FECHA DEL CAMBIO	DESCRIPCIÓN DEL CAMBIO	JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
02/04/2018	Elaboración del documento		1
30/09/2019	Ajuste codificación	Circular 010 de septiembre del 2019	2
30/04/2019	Adición y actualización de estrategias para prevenir la perdida de información.	Revisión y ajuste del Plan de seguridad de la información	3
28/11/2025	Actualización de documento	Actualización según normatividad vigente	4

1. OBJETIVO

Gestionar los riesgos que afectan la seguridad, privacidad y confidencialidad de la información de la E.S.E. Salud del Tundama mediante la implementación de controles, lineamientos y buenas prácticas alineadas al Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital, la ISO/IEC 27001:2022 y las normas nacionales de protección de datos personales. El objetivo es preservar los principios de confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de los activos de información institucionales.

2. ALCANCE

Desde la identificación de riesgos asociados de la información hasta su control y mitigación. Este Plan aplica a toda la información de la E.S.E. Salud del Tundama, en cualquier formato (digital o físico), así como a los sistemas de información, infraestructura tecnológica, y a todos los funcionarios, colaboradores y terceros con acceso a dicha información.

3. RESPONSABLE O DUEÑO DEL PROCESO

Líder del proceso de sistemas de la información.

4. SOPORTE LEGAL Y DOCUMENTAL

- Resolución 1995 de 1999 – Ministerio de Salud: Establece el manejo, contenido, responsabilidad y conservación de la historia clínica en Colombia.

- Ley 603 del 2000 por la cual se reglamenta la protección de los derechos de autor en

Colombia.

- Ley 1273 del 5 de enero de 2009 por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- Ley 1341 del 30 de Julio de 2009 Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- Artículo 269ª del Código Penal (Ley 1273 de 2009): Acceso abusivo a un sistema informático. El que, sin autorización por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro de mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mensuales vigentes.

- Artículo 269B del Código Penal (Ley 1273 de 2009): Obstaculización ilegítima de sistema informático o red de telecomunicación…incurrirá en pena de cuarenta y ocho (48) a noventa y seis
(96) meses y en multa de 100 a 1000 salarios legales vigentes.

- Artículo 269C del Código Penal (Ley 1273 de 2009): Interceptación de datos informáticos. El que sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- Artículo 269D del Código Penal (Ley 1273 de 2009): Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos o un sistema de tratamiento de información o sus partes componentes lógicos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos mensuales vigentes.

- Artículo 269E del Código Penal (Ley 1273 de 2009): Uso de software malicioso. El que sin estar facultado para ello produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros Plans de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos vigentes.

- Artículo 269F del Código Penal (Ley 1273 de 2009): Violación de datos personales. El que sin estar facultado para ello con provecho propio o de un tercero, obtenga, compila, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos mensuales vigentes.

- Artículo 269G del Código Penal (Ley 1273 de 2009): suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, Plan o envíe páginas electrónicas, enlaces o ventanas emergentes incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses en multa de 100 a 1000 salarios mensuales legales vigentes.

- Ley 1581 de 2012 Por la cual se establece la protección de datos personales, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-48 de 011 de la Corte Constitucional: Proyecto de Ley Estatutaria de Habeas Data y Protección de datos personales.

- Decreto 1377 de 2013 – Reglamentación Ley 1581: Define procedimientos para el manejo adecuado de datos personales, especialmente sobre autorizaciones y avisos de privacidad.

- Resolución 1460 del 30 de octubre de 2015: Por la cual la E.S.E. Salud del Tundama adopta la política de Confidencialidad y Seguridad de la Información.

- Resolución 224 del 03 de marzo de 2015 por la cual la E.S.E. Salud del Tundama adopta la política de Gestión de la Tecnología.

- Resolución 302 del 06 de abril de 2016. Por la cual la E.S.E. Salud del Tundama adopta la política de Gestión Documental.

- Plan anticorrupción y atención al ciudadano vigencia 2016 E.S.E. Salud del Tundama.

- Decreto 1008 de 2018 – Arquitectura TI del Estado: Establece lineamientos para la Arquitectura de TI en entidades públicas, buscando interoperabilidad, estandarización y eficiencia.

