de alguna política de seguridad de la información, ciberseguridad o protección de la privacidad de manera temporal o definitiva por causas naturales, humanas o económicas, puede solicitar una excepción temporal o definitiva para el cumplimiento de dicha política según el siguiente Instructivo:

Deberá enviar un correo electrónico documentando el caso completo y el porqué de la excepción al oficial de seguridad de la información el cual realizará el debido trámite con la alta dirección. Esta solicitud debe incluir:

- Su nombre y apellido
- Número de cédula
- Empresa donde labora
- Relación con la EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA
- Cargo o labor que desempeña
- Dependencia a la cual pertenece
- Lugar en donde lleva a cabo su labor
- Política en la cual ocurre la excepción
- Motivo de la excepción
- Fecha de solicitud de la excepción

Se le dará repuesta a su solicitud en un plazo no mayor a 30 días hábiles.

5.11. GESTIÓN DE RIESGOS

La EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA realizará evaluaciones de riesgos de seguridad de la información periódicamente para identificar amenazas y vulnerabilidades. Se implementarán controles adecuados para mitigar los riesgos identificados.

5.12. POLÍTICA GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La ESE ISABU. decide definir, implementar, operar y mejorar de forma continua una políticade Seguridad de la Información, soportada en lineamientos claros alineados con la misión,visión y funciones de la Institución.

Para el tratamiento de la información de los usuarios, así como la información de los colaboradores que participan en el desarrollo de las funciones, el instituto de salud de Bucaramanga cuenta con la "Política de Protección de Datos Personales" con la cual se da cumplimiento a lo dispuesto en la Ley 1581 de 2012, reglamentada por el Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto número 1074 de 2015, la Ley 1712 de 2014, y Decreto número 1008 de 2018, y las demás normas que los modifiquen, adicionen o complementen

La ESE ISABU, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites del instituto, identificando y mitigando los riesgos asociados mediantela definición de lineamientos y directrices a las dependencias, funcionarios, contratistas, practicantes y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su

gestión y resguardo.

Toda la información que es generada por los funcionarios, contratistas y practicantes de LaESE ISABU. en beneficio y desarrollo de las actividades propias del Instituto es propiedad de La ESE ISABU a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución.

La ESE ISABU, protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej. Contratistas, proveedores o ciudadanos), o como resultado de servicios internos en outsourcing.

La ESE ISABU. protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

LA ESE ISABU, protege su información de las amenazas originadas por parte de sus funcionarios, contratistas, practicantes y usuarios.

La ESE ISABU. protege las instalaciones de procesamiento y la infraestructura tecnológicaque soporta sus procesos críticos.

LA ESE ISABU controla la operación de sus procesos de operación garantizando la seguridad de los recursos tecnológicos, redes y bases de datos.

LA ESE ISABU implementa control de acceso a la información, aplicativos, recursos de red,portales y sistemas de información internos y externos o con accesos remotos

La ESE ISABU. garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La ESE ISABU. garantiza a través de una adecuada gestión de los eventos de seguridad ylas debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La ESE ISABU. garantiza la disponibilidad de sus procesos de operación y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La ESE ISABU. garantiza el cumplimiento de las obligaciones legales, regulatorias contractuales establecidas. Las responsabilidades frente a la seguridad de la información del Instituto son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes del Instituto.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad de la información siempre y cuando no sea contrario a lo expresado en esta política.

5.13. ARTICULACIÓN DE LA PRESERVACIÓN DIGITAL CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La ejecución de las diferentes estrategias para preservar los documentos electrónicos requiere del cumplimiento de las políticas de seguridad, de manera que se garantice la seguridad de la información específicamente en las siguientes acciones:

- Ejecutar procesos para la toma de copias de seguridad
- Controlar el acceso no autorizado
- Verificar la fiabilidad del software y hardware
- Detectar y neutralizar el ataque de virus o hackers
- Prever contingencias
- Identificar personal responsable de acceder a la información por cada dependencia.
- Sensibilización de los usuarios sobre el uso apropiado de contraseñas.

Así mismo, clasificar la información generada en la ESE-ISABU, según los establecido en el Esquema de Clasificación, el Índice de Información Clasificada y Reservada, y los niveles de acceso definidos en la Ley 1712 de 2014 (Público, Reservado y Clasificado) y adoptados en las Tablas de Retención Documental para las series y/o subseries documentales. De acuerdo a la Norma ISO 27000, que establece el modelo de referencia a la definición e implementación de un sistema de seguridad de información. Esta norma establece las políticas para

el análisis, la detección y la posible solución de riesgos de tipo informático en un determinado sistema de información y están ligadas al ámbito de la gestión de documentos con acciones cuyo enfoque de aplicación se centra en el presente y corto plazo.

Algunos controles implementados en materia de seguridad de la información y están relacionadas con la preservación digital, lo cual se relacionan a continuación:

- Seguridad organizacional.
- Desarrollo y mantenimiento de sistemas
- Control de acceso
- Seguridad del Personal
- Clasificación y control de activos

Los jefes de cada área podrán delegar el personal que tenga acceso a la información digital, adoptando las medidas que correspondan en materia de seguridad.

5.14. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN.

