INTRODUCCIÓN

La implementación de la política de seguridad y privacidad de la información (en adelante **"Política"**), busca desarrollar capacidades a través de la implementación de los lineamientos de seguridad y la privacidad de la información en todos sus procesos, áreas, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de la Clínica Internacional de Alta Tecnología Clinaltec (en adelante **"CLINALTEC"**), con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
Por tal motivo, se definen los lineamientos a través del área de Seguridad de la información se liderará su planeación, implementación, capacitación y ejecución, con el fin de mitigar los riesgos asociados a los activos de información, propendiendo así por su buen uso y privacidad.

El documento que se presenta como política de seguridad y privacidad de la información, pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que **CLINALTEC**, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias.

1. OBJETIVO GENERAL

Establecer lineamientos y directrices para proteger, conservar y asegurar la información de **CLINALTEC**, y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente amenazas internas o externas, deliberadas o accidentales.

2. OBJETIVOS ESPECÍFICOS

Implementación de la **Política** en **CLINALTEC.**

.

- Crear una cultura de apropiación de la seguridad y privacidad de la información en **CLINALTEC**.

- Gestionar los riesgos de seguridad de la información a fin de mitigar los impactos negativos ante una eventual materialización.

- Proteger los activos de información de **CLINALTEC**.

3. ALCANCE Y APLICABILIDAD

Esta **política** es transversal a todos los procesos, áreas y procedimientos institucionales de **CLINALTEC**; aplica a todos los colaboradores y otros terceros que desempeñen alguna actividad en las instalaciones de **CLINALTEC** o a nombre de esta.

El ámbito de aplicación de esta **política** es la infraestructura tecnológica y entorno informático de la red de **CLINALTEC**.

El ente que garantizará la ejecución y puesta en marcha de la normativa y políticas de seguridad, estará a cargo del proceso **SEGURIDAD DE LA INFORMACIÓN**, siendo el responsable absoluto de la supervisión y cumplimiento, supervisados por la Alta Gerencia.

4. GLOSARIO

Política de Seguridad de la Información: documento de alto nivel que denota el compromiso de la Alta Gerencia con la seguridad de la información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.

Alta Gerencia: Grupo de personas, con capacidad, virtud o eficiencia de dirigir equipos de trabajo, con facultades para contratar con entidades públicas, mixtas y/o privadas.

Mejor Práctica: regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas.

Guía: es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada.

Activo de información: se refiere a cualquier información o elemento relacionado con el tratamiento que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

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

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

Copias de Seguridad: Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla y disponerla en caso de que ocurra un fallo que afecte a esta.

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

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

Seguridad de la información: Es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción.

5. MARCO NORMATIVO

CLINALTEC por ser una entidad de salud, debe cumplir con la regulación y la normativa que establece el Estado Colombiano en materia de:

- Ley 1581 de 2012 Tratamiento de datos personales.
- NTC/ISO 27001:2022. La seguridad de la información, ciberseguridad y protección de la privacidad. Controles de Seguridad de la Información.
- Ley 1273 de 2009 de la protección de la información y de los datos.
- Ley 1480 de 2011 (Habeas Data).

6. ROLES Y RESPONSABILIDADES

A continuación, se determinan los roles y responsabilidades dentro de **CLINALTEC**, con el fin de implementar la **Política**.

6.1. Alta Gerencia.

Asignar y aprobar los recursos humanos y económicos para la implementación de la **Política** y el Sistema de Gestión de Seguridad de la Información (SGSI).

6.2. Gerencia TICs.

Tiene la responsabilidad de coordinar la administración, configuración de los recursos informáticos dentro de la plataforma tecnológica de seguridad, así como de gestionar la planificación y ejecución del plan de mantenimiento y actualización de la infraestructura tecnológica y de telecomunicaciones de la Institución y la implementación de las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicaciones de datos o infraestructura TI.
Sus responsabilidades frente al Sistema de Gestión de Seguridad de la Información son:

● Es responsable de administrar y controlar el acceso a los recursos de las diferentes plataformas tecnológicas en **CLINALTEC** de acuerdo con su perfil y descripción del cargo.
● Asegurar el correcto funcionamiento y la disponibilidad que se requiere del servicio de Internet, sobre el cual se deben aplicar los controles que se definan.
● Monitorear a través de las herramientas tecnológicas de la institución el comportamiento del uso del servicio de Internet.
● Coordinar las acciones junto con el área de seguridad de la información, para garantizar la seguridad y privacidad de los activos de información de **CLINALTEC**.
● Implementar y gestionar los controles de seguridad sobre los activos de información tecnológicos de la institución.