- Guía de Habeas Data – Superintendencia de Industria y Comercio (2019): Orienta a entidades públicas y privadas sobre cumplimiento práctico de la Ley 1581 y protección efectiva del titular.

- Decreto 612 de 2021 – Gobierno Digital: Actualiza los lineamientos de la Política de Gobierno Digital para entidades públicas, incluyendo seguridad, servicios digitales y datos.

- Resolución 866 de 2021 – Interoperabilidad en Salud: Define estándares técnicos y lineamientos para que las instituciones de salud intercambien información clínica de forma segura.

- Política de Gobierno Digital – MINTIC (Actualización 2021): Marco general que regula el uso de tecnologías, seguridad digital, servicios al ciudadano y gestión de datos en entidades públicas.

- Guía del Modelo de Seguridad y Privacidad de la Información – MSPI (2021): Modelo oficial del MINTIC que define cómo implementar seguridad de la información y protección de datos en el sector público.

- Guía de Continuidad del Negocio – MINTIC (2021): Establece los lineamientos para diseñar, implementar y mantener planes de continuidad en entidades del Estado.

- Directiva Presidencial 03 de 2022 – Ciberseguridad Estatal: Ordena fortalecer la ciberseguridad, reporte de incidentes y coordinación con CSIRT Colombia en todas las entidades públicas.

- Circular 007 de 2022 – Ciberseguridad en Entidades Públicas: Exige medidas mínimas de protección, reporte inmediato de incidentes y fortalecimiento de capacidades de seguridad digital.

- ISO/IEC 27001:2022 – SGSI: Norma internacional que define requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

- ISO/IEC 27002:2022 – Controles de Seguridad: Complemento de la 27001 que establece los controles específicos para proteger información, activos, procesos y tecnologías.

- Norma ISO 27001: SO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

5. DEFINICIONES

- **Activo de Información:** Todo conocimiento o dato que tiene valor para la E.S.E., así como los sistemas, equipos o infraestructura que lo procesa, almacena o transmite.

- **Análisis de riesgo:** Es un proceso dirigido a determinar la posibilidad que las amenazas se materialicen sobre los bienes informáticos ya sean físicos o magnéticos e implica la identificación de la información a proteger, las amenazas que actúan sobre ellos, su probabilidad de ocurrencia y el impacto que pueden cause.

- **Amenaza:** Es una situación o acontecimiento que puede causar daño a los bienes informáticos físicos o magnéticos, puede ser una persona, un Plan malicioso un suceso natural o de otra índole que representan los posibles atacantes o factores que inciden negativamente en la seguridad de la información.

- **Bienes informáticos**: Elementos, componentes, documentos físicos y magnéticos que deben ser protegidos para evitar la ocurrencia de una amenaza.

- **Clasificación de la Información:** Proceso mediante el cual se determina si la

información es pública, interna, reservada o confidencial.

- Confidencialidad: Principio que garantiza que la información solo es accesible a personas autorizadas.

- Control de Seguridad: Medida administrativa, técnica o física diseñada para reducir riesgos y proteger la información.

- Continuidad del Negocio: Capacidad de una entidad para mantener sus funciones esenciales ante interrupciones, mediante planes y procedimientos definidos.

- Copia de Seguridad (Backup): Duplicado de información esencial que permite su recuperación en caso de pérdida, daño o incidente.

- Ciberseguridad: Conjunto de prácticas, herramientas y medidas orientadas a proteger redes, sistemas y datos frente a ataques o accesos no autorizados.

- **Datos Personales Sensibles:** Información cuyo uso indebido puede afectar derechos fundamentales.

- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.

- **Encargado del Tratamiento:** Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable.

- **Responsable del Tratamiento:** Persona natural o jurídica que decide sobre el tratamiento de datos personales y las finalidades del mismo.

- **Gobierno de Seguridad:** Conjunto de responsabilidades y autoridades de la alta dirección sobre la seguridad y privacidad.

- **Incidente de Seguridad:** Evento que afecta o puede afectar la confidencialidad, integridad o disponibilidad de la información.

- **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

- I**mpacto**: Es el daño producido por la materialización de una amenaza contra la seguridad de la información.

- **Resiliencia:** Capacidad de la entidad para continuar operando tras incidentes.

- **Riesgo**: Probabilidad que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto negativo en la entidad.