En la era digital en la que vivimos, la seguridad de la información se ha convertido en un aspecto fundamental para proteger los activos y datos sensibles de las organizaciones. La creciente cantidad de amenazas cibernéticas y las regulaciones de privacidad cada vez más estrictas han generado la necesidad de implementar un modelo de seguridad y privacidad de la información (MSPI). En este contexto, el establecimiento de roles y responsabilidades claros y bien definidos se vuelve crucial para garantizar el cumplimiento de dicho modelo.
En esta introducción, exploraremos las razones por las cuales es necesario implementar roles y responsabilidades en seguridad de la información, y cómo contribuyen a cumplir con un modelo de seguridad y privacidad efectivo. Los roles y responsabilidades adecuadamente definidos no solo permiten asignar las tareas y funciones necesarias, sino que también fomentan la responsabilidad individual y colectiva en la protección de la información sensible.

A medida que avanzamos hacia una sociedad cada vez más conectada, las organizaciones enfrentan constantemente riesgos y desafíos en términos de seguridad y privacidad de la información. Las amenazas cibernéticas, como el robo de datos, el malware y los ataques de phishing, pueden tener un impacto significativo en la confidencialidad, integridad y disponibilidad de la información. Además, la adopción de regulaciones y leyes de privacidad, ha impuesto obligaciones legales más estrictas para garantizar la protección de los datos personales. En este sentido, la implementación de roles y responsabilidades en seguridad de la información se convierte en una práctica esencial para gestionar eficazmente estos riesgos y cumplir con las regulaciones.
Al establecer roles y responsabilidades claros, las organizaciones pueden asignar tareas y autoridad adecuadas a los profesionales responsables de la seguridad de la información. Esto permite una mejor gestión de los riesgos, una respuesta más rápida y eficiente a los incidentes de seguridad y una protección más efectiva de la información. Además, promueve la conciencia y la cultura de seguridad en todos los niveles de la organización, ya que cada miembro comprende su papel y contribución para mantener la confidencialidad, integridad y disponibilidad de la información.

ROL	RESPONSABILIDADES
Alta dirección	• Asignar los recursos financieros, humanos y tecnológicos necesarios para implementar y mantener un modelo de seguridad y privacidad de la información efectivo. Esto incluye la inversión en tecnologías de seguridad, la capacitación del personal y la contratación de expertos en seguridad de la información. • Definir y asignar los roles y responsabilidades dentro de la organización en relación con la seguridad de la información. Esto implica designar a un responsable de seguridad de la información y establecer otros roles relevantes.
Coordinador de sistemas	• Liderar la estrategia y planificación de TI • Realizar la gestión de Proyectos de TI • Liderar la gestión de los servicios de TI • Garantizar gobierno y cumplimiento de TI en todo el marco normativo • Aprobar la gestión de Riesgos y Continuidad del Negocio de TI
Profesional especializado en seguridad de la información, seguridad digital, y oficial de protección de datos personales.	• Liderar la implementación del Sistema de gestión de seguridad de la información basado en el Modelo de seguridad y privacidad de la información en la entidad. • Fomentar la implementación de la Política de seguridad de la información.

ROL	RESPONSABILIDADES
	• Asesorar a la entidad en el diseño, implementación y mantenimiento del Sistema de gestión de seguridad de la información basado en el Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente. • Realizar la estimación, planificación y cronograma de la implementación del Sistema de gestión de seguridad de la información basado en el Modelo de Seguridad y privacidad de la Información MSPI. • Liderar la implementación y hacer seguimiento a las tareas y cronograma definido. • Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del Sistema de gestión de seguridad de la información y el Modelo de Seguridad y privacidad de la Información MSPI. • De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información. • Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia. • Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información. • Definir e implementar en coordinación con las dependencias de la entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para toda la organización. • Apoyar a los procesos de la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. • Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad. • Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información. • Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente. • Definir las herramientas, metodologías y lineamientos necesarios para la implementación del Sistema de gestión de seguridad de la información basado en el Modelo de Seguridad y Privacidad de la Información. • Realizar seguimiento a los objetivos planteados frente al Sistema de Gestión de Seguridad de la Información y Modelo de Seguridad y Privacidad de la Información, para detectar desviaciones y tomar las acciones correctivas necesarias. • Realizar la clasificación y valorización de los activos de información y revisarla como mínimo anualmente para garantizar que corresponde a los requisitos legales, normativos, contractuales y de la entidad. • Revisar y gestionar para que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso. • Realizar registro nacional de base de datos para dar cumplimiento a la ley 1581 e 2012.
Líder de infraestructura	• Coordinar, supervisar y asegurar la correcta operación y funcionamiento de la infraestructura y servicios tecnológicos. • Diseñar estrategias que incorporen las tendencias y cambios tecnológicos que sean pertinentes con los objetivos misionales de la entidad. • Implementar y mantener controles de seguridad en la infraestructura tecnológica de la organización. Esto implica configurar y administrar firewalls, sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y otros mecanismos de seguridad para proteger los sistemas y datos de la organización. • Establecer y mantener políticas y procedimientos para la gestión de accesos y privilegios en los sistemas de la infraestructura. Esto incluye garantizar que solo los usuarios autorizados tengan acceso a los recursos, implementar autenticación y control de acceso adecuados, y gestionar los privilegios de usuario para minimizar los riesgos de seguridad. • Establecer sistemas y procedimientos de monitoreo y detección de amenazas en la infraestructura tecnológica. Esto implica implementar soluciones de monitoreo de seguridad, analizar registros y alertas para identificar posibles incidentes de seguridad, y tomar medidas adecuadas para mitigar las amenazas detectadas. • Coordinar y participar en la respuesta a incidentes de seguridad. • Asegurar que la infraestructura tecnológica cumpla con los requisitos normativos y regulatorios en materia de seguridad de la información. Esto implica mantenerse actualizado sobre las leyes y regulaciones aplicables, asegurar la implementación de controles y medidas adecuadas para cumplir con los requisitos legales, y participar en auditorías de seguridad y cumplimiento normativo.