6.3. Gerentes, Directores y Líderes de Proceso.

Dentro del organigrama de **CLINALTEC** se encuentran niveles de Gestión, los cuales se dividen en:

- Nivel estratégico del organigrama: (Roles) Gerentes y Directores
- Nivel táctico del organigrama: (Roles) Jefes de área y departamentos, Coordinadores de oficinas administrativas.
- Nivel operativo del organigrama: (Roles) Profesionales, Tecnicos y tecnologos y Operarios.

Todos estos roles deben asumir las responsabilidades que les sean asignadas para apoyar que todos los procedimientos de seguridad de la información se realizan correctamente para lograr el cumplimiento de todas las políticas y estándares de seguridad y privacidad de la información.

Estos Roles son responsables de la Información que administren en sus respectivas áreas, y deberán realizar su valoración para reconocer los riesgos a que se expone y a su vez cuidar de que se provean los mecanismos necesarios para mitigar los riesgos a niveles aceptables apoyándose con el área de seguridad de la información para gestionarlos.

Frente a otras responsabilidades que tienen a nivel de seguridad de la información, están:

- Identificar los activos, riesgos y controles para el manejo de la información.

- Sugerir posibles ajustes para la mejora continua del Sistema de Gestión de Seguridad de la Información.

- Informar al área de seguridad de la información, cuando detecte cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles.

- Apoyar al área de Seguridad de la Información en la identificación de los requerimientos relacionados con seguridad.

- Participar en las Auditorías del Sistema de Gestión de Seguridad de la Información.

- Solicitar los accesos a los sistemas de información sobre los cuales sean responsables de acuerdo con los lineamientos definidos por la Gerencia TICs.

- Informar de manera oportuna a la Gerencia TICs cuando el funcionario ha dejado de pertenecer a la entidad, inicie su periodo de vacaciones o licencia, o cuando algún usuario tenga novedades en sus roles o funciones, para revocar o modificar las credenciales asignadas para las aplicaciones y servicios a los cuales tiene acceso

6.4. Oficial de Seguridad de la Información.

Es el responsable de implementar acciones para alinear la implementación del Sistema de Gestión de Seguridad de la Información con los objetivos institucionales, así mismo define la normativa de seguridad y privacidad de la información y vela por su cumplimiento, previene, detecta y analiza las vulnerabilidades.

Interactúa directamente con la Alta Gerencia para informar y reportar lo relacionado con la seguridad y privacidad de la información, da respuesta inmediata ante cualquier incidente de ciberseguridad y finalmente forma, concientiza y sensibiliza a la institución en materia de seguridad de la información.
Frente a otras responsabilidades están:

- Acompañar a las áreas y/o procesos en la identificación y gestión de los riesgos de seguridad de la información, realizando la revisión, análisis y consolidación de la información.
- Definir e implementar en coordinación con las áreas de **CLINALTEC**, las estrategias de sensibilización y divulgación de seguridad y privacidad de la información.
- Atender los incidentes de Seguridad de la Información así como la investigación de infracciones de la seguridad y ejecutar actividades de seguimiento.
- Asesorar en materia de Seguridad de la Información y ciberseguridad a la institución.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en **CLINALTEC**.
- Trabajar con la Alta Gerencia y los responsables de los procesos misionales dentro de **CLINALTEC** en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
- Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales, así mismo tramitar las consultas, solicitudes y reclamos respetando las condiciones de seguridad y privacidad de información del titular

6.5. Gerente Legal y de Cumplimiento:

- Brindar asesoría a los procesos de **CLINALTEC** en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Brindar asesoría al Comité de Seguridad de la Información en temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

● Representar a **CLINALTEC** en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.