- **Riesgo aceptable**: El riesgo se encuentra en un nivel que se puede aceptar sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

- **Seguridad**: es usada para minimizar los riesgos a que están expuestos los bienes informáticos sean físicos o magnéticos.

- **Teletrabajo y Movilidad:** Lineamientos para acceso remoto seguro mediante VPN, cifrado y MFA.

- **Trazabilidad:** Capacidad de registrar, seguir y auditar las acciones realizadas sobre la información y los sistemas que la gestionan.

- **Usuario Final:** Persona autorizada para acceder, usar o manipular información o sistemas institucionales.

- **Vulnerabilidad**: En un sistema informático es un punto o aspecto susceptible de ser atacado o de dañar su seguridad; representan las debilidades o aspectos fiables o atacables en el sistema de información y califican el nivel de riesgo del mismo.

6. DESARROLLO

El desarrollo del Plan se estructura conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MINTIC, adoptando un enfoque basado en riesgo, mejora continua (PHVA) y controles administrativos, físicos y tecnológicos

establecidos en la Política de Gobierno Digital.

6.1 Fundamentos del Plan

El Plan de seguridad de la información se conforma de un conjunto de proyectos, iniciativas y actividades realizadas de manera coordinada para lograr una estrategia de seguridad que permita alcanzar los objetivos de protección de la organización. Esta gestión incluye dirigir, monitorear, evaluar y mejorar todas las actividades relacionadas con la seguridad, haciendo uso óptimo de los recursos y generando información oportuna para la toma de decisiones.

Antes de su puesta en marcha, el respaldo de la alta dirección es determinante. La directiva debe asumir responsabilidades de acuerdo con el MSPI: asignación de roles formales, aprobación del análisis de riesgos, disponibilidad de recursos y seguimiento a indicadores clave de desempeño.

Asimismo, el compromiso de cada proceso y subproceso institucional es esencial para asegurar la colaboración de los colaboradores y una implementación homogénea en toda la entidad.

6.2 Estructura del Plan según el MSPI

La estructura del Plan define la organización formal del sistema de seguridad y privacidad de la información, permitiendo distribuir adecuadamente roles, responsabilidades y mecanismos de control. Esta estructura se fundamenta en los dominios establecidos por el Modelo de Seguridad y Privacidad de la Información del MINTIC, los cuales proporcionan un marco ordenado y completo para garantizar la administración eficaz de la seguridad. En esta sección se presenta la forma en que la entidad adopta dichos dominios, integrando prácticas modernas y requisitos legales que fortalecen la gestión institucional. El Plan adopta los seis dominios definidos por el MINTIC:

- **Gobernanza:** creación del Comité de Seguridad y Privacidad, roles y responsabilidades.

- **Gestión del riesgo:** identificación, valoración y monitoreo continuo.

- **Controles de seguridad:** medidas administrativas, físicas y técnicas.
- **Ciberseguridad:** prevención, detección y respuesta ante amenazas.
- **Protección de datos personales:** cumplimiento de Ley 1581 y normatividad asociada.
- **Gestión de incidentes:** lineamientos para reporte, análisis, contención y cierre.

6.3 Estrategia del Plan

La estrategia del Plan constituye la hoja de ruta que orienta las decisiones y actividades relacionadas con la seguridad de la información. Su finalidad es asegurar que los esfuerzos se encuentren alineados con los objetivos institucionales, los riesgos identificados y las obligaciones normativas vigentes. Este apartado introduce la importancia de planificar de manera integral, articulando controles, evaluaciones periódicas y mecanismos de mejora continua para fortalecer la resiliencia organizacional y garantizar la protección de los activos de información. La estrategia del Plan debe derivarse del análisis de riesgos, de los objetivos institucionales y de los lineamientos vigentes del MINTIC. Esta estrategia considera:

- Alineación a los objetivos estratégicos de la E.S.E.
- Resultados de la evaluación de riesgos.
- Prioridades basadas en criticidad e impacto.
- Requisitos establecidos por ISO/IEC 27001:2022.

Incluye actividades como planeación de controles, monitoreo permanente, implementación de auditorías internas y aplicación del ciclo PHVA.