ROL	RESPONSABILIDADES
Líder de sistema de información	• Planificar, implementar y gestionar los sistemas de información de la entidad. Esto implica identificar las necesidades tecnológicas de la empresa, seleccionar y adquirir sistemas adecuados, y garantizar su correcta configuración, integración y funcionamiento. • Asegurar la seguridad de los sistemas de información de la entidad. • Asegurar la disponibilidad, integridad y confidencialidad de los datos almacenados, así como establecer políticas y procedimientos para el respaldo, la recuperación y el archivado de la información. • Coordinar proyectos de tecnología de la información dentro de la organización. Esto incluye la planificación, ejecución y seguimiento de proyectos relacionados con sistemas de información, infraestructura tecnológica, aplicaciones o mejoras tecnológicas, asegurando el cumplimiento de plazos, presupuestos y objetivos. • Brindar soporte técnico y resolver problemas relacionados con los sistemas de información. Esto implica atender las consultas y solicitudes de los usuarios, diagnosticar y solucionar fallas o incidentes técnicos, y mantener un alto nivel de disponibilidad y rendimiento de los sistemas. • Mantener y actualizar los sistemas de información de la organización. Esto implica aplicar parches de seguridad, actualizaciones de software y firmware, y gestionar las licencias de los sistemas. Además, debe evaluar y recomendar nuevas tecnologías y soluciones que puedan mejorar la eficiencia y la seguridad de los sistemas existentes. • Gestionar las relaciones con los proveedores de servicios y productos de tecnología de la información. Esto implica negociar contratos favorables, supervisar el cumplimiento de los acuerdos, evaluar y seleccionar proveedores confiables, y garantizar que se cumplan los niveles de servicio acordados.
Usuarios, contratistas, proveedores y practicantes.	• Cumplir con las políticas, lineamientos y procedimientos de seguridad de la información. • Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos. • Utilizar la información de la entidad únicamente para los propósitos autorizados. • Participar en los entrenamientos, capacitación y programas de sensibilización en temas de seguridad de la información. • Reportar cualquier incidente, potencial incidente u oportunidades de mejora de seguridad de la información. • No divulgar o utilizar información contenida en los sistemas, plataformas, aplicativos y otros recursos informáticos que se hayan facilitado en un entorno de trabajo remoto, presencial o mixto, para propósitos ajenos a sus funciones; realizando una adecuada utilización y manteniendo la debida confidencialidad y protección de datos. • Valorar y clasificar la información que está bajo su administración y/o generación. • Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información. • Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes. Determinar y evaluar de forma permanente los riesgos asociados a la información así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma. • Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 o Contrato. • Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio. • Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido • Evitar la divulgación no autorizada o el uso indebido de la información. • Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma. • Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas. • Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico- científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al instituto a la red Institucional ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Tecnologías de la Información. • Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de

ROL	RESPONSABILIDADES
	sus superiores y visto bueno de la Oficina de Tecnologías de la Información. • Conocer y cumplir las políticas de seguridad de la información establecidas dentro de la red del ESE ISABU. • Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General del Instituto puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del Instituto, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales. • Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución. La ESE ISABU no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito. • Y otros lineamientos descritos en las políticas de la entidad.

5.15. LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.15.1. USO DE USUARIOS Y CONTRASEÑAS

La asignación de usuarios y contraseñas es un permiso que La ESE ISABU. otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional. Estos usuarios serán creados en el Controlador de Dominio que se tiene para la entidad.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

- Presentar a todos los funcionarios y contratistas de La ESE ISABU. responsables de la asignación, creación y modificación de usuarios y contraseñas las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de La ESE ISABU.
- Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.
- La asignación de credenciales: usuarios (Login o UserId) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes, así como su desactivación de los sistemas se harán de acuerdo con los procedimientos establecidos y según sea solicitado por los directores, jefes de oficina o por los procesos de Talento Humano y Gestión Jurídica.
- Las cuentas de usuario son entera responsabilidad del funcionario, contratista o practicante al que se le asigne. La cuenta es para uso personal e intransferible.
- Las cuentas de usuario (usuario y clave) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan.
- De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido al Grupo de Sistemas.

Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración de la Oficina de Sistemas

5.15.2. TIPOS DE CUENTAS DE USUARIO

Todas las cuentas de acceso a las plataformas tecnológicas como a los sistemas de información y aplicaciones son propiedad de la Institución. Para efectos del presente lineamiento, se definen dos tipos de cuentas:

a. Cuenta de Usuario de Sistema de Información:

- Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular, ejemplo CNT.
- Se debe diligenciar el formato de solicitud por parte del personal administrativo del nivel directivo responsable del área al cual va a pertenecer el usuario al cual se le solicita el usuario y la contraseña en el sistema de información
- Se define como obligatorio para Médicos, Enfermeras, auxiliares de enfermería, odontólogos, especialistas, Fisioterapeutas y Personal administrativo que tiene el Rol de Utilización del Sistema de información en los módulos tales como Contabilidad, Nomina, Presupuesto, cuentas por Pagar, Cartera, Facturación, nomina la participación en capacitación en el sistema de información PANACEA, quienes no asisten a esta capacitación NO RECIBEN USUARIO NI CONTRASEÑA del sistema. Esto con el fin de garantizar la calidad de los datos que estos profesionales ingresan en el sistema.
- El procedimiento para las modificaciones a la base de datos de CNT, el cual inicia con una solicitud mediante el formato solicitud modificación en CNT[37], el cual debe ir diligenciado por la persona que realiza la solicitud de cambio y donde se debe explicar claramente QUE SUCEDIÓ, EN QUE PROCESO Y CUALES DATOS REQUIEREN QUE
- SE MODIFIQUEN. Además de explicar el porqué de la solicitud. (Motivo). Este formato además debe ir aprobado por el personal directivo de quien depende el área solicitante

b. Cuenta de Administración de Sistema de Información:

Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte del Grupo de Soporte Tecnológico y/o la Oficina de Tecnologías de la Información.