● Los contratos o acuerdos de tercerización total o parcial para la administración y/o control de sistemas de información en redes de datos y/o ambientes de desarrollo, se contemplarán requerimientos de Seguridad que se alineen a nuestras políticas de seguridad y privacidad de la información.

6.6. Colaboradores y Terceros: el rol y responsabilidad principal de los usuarios que acceden a los sistemas de información y servicios tecnológicos institucionales para el cumplimiento de sus funciones y obligaciones tienen la responsabilidad de cumplir y aplicar la política de seguridad y privacidad de la información establecida.
Frente a otras responsabilidades están:

● El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo o área puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña de calidad, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

● Evitar guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guarde en un lugar seguro.

● Cualquier usuario que encuentre un vulnerabilidad o falla de seguridad en los sistemas informáticos de **CLINALTEC**, está obligado a reportarlo a los administradores del sistema y al área de seguridad de la información.

● Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función de **CLINALTEC**.

● La información confidencial a cargo de terceros debe ser tratada bajo los mismos lineamientos establecidos para el tratamiento de la información confidencial de **CLINALTEC**.

● El acceso de terceros a la red de **CLINALTEC** será concedido siempre y cuando se cumplan con los requisitos de seguridad, del equipo externo, este debe contar con antivirus actualizado, firewall y no poseer software de descargas de archivos o música que se ejecutan en segundo plano. El área Gerencia TICs se reserva el derecho a conceder o no el acceso a equipos informáticos de terceros dependiendo de las condiciones de seguridad del dispositivo sin previa autorización.

● Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

6.7. Jefatura Departamento de Gestión Humana:

● Controlar y salvaguardar la información de datos personales de los colaboradores de **CLINALTEC**, en concordancia con la normatividad vigente.

● Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

● Al cambiar la relación laboral de cualquier funcionario (despido, renuncia, traslado, etc.), será responsabilidad del área Jefatura Departamento de Gestión Humana informar al área Gerencia TICs las novedades de personal, quien a su vez deberá revocar y/o cambiar los derechos del usuario en todos los sistemas de información que se encuentre asociado, también se deben preservar los archivos alojados por el usuario en el servidor destinado para tal fin; El perfil local del usuario (PC de trabajo) será almacenado por un tiempo pertinente para su posterior acceso en caso de ser necesario.

6.8. Comité de Seguridad de la Información:

● Revisar y aprobar, las políticas y las responsabilidades generales en materia de seguridad de la información.

● Monitorear cambios significativos en la exposición de activos de información frente a las amenazas más importantes.

● Revisar y monitorear los incidentes relativos a la seguridad.

● Aprobar las principales iniciativas para incrementar la seguridad de la información.

● Acordar funciones y responsabilidades específicas relativas a seguridad de la información para toda institución.

● Acordar metodologías y procesos específicos relativos a la seguridad de la información.

● Evaluar y coordinar la pertinencia y la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

7. PRINCIPIOS DE LA POLÍTICA

La política de seguridad y privacidad de la información de **CLINALTEC** se rige por los siguientes principios, a fin de proteger los Activos de Información de cualquier pérdida de Confidencialidad, Integridad y/o Disponibilidad de forma accidental y/o intencionada.

- **CLINALTEC**, asegurará la protección de la información generada, procesada y/o resguardada por los procesos de negocio y su infraestructura tecnológica, buscando mantener la Disponibilidad, Integridad y Confidencialidad de esta.
- La responsabilidad de la seguridad de la información es de todos y debe ser parte integral del ciclo de vida de la información.
- **CLINALTEC**, protegerá la información por medio de la identificación de los Activos de Información y la gestión de riesgos de Seguridad de la Información a través de controles de seguridad.

8. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CLINALTEC, entendiendo la importancia sobre la gestión de la información, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer confianza en el ejercicio de sus funciones y la prestación de servicios con sus grupos de interés. Lo anterior enmarcado en el cumplimiento de la normatividad vigente y alineado con la misión y visión institucional.