6.4 Lineamientos para el uso de contraseñas

Los lineamientos sobre contraseñas establecen las reglas necesarias para garantizar un control seguro de acceso a los sistemas y recursos institucionales. En un entorno donde las amenazas digitales son frecuentes, una política sólida de contraseñas se convierte en un elemento crítico para evitar accesos no autorizados y compromisos de seguridad. Esta sección introduce los principios generales que orientan la creación, uso y protección de contraseñas, integrando buenas prácticas internacionales y normativas nacionales.

Se incorporan las reglas históricas de la entidad junto con los requerimientos actuales del MINTIC:

- Longitud mínima recomendada: **12 caracteres**.
- Evitar cambios periódicos injustificados; sólo cambiar ante compromiso.
- Uso obligatorio de autenticación multifactor (MFA) para accesos críticos.
- No reutilizar contraseñas ni emplear datos personales.
- Prohibir cadenas obvias (qwerty, 12345, etc.).

Las directrices existentes permanecen como medidas complementarias.

6.5 Identificación y análisis de riesgos

La identificación y análisis de riesgos constituye uno de los pilares más importantes del Plan de seguridad, ya que permite anticipar amenazas, detectar vulnerabilidades y establecer tratamientos eficaces. Un adecuado proceso de análisis de riesgos proporciona información valiosa para la toma de decisiones, optimiza el uso de recursos e impulsa la implementación de controles basados en impacto y probabilidad. Este apartado introduce la importancia de adoptar una gestión de riesgos continua, documentada y alineada a los estándares del MINTIC y las normas ISO. El Comité de Seguridad de la Información continúa siendo responsable del análisis de riesgos, el cual ahora se fortalece mediante:

- Aplicación de metodologías del MSPI.
- Identificación, valoración, tratamiento y monitoreo continuo.
- Registro formal de vulnerabilidades y exposición crítica.
- Relación directa entre riesgos y activación del proceso de gestión de incidentes.

La gestión del riesgo se convierte en un proceso continuo, no limitado a una revisión anual.

6.6 Controles para prevenir la pérdida de información

Los controles de prevención de pérdida de información buscan reducir o eliminar los riesgos asociados al manejo, almacenamiento y transmisión de datos institucionales. La

protección de la información es fundamental para el cumplimiento normativo, la continuidad del negocio y la confianza de la ciudadanía. En esta sección se presenta un marco introductorio sobre la importancia de aplicar medidas administrativas, técnicas y físicas que garanticen la integridad y disponibilidad de los activos de información de la E.S.E. Se mantienen los 12 controles históricos, integrados ahora bajo los lineamientos de ISO 27002:2022. Entre ellos:

- Cumplimiento de políticas internas.
- Actualización de antivirus y antispam.
- Prevención de malware.
- Protección en el transporte de información.
- Gestión de contraseñas.
- Prevención de phishing.
- Protección de información fuera de la entidad.
- Copias de seguridad.
- Gestión del ciclo de vida de usuarios.
- Capacitación continua.

Cada control forma parte del marco de seguridad reforzado y medible.

6.7 Continuidad del negocio

La continuidad del negocio constituye un componente estratégico fundamental para garantizar que la E.S.E. pueda mantener la operación de sus servicios esenciales ante cualquier evento disruptivo, ya sea una falla tecnológica, un incidente de ciberseguridad, un desastre natural o una contingencia operativa. Una adecuada gestión de la continuidad permite anticipar riesgos, definir prioridades y establecer procedimientos claros que aseguren la recuperación de los procesos críticos en tiempos aceptables. Este enfoque fortalece la resiliencia institucional, protege la prestación de los servicios de salud y permite minimizar el impacto sobre la ciudadanía. Para lograrlo, la entidad debe contar con un plan estructurado, documentado y probado periódicamente, el cual incorpore análisis, estrategias de recuperación y responsabilidades claramente definidas. A continuación, se presentan los elementos mínimos que debe contener el Plan de Continuidad del Negocio.

- Análisis de Impacto al Negocio (BIA).
- Identificación de procesos críticos.
- RTO y RPO definidos.
- Estrategias de recuperación.
- Pruebas anuales documentadas.