El Jefe de la oficina de Tecnologías de la Información deberá contar con la lista de las contraseñas sensibles para la administración de los sistemas de información, plataformas tecnológicas y bases de datos. Esto resguardado bien sea en caja fuerte interna o en proveedor externo de custodia y protección de copias de seguridad.

Estas cuentas de usuario igualmente deben mantener las siguientes políticas

- Todas las contraseñas de usuarios administradores deben ser cambiadas al menos cada90 días.
- Todas las contraseñas deben ser tratadas con carácter confidencial.
- Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería belectrónica instantánea ni vía telefónica.
- Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente deotros.
- Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.
- Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
- Se evitará el activar o hacer uso de la utilidad de recordar clave o recordarPassword de las aplicaciones.

5.15.3. USO APROPIADO DE USUARIOS Y CONTRASEÑAS

- Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente parafines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
- Cambiar periódicamente las contraseñas de los sistemas de información o serviciotecnológicos autorizados.

5.15.4. USO INDEBIDO DEL SERVICIO DE USUARIOS Y CONTRASEÑAS

- Permitir el conocimiento de las claves a terceros.
- Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documentogenerado deberá ser único y bajo resguardo.
- Almacenar las credenciales sin protección, en sistemas electrónicos personales (Tablets, memorias USB, teléfonos celulares, agendas electrónicas, etc.).
- Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
- Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
- Utilizar su usuario y contraseña para propósitos comerciales ajenos al Instituto.
- Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de La ESE ISABU.

5.15.5. RESPONSABILIDADES DE LOS FUNCIONARIOS, CONTRATISTAS Y PRACTICANTES CON USUARIOS Y CONTRASEÑAS ASIGNADOS

- Conocer, adoptar y acatar este lineamiento.
- Velar por la seguridad de la información a la que tenga acceso a través de las credenciales asignadas y a los sistemas de información autorizados para su acceso.
- Cerrar totalmente su sesión de trabajo para evitar el uso de su identidad, cuando se retire del equipo en que se encuentre laborando.
- Dar aviso al Grupo de Soporte Tecnológico, a través de los medios establecidos, de cualquier fallo de seguridad, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

5.16. MONITOREO DE INFRAESTRUCTURA Y SISTEMAS DE INFORMACIÓN

- Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.
- La Oficina de Tecnología podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.

5.17. ACUERDOS DE CONFIDENCIALIDAD

Todos los colaboradores, contratistas y/o proveedores de servicio deben aceptar los acuerdos de confidencialidad definidos por EL ISABU, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del ISABU a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

5.18. CONTROL DE ACCESO

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del ISABU, debe ser asignado de acuerdo con la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica del ISABU asignaran los accesos a plataformas, usuarios y segmentos de red de acuerdo con procesos formales de autorización los cuales deben ser revisados de manera periódica por el área responsable.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios e implementada por el área de Sistemas.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información del ISABU, sea por Internet, o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

El ISABU brinda tecnologías de acceso por VPN para que funcionarios, o algunos usuarios externos puedan ingresar a las plataformas y aplicativos remotamente.

Para conceder el acceso mediante cliente VPN el funcionario o usuario externo debe diligenciar el formato de solicitud para la creación de usuarios, donde se especifica la razón por la cual requiere el acceso, a que servidores y/o aplicativos, y el periodo de tiempo requeridos. Una vez el formato es aprobado por el área de Sistemas, se configura el acceso y se envían las credenciales para realizar las pruebas respectivas.

El acceso a la VPN se deberá realizar con el aplicativo cliente de la página del cliente web del fabricante del dispositivo Firewall de seguridad perimetral en su última versión y con el formato para la configuración enviado por el área de Sistemas.

Todos los funcionarios deberán contar con perfiles y credenciales de acceso a las diferentes plataformas, portales y aplicativos ejecutados sobre la infraestructura del ISABU.

5.19. BLOQUEO DE PANTALLAS

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios del ESE ISABU 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 de manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su Computador en el momento en que se retiren del puesto, 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.

Todos los computadores deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de diez (10) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

5.20. ADECUADO DE LOS ACTIVOS DE INFORMACIÓN

Las autorizaciones para el uso de una aplicación y los datos relacionados son responsabilidad exclusiva del líder de sistemas de información.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y/o proveedores determinada por los responsables de los

procesos. En el levantamiento de activos de información, se establece la clasificación de estos, y se determina el nivel de protección que se debe dar a cada uno.

Para la consulta de documentos cargados en el software de Gestión Documental (si existe) se establecerán privilegios de acceso a los colaboradores y/o proveedores de acuerdo con el desarrollo de sus funciones y competencias.

Dichos privilegios serán establecidos por el Gerente del Área o quien haga sus veces, quien comunicará al área de Tecnología e Informática (administrador del software) el listado con los colaboradores y sus privilegios.