Por tal motivo, adopta su Política de Seguridad y Privacidad de la Información con el fin de velar por la protección, confidencialidad, integridad y disponibilidad de los activos de información (procesos, hardware, software, infraestructura, información, funcionarios, contratistas, terceros) que soportan los procesos de la entidad, mediante la implementación de lineamientos, procedimientos y la asignación de responsabilidades, los cuales están orientados a mitigar los riesgos y prevenir incidentes de seguridad dentro de un proceso de mejora continua.

Esta Política se conforma por una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen las siguientes secciones:

Controles Organizacionales: Orientado a la forma de operar, que hace cada persona y que hace el equipo de trabajo en materia de seguridad de la información dentro de **CLINALTEC** y establecer un marco gerencial para controlar su implementación.

Controles de Personas: Orientado al manejo de las relaciones con los colaboradores y/o proveedores, antes, durante y después de la prestación de los servicios a la institución con relación a temas de seguridad de la información, con el fin de reducir los riesgos contra **CLINALTEC**.

Controles Físicos: Están relacionados con la protección de los activos de información de riesgos físicos como la temperatura, espacio físico, intrusiones en perímetros físicos, energía, conectividad etc.

Controles Tecnológicos: Relacionados con controles de accesos lógicos, actualizaciones de sistemas operativos, uso de software como servicio, infraestructura como servicio, utilidad de antimalware etc.

9. CONTROLES ORGANIZACIONALES.

9.1. Políticas de Seguridad de la Información: El objetivo principal es brindar orientación y apoyo en la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes; así mismo definir un conjunto de políticas para la seguridad de la información, aprobada por la Alta Gerencia, publicada y comunicada a los empleados y partes externas pertinentes.

Las políticas de seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

9.2. Roles y Responsabilidades: La Alta Gerencia designa a un "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de **CLINALTEC**, lo cual incluye la supervisión de todos los aspectos inherentes a la seguridad de la información, cualquiera sea el medio de almacenamiento, tratados en la presente Política.

9.3. Responsabilidades de Gestión: La Alta Gerencia exigirá a todo el personal de **CLINALTEC** que aplique la seguridad de la información de acuerdo con la presente política y las políticas y los procedimientos derivados establecidos por la organización.

9.4. Seguridad de la Información en la Gestión de Proyectos: Enfatiza la importancia de integrar las consideraciones de seguridad de la información en todas las fases de la gestión de proyectos, desde la planificación y el inicio hasta la ejecución, el monitoreo y el cierre. Su objetivo es salvaguardar la información confidencial involucrada en los proyectos y prevenir posibles brechas de seguridad que podrían poner en peligro los entregables del proyecto y la postura general de seguridad de la organización.

9.5. Uso Aceptable de la Información y otros Activos Asociados: se debe asegurar que el personal y proveedores o contratistas de **CLINALTEC,** comprendan que los activos de información tales como equipos (por ej., PCs, laptops, medios de almacenamiento,

dispositivos móviles, etc.), el acceso a Internet, las aplicaciones y los servicios de mensajería electrónica son exclusivamente para fines laborales. Se pretende que el personal y proveedores conozcan las pautas y tomen los recaudos necesarios para proteger los activos de información de la entidad.
El alcance abarca todo el personal de **CLINALTEC** y proveedores que hacen uso de activos de información para desempeñar sus responsabilidades laborales.

9.6. Devolución de Activos: Enfatiza el establecimiento e implementación de procedimientos para el personal y otras partes interesadas, según corresponda, devolver todos los activos de **CLINALTEC** que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.

9.7. Clasificación de la Información: Enfatiza el establecimiento e implementación de un enfoque sistemático para clasificar los activos de información en función de su valor, sensibilidad y criticidad para la organización.
Para esto se aplican criterios de clasificación definidos a cada activo de información, asignándole un nivel de clasificación (por ejemplo, confidencial, restringido, interno, pública) basado en su sensibilidad e importancia.
Así mismo se aplicarán medidas de seguridad apropiadas según el nivel de clasificación de cada activo de información, tales como controles de acceso, cifrado de datos y medidas de seguridad física.