6.8 Proceso de Backup

El proceso de backup es una medida fundamental para garantizar la disponibilidad, integridad y recuperación de la información institucional ante incidentes que puedan generar pérdida, corrupción o inaccesibilidad de los datos. Contar con copias de seguridad confiables permite mitigar el impacto de fallas técnicas, errores humanos, ataques de ciberseguridad o desastres que afecten la infraestructura tecnológica. La E.S.E adopta un enfoque estructurado que integra prácticas de alto estándar, controles de verificación y mecanismos de protección que aseguran la confidencialidad de los datos respaldados. Este proceso debe mantenerse documentado, automatizado y probado periódicamente, garantizando que la información pueda ser restaurada de manera oportuna y efectiva ante cualquier contingencia.

Para ello, el proceso de backup institucional incorpora los siguientes elementos esenciales:

- Copias de seguridad cifradas.
- Almacenamiento externo (offsite).
- Verificación de integridad mediante hash.
- Pruebas periódicas de restauración.
- Respaldo del software institucional, sus bases de datos y estructuras críticas.

Adicionalmente, el proceso de respaldo de información de los colaboradores garantiza la protección y disponibilidad de los archivos institucionales almacenados en los equipos de trabajo. Este procedimiento se aplica de manera obligatoria a todos los equipos del área administrativa y, en el área asistencial, únicamente a aquellos que cada líder de proceso determine como críticos o necesarios para la continuidad operativa. Su correcta ejecución permite prevenir pérdidas de información, facilitar la recuperación ante incidentes y fortalecer la seguridad institucional. Para conocer en detalle las actividades, responsabilidades y parámetros técnicos de este proceso, debe consultarse el

documento “Guía para la Creación de Copias de Seguridad a Softwares Institucionales AGICOg04-220 del 01-07-2025”.

6.9 Monitoreo del Plan

El monitoreo del Plan de seguridad y privacidad constituye un componente fundamental para evaluar la efectividad de los controles implementados y garantizar el cumplimiento de los lineamientos institucionales y normativos. A través de un seguimiento sistemático, la entidad puede identificar desviaciones, detectar oportunidades de mejora y tomar decisiones oportunas que fortalezcan la protección de los activos de información. Este proceso requiere el uso de indicadores claros, mediciones periódicas y reportes confiables que permitan a la alta dirección comprender el estado real del Plan y orientar las acciones necesarias. El monitoreo continuo no solo permite evidenciar avances, sino también asegurar la mejora constante del sistema de gestión. A continuación, se presenta el mecanismo de seguimiento aplicado por la entidad.

7. CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información es un proceso esencial para garantizar que los datos institucionales reciban el nivel adecuado de protección según su sensibilidad, criticidad y valor para la entidad. Esta categorización permite establecer controles diferenciados que aseguren el manejo correcto de la información, previniendo accesos no autorizados, pérdidas, filtraciones o uso indebido. Además, facilita el cumplimiento de las normativas de transparencia pública, protección de datos personales y lineamientos del MINTIC, asegurando un tratamiento responsable y seguro de los activos informacionales. La correcta clasificación también orienta a los colaboradores sobre las medidas que deben aplicar durante la creación, almacenamiento, transmisión y disposición final de los documentos y datos. A continuación, se presentan los niveles de clasificación adoptados por la E.S.E.

- **Pública:** Se divulga sin restricciones y puede publicarse en la página web, redes institucionales o entregarse por transparencia. Solo requiere garantizar su integridad y actualización.

- **Interna:** De uso exclusivo dentro de la entidad. Acceso limitado al personal

autorizado según rol. Se almacena en repositorios institucionales y no puede compartirse con externos sin aprobación.

• **Reservada (Ley 1712 de 2014):** Acceso restringido por razones legales o de seguridad. Solo personal autorizado puede consultarla. Debe almacenarse con controles estrictos, cifrado y trazabilidad de accesos.

• **Confidencial (datos personales y sensibles):** Incluye datos personales y sensibles. Su acceso es altamente restringido y controlado. Requiere cifrado, autenticación fuerte y manejo seguro, evitando copias y usos no autorizados.

8. CONTROLES DE SEGURIDAD

Los controles de seguridad constituyen el conjunto de medidas técnicas, administrativas y físicas implementadas para proteger los activos de información frente a amenazas internas y externas. Estos controles permiten garantizar la confidencialidad, integridad y disponibilidad de los datos institucionales, alineándose con los lineamientos del MINTIC, el MSPI y los estándares internacionales como ISO/IEC 27002. Su adecuada aplicación reduce la probabilidad de incidentes, fortalece la resiliencia operativa y asegura que los procesos críticos funcionen de manera segura. En esta sección se presenta el conjunto de controles adoptados por la E.S.E., los cuales se fortalecen con prácticas actualizadas en materia de contraseñas, copias de seguridad y teletrabajo.