La Entidad debe asegurar que toda información de valor para la institución, que sea manejada por los usuarios, y compartida entre dependencias, se realice por medios seguros y confiables, mediante mecanismos y controles adecuados que garanticen su protección, integridad y disponibilidad, cumpliendo con lo que se establezca en plan de resguardo de información de activos.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un "incidente de seguridad".

Inventario de Activos: Los activos de la ESE ISABU deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de la información de propiedad del Instituto, discriminado por procesos. Para efectos de implantar los controles de Seguridad y Privacidad, las dependencias que tienen la custodia de la información generada en el marco de su función, se encargarán de proteger la información y de mantener y actualizar el inventario de activos de información relacionados con sus servicios (Información, software, hardware)

5.21. RECURSOS TECNOLOGICOS

El uso adecuado de los recursos tecnológicos asignados por el ESE ISABU, a sus funcionarios y/o proveedores se reglamenta bajo los siguientes lineamientos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo propiedad del ISABU es responsabilidad del área de Sistemas y por tanto son los únicos autorizados para realizar esta labor. En este orden de ideas, los medios de instalación de software deben ser los proporcionados por la Institución a través de la mencionada área y deben contar con la licencia de uso requerida, si aplica.
- Los usuarios no deben realizar cambios en los equipos de cómputo propiedad del ISABU, relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios deben ser realizados únicamente por el área de sistemas.
- El área de Sistemas del ISABU debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en los equipos de cómputo de los funcionarios de acuerdo con sus procesos y labores. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas, y mantener al día el inventario de software y hardware de los equipos de cómputo personales.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del ISABU; las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidas por el área de Sistemas
- Los equipos de cómputo) software y elementos tecnológicos que requieran ser ingresados y conectados a la red corporativa del ISABU debe contar con los soportes de licenciamiento conforme a lo establecido por la ley (licenciamiento y legalidad de software), al igual que antivirus debidamente actualizado.
- Todos los funcionarios y/o colaboradores de la institución que utilicen equipos corporativos, deben autenticarse ante el controlador de dominio del ISABU,
- Es responsabilidad de los usuarios proteger y usar apropiadamente la información sobre la cual tienen

acceso y los equipos informáticos entregados como dotación para el desempeño de las labores asignadas. Se debe firmar el inventario de recursos informáticos entregados al funcionario, donde se indica el estado, tanto para su ingreso, retiro o movimiento que puedan tener,

- El equipo de cómputo o cualquier recurso de tecnología de información que sufra algún daño por maltrato, descuido o negligencia por parte del usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso se determinará la causa de dicho daño, y si fue responsabilidad del usuario.

5.22. ACCESO A INTERNET

El internet es una herramienta de trabajo que permite navegar en muchos, otros sitios relacionados o no con las actividades propias del negocio del ESE isabu, y permite el acceso a los servicios propios de la entidad, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking, streaming juegos y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos redes sociales como Facebook, Instagram, Snapchat 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 ESE ISABU.
- El intercambio no autorizado de información de propiedad de la ESE ISABU, de sus usuarios y/o de sus colaboradores, con terceros, utilizando estos medios.
- 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, 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 el área de sistemas, 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.
- El ESE ISABU debe realizar monitoreo permanente de tiempos de navegación, páginas visitadas y aplicaciones que se ejecutan por parte de los funcionarios, colaboradores y/o terceros. Así mismo, puede inspeccionar, registrar, evaluar y controlar todas las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente por medio de su UTM o Firewall. El uso de este recurso debe estar acorde a las funciones de su labor dentro de la Institución.
- Cada uno de los funcionarios y/o colaboradores es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.
- Los funcionarios y/o colaboradores, proveedores no pueden asumir en nombre del ESE ISABU, posiciones personales en redes sociales, encuestas de opinión, foros u otros medios similares.
- El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del ESE ISABU.
- El ESE ISABU debe garantizar la disponibilidad del servicio de internet, tanto a nivel de canales de conexión, como del dispositivo que controla todo el tráfico, tener protegido el acceso a las configuraciones de estos dispositivos, y mantener actualizadas todas las reglas de configuración de estos.
- Los usuarios móviles y remotos del ESE ISABU podrán tener acceso a la red interna privada cuando se encuentren fuera de la empresa en cualquier ubicación con acceso a una conexión a Internet segura y evitando las conexiones públicas o gratuitas, utilizando las redes privadas VPN

habilitadas por el área de sistemas.

- El personal encargado del área de sistemas serán los únicos autorizados de configurar el software necesario y asignar las claves a los usuarios que lo soliciten, según el procedimiento requerido para esto.

- Se debe estar alineado con las normas sobre nuevos protocolos y tecnologías, impartidas por el Ministerio de Telecomunicaciones.

5.23. CORREO ELECTRONICO Y ALMACENAMIENTO EN LA NUBE

Los funcionarios, contratistas, colaboradores y/o proveedores autorizados a quienes el ESE ISABU les asigne una cuenta de correo electrónico deberán seguir los siguientes lineamientos:

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la Institución.
- Los mensajes y la información contenida en los buzones de correo electrónico son propiedad de ESE ISABU y del usuario
- El tamaño de los buzones de correo es determinado por el área de Sistemas de acuerdo con los perfiles y roles que desempeñan los funcionarios
- El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de éstos están definidos de acuerdo con los perfiles y roles que desempeñan los funcionarios del ESE ISABU
- Cuando un funcionario requiere ausentarse de la Institución por un periodo superior a 3 días debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.
- Antes de enviar un mensaje de correo electrónico se deberá verificar que este va dirigido solamente a los interesados y/o a quienes deban conocer dicho mensaje
- Todo mensaje tipo phishing, spam, smishing, vishing, o alguno similar, debe ser calificado como correo no deseado, eliminado, y nunca respondido. Y reportarse de inmediato al personal de seguridad informática.
- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el ESE ISABU les proporciona. De igual manera, las cuentas de correo corporativas no se deben emplear para uso personal.
- El uso del email es personal y sus claves confidenciales. Por ningún concepto se puede entrar a revisar la información dirigida a otra persona.
- La información que se recibe de manera personal y confidencial por correo electrónico, no se puede dirigir a otra persona, sin la autorización del remitente.
- El envío masivo de mensajes publicitarios corporativos solo podrá ser utilizado a través de los medios y/o dependencias autorizadas para tal fin. Además, en el caso que dichos mensajes tengan como usuario final terceros a la Institución se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia realizar envío de correo masivo de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.
- Toda información del ESE ISABU generada con los diferentes aplicativos que utilice y que requiera ser enviada fuera de la compañía, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de tecnología informática. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el ESE ISABU y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Tanto para la información guardada en los buzones corporativos, o si se utiliza almacenamiento en

nube el ESE ISABU debe asegurar que toda información de valor para la institución, y que sea manejada por los usuarios, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, cumpliendo con lo que se establezca en plan de resguardo de información de activos.

5.24. POLITICAS ESPECIFICAS POR AREAS

5.24.1. EQUIPOS DE COMPUTO PERSONALES

- No se debe permitir el inicio de los equipos mediante CDROM o USB
- La Entidad debe asegurar que toda información de valor para la institución, y que se almacene en equipos de cómputo personales, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, cumpliendo con lo que se establezca en plan de resguardo de información de activos
- No se den compartir carpetas locales entre equipos de cómputo. Si se requiere tener información compartida, el personal de TIC debe determinar el procedimiento para hacerlo, para garantizar los principios de seguridad informática.
- Toda novedad en la infraestructura de equipos de cómputo, y de las labores de mantenimiento de estas, debe quedar registrada y documentada con detalle de actividades realizadas.
- En los equipos de cómputo personales solo deben estar activos los servicios que se requieran para la operación de estos y las aplicaciones que allí se ejecuten necesarias para la empresa, y para tener un óptimo rendimiento se debe desactivar lo que no se utilice o requiera.
- Debe existir un plan de mantenimiento físico y lógico de equipos de cómputo personales, sistemas operativos y aplicativos, de por lo menos dos veces al año. En estas labores se debe garantizar la vinculación al controlador de dominio y correcto estado de antivirus.
- El ESE ISABU establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware, antipishing y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso. Será responsabilidad del área de Sistemas autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente. Se deben programar labores de scan fuertes, por parte de estas herramientas.
- Se debe controlar el uso de dispositivos de almacenamiento externo, tales como USB. CD, DVD, etc. Restringir el uso de Discos Extraíbles (Memorias USB, discos duros externos, memorias SD, microSD, celulares, Tablet, entre otros) y unidades lectoras de DVD-CD.
- Se debe garantizar el respaldo eléctrico por el tiempo suficiente que permita apagado de forma correcta de los equipos

5.24.2. ADMINISTRACION DE USUARIOS

- Todo usuario debe tener una identificación única en la red, con su respectiva contraseña, la cual no puede ser transferida a otra persona sin previa autorización del área de Sistemas.
- Todos los recursos de información críticos del ESE ISABU tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por el líder de sistemas de información.
- Toda novedad de ingreso de personal nuevo o modificación de personal, que requiera la utilización de recursos informáticos, debe ser reportada por el líder del proceso al área de Sistemas; justificando los servicios y herramientas que el nuevo usuario necesitará para el desempeño de sus funciones. Esta solicitud debe de ser realizada por escrito en un correo electrónico y se debe de adjuntar el formato totalmente diligenciado.

- Toda novedad de retiro de personal debe ser reportada por el mismo líder del proceso o por la dirección del área de Recurso humano al área de Sistemas; a más tardar el día siguiente del retiro. El área de Sistemas se encargará de eliminar las cuentas y accesos a la red, correo y demás aplicativos internos y externos, así como de dar destino a los equipos de cómputo que se liberen.
- La contraseña o clave de acceso es personal e intransferible y no debe ser compartida, escrita, ni revelada. Las actividades que se realicen con su identificación son responsabilidad del propietario de la cuenta.
- En caso de que algún funcionario necesite acceder a un equipo de cómputo corporativo que no es el asignado a esta persona y no tenga conocimiento previo de la contraseña, debe de solicitar la debida autorización escrita al líder del proceso para que solicite al personal del área de Sistemas , el acceso , cambiando la contraseña de dicho usuario.
- Una vez digitada la contraseña, no se debe dejar el equipo de cómputo solo y desbloqueado, si va a ausentarse bloquee la pantalla (CTRL + ALT + SUPR + BLOQUEAR EQUIPO) o apáguela.
- Se debe tener control sobre los recursos de almacenamiento y definir los espacios máximos a utilizar por parte de los usuarios. El espacio en disco a que tienen derecho en un sistema debe ser controlado.