Contraseñas

- Mínimo 12 caracteres.
- Evitar complejidad obligatoria innecesaria.
- Activar MFA en sistemas críticos.

Copias de seguridad

- Backups cifrados.
- Verificación mediante hash.
- Pruebas de restauración anuales.
- Almacenamiento externo (offsite).

Teletrabajo

- Acceso mediante VPN.
- Prohibición de uso de redes públicas sin cifrado.
- Lineamientos para equipos corporativos o personales (BYOD) según riesgo.

9. PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio constituye un componente fundamental para garantizar que la E.S.E. pueda mantener o restablecer sus servicios esenciales ante eventos disruptivos, fallas tecnológicas, ciberataques o situaciones de emergencia. Su propósito es asegurar que los procesos críticos continúen operando dentro de tiempos aceptables, minimizando el impacto en la atención en salud y en las operaciones institucionales. Este plan debe estar alineado con los lineamientos del MINTIC y las mejores prácticas internacionales, incorporando análisis, estrategias y pruebas que permitan validar su efectividad. A continuación, se presentan los elementos clave que la E.S.E. debe definir para garantizar una continuidad operativa adecuada.

La E.S.E definirá:

- Procesos críticos.
- RTO (Recovery Time Objective).
- RPO (Recovery Point Objective).
- Pruebas de continuidad anuales.

10. GESTIÓN DE USUARIOS

La gestión de usuarios es un componente esencial para garantizar que los accesos a los sistemas, aplicaciones y recursos institucionales se administren de manera segura, controlada y acorde con las funciones asignadas a cada colaborador. Una correcta administración del ciclo de vida de los usuarios permite prevenir accesos indebidos, reducir riesgos operativos, evitar privilegios excesivos y asegurar la trazabilidad de todas las acciones realizadas en los sistemas de información. Este proceso debe ejecutarse siguiendo los lineamientos del MINTIC y las mejores prácticas internacionales, manteniendo actualizada la información de usuarios, evaluando de forma continua la

pertinencia de los permisos y aplicando medidas correctivas oportunas. A continuación, se describen los elementos clave que conforman la gestión de usuarios en la E.S.E.

- Ciclo de vida completo (creación, modificación, baja).
- Revisión periódica de permisos.
- Eliminación inmediata de accesos a usuarios inactivos.

10.1 Cláusula de confidencialidad y manejo de la información

La cláusula de confidencialidad tiene como propósito garantizar que toda la información generada, recibida o administrada por la E.S.E. Salud del Tundama sea tratada de manera responsable, segura y conforme a la normatividad vigente. Todo funcionario, contratista, proveedor o tercero que acceda a información institucional se compromete a protegerla, evitar su divulgación no autorizada y usarla únicamente para el desarrollo de las funciones asignadas. Este compromiso incluye la preservación de la confidencialidad, integridad y disponibilidad de los datos, especialmente aquellos clasificados como reservados, confidenciales o que contengan datos personales o sensibles.

Para mayor información sobre responsabilidades, obligaciones y compromisos formales, se debe consultar el documento AGICOp17-220 Procedimiento de Seguridad y Confidencialidad de la Información y el documento AGICOf35-220 Compromiso de Confidencialidad y Manejo de Información de Terceros V1, los cuales amplían los criterios, lineamientos y sanciones aplicables. El incumplimiento de estas obligaciones constituye una falta grave y podrá generar sanciones disciplinarias, contractuales y legales según corresponda.

10.2 Uso de los equipos

El uso de los equipos institucionales está estrictamente regulado con el fin de garantizar su operación segura, la protección de la información que contienen y el cumplimiento de las políticas internas de seguridad de la E.S.E. Salud del Tundama. Solo el personal vinculado mediante contrato —ya sea de planta o por prestación de servicios— que cuente con la capacitación necesaria y las competencias técnicas requeridas, está autorizado para manipularlos. Esta restricción busca prevenir daños, accesos no autorizados, fugas de información y cualquier riesgo asociado al uso inadecuado de los

recursos tecnológicos. En esta sección se establecen los requisitos mínimos que deben estar definidos en los contratos y que son obligatorios para quienes hagan uso de los equipos institucionales.

- Personas idóneas, capacitadas y entrenadas en el correcto uso de los diferentes equipos a su cargo.
- Cumplimiento del código de ética institucional.
- Inclusión de cláusula de manejo seguro de la información.
- Adhesión formal a la política de confidencialidad de la E.S.E. Salud del Tundama.

11. ESTRATEGIAS DE SENSIBILIZACIÓN

Las estrategias de sensibilización constituyen un componente esencial del Modelo de Seguridad y Privacidad de la Información, ya que permiten fortalecer la cultura organizacional en torno a la protección de los activos de información. La E.S.E. Salud del Tundama reconoce que la seguridad no depende únicamente de herramientas tecnológicas, sino también del comportamiento responsable y consciente de todos los funcionarios, contratistas y terceros que manejan información institucional. Por ello, se implementan acciones permanentes de capacitación, comunicación y acompañamiento orientadas a promover buenas prácticas, prevenir incidentes y asegurar el cumplimiento de las políticas, procedimientos y obligaciones legales vigentes. Estas actividades buscan generar un entorno seguro, reducir riesgos humanos y garantizar que cada colaborador comprenda su rol dentro del sistema de seguridad de la información.

Las estrategias de sensibilización incluyen:

Plan de capacitación periódica: Capacitaciones presenciales o virtuales sobre políticas de seguridad, protección de datos personales, clasificación de la información, uso seguro de contraseñas, teletrabajo, manejo de incidentes y responsabilidad institucional.

Campañas de comunicación interna: Difusión continua de mensajes preventivos mediante correos, carteleras, infografías, boletines digitales y recordatorios de buenas prácticas, alineados al MSPI y a las normas internas.

Talleres prácticos y simulaciones: Ejercicios de identificación de riesgos, uso seguro de dispositivos, atención de incidentes y manejo adecuado de información confidencial y sensible.

Sensibilización durante el proceso de inducción: Todos los nuevos colaboradores reciben orientación formal sobre políticas, acuerdos de confidencialidad, clasificación de la información, uso aceptable de equipos y protocolos de seguridad.

Refuerzo en momentos críticos: Recordatorios estratégicos durante temporadas de alto riesgo (vacaciones, cambios de personal, auditorías, activación de teletrabajo, contingencias tecnológicas, etc.).

Actualización anual obligatoria: Sesiones de repaso que garanticen que cada funcionario se mantenga actualizado frente a cambios en normatividad, políticas internas, hallazgos de auditoría y nuevas amenazas.

Registro de participación y evidencias: Cada actividad de sensibilización queda documentada para control interno, auditoría y cumplimiento del MSPI y del Sistema de Gestión Institucional.

12. INDICADORES

Los estipulados en el tablero de mando de indicadores de gestión.

13. DOCUMENTOS REFERENCIA

- Política de Seguridad de la Información de la E.S.E.
- Ley 1581 de 2012 y Decreto 1377 de 2013 – Protección de datos personales.
- Política de Gobierno Digital y MSPI – MINTIC.
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022.
- ISO 22301 – Continuidad del Negocio.

- Resolución 1995 de 1999 y Resolución 866 de 2021 (sector salud).
- AGICOg04-220 – Guía de Copias de Seguridad.
- AGICOf35-220 – Compromiso de Confidencialidad de Terceros.
- AGICOp17-220 – Procedimiento de Seguridad y Confidencialidad.

Elaborado por: Edwin Andrés Romero Agudelo	**Cargo:** Líder Sistemas de Información	**Fecha:** 02/04/2018
Ultima Actualización: Edwin Andrés Romero Agudelo	**Cargo:** Líder Sistemas de Información y Comunicación Organizacional	**Fecha:** 04/12/2025 **Firma:** 
Revisado por: Sandra Victoria Avendaño Merchán	**Cargo:** Líder de Mejoramiento Continuo	**Fecha:** 04/12/2025 **Firma:** 
Aprobado por: Andrea Liliana Arias Perdomo	**Cargo:** Gerente	**Fecha:** 04/12/2025 **Firma:**