5.24.3. APLICATIVOS BD Y SERVICIOS WEB

- Todos los servicios prestados al público por la entidad se deben poder acceder por un Único URL, tanto desde la red externa como interna.
- Se debe definir el RTO y RPO, para cada aplicativo del ESE ISABU.
- El ESE ISABU debe asegurar que la información de las bases de datos institucionales sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, cumpliendo con el RPO definido por el área de Tecnología. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado. Se debe cumplir con mínimo con la estrategia de backup 3 2 1.
- El ESE Isabu debe asegurar que los servidores físicos y virtuales institucionales sean periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, cumpliendo con el RTO y RPO definido por el área de Tecnología. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado. Se debe cumplir con mínimo con la estrategia de backup 3 2 1.
- Los procedimientos de Backup, transporte, restauración y verificación de la información de la entidad, deben estar debidamente documentados y actualizados. Su ejecución periódica son la garantía de la integridad y confiabilidad de la información.
- Toda novedad en la estructura de las Bases de Datos, roles, usuarios, actividades de mantenimiento de estas debe quedar registrada y documentada con detalle de actividades realizadas.
- Se debe contar con un plan de continuidad del negocio para garantizar la Disponibilidad de los aplicativos y servicios que presta el ISABU.
- Se debe definir el RTO y RPO, para los aplicativos y servicios que presta el ISABU, de tal forma que se cumpla con los objetivos de los mismos, de acuerdo a su función, y disponibilidad de la información.
- Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

5.24.4. SERVIDORES

- Solo deben estar activos los servicios y puertos que se requieran para la operación de estos , las aplicaciones que allí se ejecuten y que son necesarias para el ESE ISABU

- Deben estar actualizados en sus sistemas operativos y aplicativos a las versiones que se recomienden, y estos procesos deben quedar documentados en detalle, así como el de regresar esta actualización en caso de falla.
- Se debe garantizar la confidencialidad de las claves de los usuarios que administran los servidores.
- Todo proceso de recuperación de claves, para los servidores con diversos sistemas operativos debe estar completamente documentado con el paso a paso, de actividades para tal fin. Si se requiere generación de medios de recuperación, se deben tener.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del ESE Isabu, las conexiones establecidas para este fin deben utilizar los esquemas y herramientas de seguridad y administración definidas por el área de Sistemas.
- Toda novedad en la infraestructura de servidores (físicos o virtuales) y de las labores de mantenimiento de estos, debe quedar registrada y documentada con detalle de actividades realizadas.
- Debe existir un plan de mantenimiento físico y lógico de servidores, sistemas operativos y aplicativos, de por lo menos una vez al año.
- Dentro de los mantenimientos preventivos de servidores (físicos o virtuales), se deben incluir tareas de revisión de logs del sistema o de eventos, y registrar recomendaciones.
- Se debe definir el RTO y RPO, para los servidores físicos o virtuales del ESE ISABU, de acuerdo con su criticidad y de los aplicativos que residen en ellos.
- Las características de hardware y software de los servidores deben ser las óptimas para satisfacer los requerimientos que demandan los diversos aplicativos y servicios que ellos prestan y deben garantizar la disponibilidad de los mismos.
- Se deben tener definidos, y documentados, los procesos de recuperación ante desastres o fallas de servidores.
- La infraestructura de servidores debe garantizar la disponibilidad de los mismos, y para el caso de repuestos, se debe contar con los contratos de mantenimiento que entreguen en el tiempo que especificó el departamento de sistemas, o contar con el KIT de repuestos para cambio en el menor tiempo posible.
- La Entidad debe asegurar que los servidores físicos y virtuales institucionales sean periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, cumpliendo con el RTO y RPO definido por el área de Tecnología. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado. Se debe cumplir con mínimo con la estrategia de backup 3 2 1
- Se debe unificar toda la gestión de servidores virtuales o físicos para facilitar su administración y tener tiempos de reacción de acuerdo a la criticidad de los eventos que ocurran.
- Para los servidores que lo permitan, se debe tener acceso a las interfaces de administración a bajo nivel que los diversos fabricantes ofrecen con estos equipos.
- Para los mantenimientos preventivos o correctivos de servidores, se deben tener los procedimientos óptimos para minimizar las ventanas de mantenimiento.
- Se debe contar con un inventario completo y detallado de todos los servidores, sus características de hardware y software, esquemas de conexiones.
- Se debe contar con un plan de continuidad del negocio para garantizar la Disponibilidad de los aplicativos y servicios que presta el ISABU.
- Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
- Se debe monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

5.24.5. REDES LAN Y SEDES

- Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- Se deberá verificar por parte del personal de redes y telecomunicaciones el cambio de claves por defecto de todos los dispositivos de red del ESE ISABU.
- Se actualizarán continuamente el firmware de los dispositivos de red y seguridad perimetral del ESE ISABU, garantizando altos estándares de seguridad e intrusión desde internet.
- Los gabinetes de cableado estructurado, servidores deben estar organizados, ordenados, con todos los cables identificados y marcados.
- Se deben tener los diagramas de conexión de todos los dispositivos de red, dentro de los diversos gabinetes, y que se indiquen los puertos usados para estas conexiones.
- La infraestructura de red debe cumplir con el principio de disponibilidad, al menos a nivel de backbone.
- La topología de red, debe garantizar los mejores tiempos de conexión entre dispositivos.
- El ESE ISABU, para todas sus dependencias debe considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.
- El resguardo de los dispositivos de red deberá quedar bajo el área de Sistemas contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos y que no permita la manipulación por parte de los usuarios.
- Se debe garantizar la gestión, administración y visibilidad de todos los dispositivos de la red del ESE ISABU.
- La infraestructura de la red debe contar con la documentación respectiva, incluyendo diagramas con topologías, detalle de conexiones, y marcación adecuada de los cables.
- Toda novedad en infraestructura de la red debe quedar registrada y documentada con detalle de actividades.
- El control y gestión del direccionamiento IP para la red interna debe ser administrado por sistemas y se debe garantizar que no existan conflictos. Esto debe aplicar también a los centros de salud.
- El control y gestión de las subredes para la red interna debe ser administrado por sistemas y se debe garantizar que los equipos se conecten a la subred destinada para su departamento o dependencia.
- El control y gestión de las subredes para la red interna debe ser administrado por sistemas y se debe garantizar que los equipos se conecten a la subred destinada para su departamento o dependencia.
- La infraestructura de red entre dependencia y sedes debe cumplir con el principio de integridad y privacidad, garantizando que el acceso a la administración de los dispositivos, solo se realiza desde equipos y personal autorizado
- La infraestructura de red entre sedes debe cumplir con el principio de disponibilidad y tener las redundancias necesarias.

5.24.6. DATA CENTER

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los servidores, almacenamiento y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.
- El control de acceso físico por dispositivo en los sitios que se aplique debe estar en correcto funcionamiento, y actualizada la información de las personas permitidas y el método de acceso, si es por huella, tarjeta u otro.
- Las condiciones ambientales (temperatura, humedad, etc.), controles de acceso físico, espacios requeridos, en el área de servidores de la data center, centros de cableado y cuartos técnicos deben

ser las aptas para el correcto funcionamiento de los equipos, e identificar eventos que atenten contra esta infraestructura.

- Los gabinetes de cableado estructurado, servidores deben estar organizados, ordenados, con todos los cables identificados y marcados.
- Se deben tener los diagramas de conexión de todos los dispositivos de red, servidores y otros equipos dentro de los diversos gabinetes, y que se indiquen los puertos usados para conexiones.
- Toda actividad de cambios en conexiones, modificación de infraestructura, o soportes técnicos debe quedar registrada y documentada.
- Se debe conocer el detalle de consumo de cada elemento que hace parte de la data center, tanto para energía como para aire acondicionado, y así determinar si los sistemas actuales son suficientes, con el fin de mantener las condiciones ambientales especificados por los fabricantes de los equipos que albergan.

5.25. CONCIENCIACIÓN Y FORMACIÓN

La entidad proporciona formación en seguridad de la información a todos los empleados y contratistas para aumentar la concienciación sobre la seguridad.

5.26. MONITORIZACIÓN Y REVISIÓN

Se ejecutan auditorías y revisiones periódicas de la seguridad de la información con el propósito de garantizar la efectividad de los controles implementados. Además, anualmente, el Oficial de Seguridad de la Información junto con la Alta Dirección lleva a cabo una revisión exhaustiva para identificar y aplicar actualizaciones, modificaciones o ajustes basados en las recomendaciones y sugerencias recopiladas durante dicho proceso.

Para la entidad, la información representa un activo fundamental tanto para la prestación de nuestros servicios como para la toma de decisiones eficientes. En este sentido, mantenemos un compromiso firme en la protección de nuestros activos de información como parte integral de nuestra estrategia orientada a:

- Garantizar la continuidad del negocio.
- Administrar de manera efectiva los riesgos asociados a la información.
- Fomentar una cultura de seguridad en el manejo y procesamiento de la información en toda la organización.

5.27. MEJORA CONTINUA

La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** se compromete a mejorar continuamente sus prácticas de seguridad de la información en función de las lecciones aprendidas y las mejores prácticas de la industria. Esta política de seguridad de la información entra en vigencia a partir de la fecha de aprobación y se revisará y actualizará regularmente para mantener su relevancia y eficacia mínimo una vez al año.

6. REFERENCIAS

Excellence, I. (s.f.). Blog especializado en Seguridad de la. Obtenido de https://www.pmg. ssi.com/2015/03/iso-27001 -los-activos-de-información/ libre, I. e. (s.f.). Wikipedia. Obtenido de https://es.wikipedia.org/wiki/Contrase%C3%B1a Litoral, U. I. (s.f.). Obtenido de http://www.unl.edu.ar/ingreso/cursos/cac/210t/ Pérez Porto, J. G. (20 de 06 de .2008). Concepto de información - Definición, Significado y Qué es. Obtenido de https://definicion.de/inforrnacion/ Wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Confidencialidad

ISO/IEC 27001:2022. Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos. Organización Internacional de Normalización (ISO), 2022.

7. CONTROL DE MODIFICACIONES

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	25/11/2020	Emisión inicial del documento	Oficina de gestión de las TICS
2	21/11/2023	Actualización de manual de la política de seguridad de la información, ajustes realizados: ▪ Cambio de nombre de manual a política de seguridad de la información, ciberseguridad y protección de la privacidad. ▪ Cambio de objetivo en el objetivo de la política ▪ Inclusión del apartado lineamiento ▪ Inclusión del apartado declaración de compromiso ▪ Inclusión del apartado declaración de aprobación ▪ Actualización del apartado referencias y otros documentos se actualizó ▪ Inclusión del apartado principios de la seguridad de la información ▪ Inclusión del apartado privacidad de la información y datos personales ▪ Inclusión del apartado responsable ▪ Inclusión del apartado Contacto de la política ▪ Inclusión del apartado procedimiento para solicitar excepciones ▪ Inclusión del apartado gestión de riesgos ▪ actualización del apartado roles y responsabilidades ▪ Inclusión del apartado concienciación y formación ▪ Inclusión del apartado monitorización y revisión ▪ Inclusión del apartado mejora continua	Profesional en seguridad Informatica – Ing. Jose Joaquín Salcedo Duran