9.8. Niveles de clasificación:

En función de la sensibilidad de la información, **CLINALTEC** deberá catalogar la información en cinco niveles, véase la definición precisa en el Anexo “Niveles de clasificación”:

• Uso público
• Información confidencial
• Información interna
• Información restringida

9.9. Gestión de información privilegiada:

La información que se considere reservada, confidencial o secreta se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

10.0. Etiquetado de la información:

CLINALTEC deberá etiquetar mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.
Se deberán etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información definidos en el subapartado anterior, exceptuando la información considerada de "Uso público".

10.1. Control de acceso:

Todos los sistemas de información de **CLINALTEC** deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.
El control de acceso se entenderá desde la perspectiva tanto lógica (enfocado a sistemas de la información) como física y del entorno.

10.2. Derechos de Acceso: CLINALTEC establece políticas claras y documentadas que definan quién tiene acceso a qué información y recursos, según sus roles, responsabilidades y necesidades del negocio.
A su vez se implementan mecanismos de control de acceso que emplean controles técnicos y procedimentales apropiados para aplicar las políticas de derechos de acceso.

Otorgar y Revocar Derechos de Acceso: Se tiene implementado un proceso formal para otorgar y revocar derechos de acceso de manera oportuna, basado en cambios en los roles de trabajo, responsabilidades o terminación del empleo.

Supervisar y Revisar los Derechos de Acceso: Se realizará monitoreo y se revisa continuamente los derechos de acceso para identificar y abordar cualquier riesgo potencial o intento de acceso no autorizado. Esto incluye auditorías regulares, análisis de registros y procedimientos de respuesta a incidentes.

10.3. Seguridad de la Información en las Relaciones con los Proveedores: CLINALTEC establece las siguientes consideraciones:

Selección y Contratación de Proveedores Seguros: Se tiene implementado un proceso riguroso de selección de proveedores que prioriza las consideraciones de seguridad, incluida la evaluación de las políticas de seguridad, los procedimientos y las salvaguardas técnicas del proveedor. Se incorporan cláusulas de seguridad en los contratos que definen claramente

las responsabilidades del proveedor para proteger la información y cumplir con los estándares de seguridad de la organización.

Supervisión y Revisión del Desempeño del Proveedor: Se supervisa y se revisa continuamente el desempeño del proveedor para garantizar que cumpla con los requisitos de seguridad acordados, incluidas auditorías periódicas, pruebas de penetración en caso que aplique y evaluación de riesgos. Así mismo se implementan controles adecuados para abordar cualquier no conformidad o brecha de seguridad identificada.

Terminación o Modificación de Relaciones: Desde el área de Gerencia Legal y de Cumplimiento se establecen procedimientos claros para terminar o modificar las relaciones con los proveedores cuando las preocupaciones de seguridad no se puedan abordar adecuadamente o el proveedor no cumpla con los estándares de seguridad de la organización.

10.4. Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores: CLINALTEC establece las siguientes consideraciones:

El Gerente Legal y de Cumplimiento deberá mantener registros precisos y actualizados de todos los acuerdos de servicios con proveedores, incluyendo acuerdos de nivel de servicio (SLA) que definen las expectativas de rendimiento y las medidas correctivas por incumplimiento.

10.5. Gestión de Incidentes:

Los empleados de **CLINALTEC** tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, **CLINALTEC** deberá implementar procedimientos para la correcta gestión de los incidentes detectados.
Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

Implementación de Acciones Correctivas y Preventivas: Tomar las medidas adecuadas para abordar las preocupaciones inmediatas planteadas por el evento y prevenir situaciones similares en el futuro. Esto puede incluir:

Acciones de Contención: Medidas para aislar y contener el evento para minimizar su impacto posterior.

Acciones de Erradicación: Pasos para eliminar la causa raíz del evento y abordar cualquier vulnerabilidad o debilidad que haya sido vulnerada.

Acciones preventivas: Implementar cambios en procesos, controles o capacitación para evitar que vuelvan a ocurrir eventos similares.

10.6. Continuidad de Negocio:

Respondiendo a requerimientos de calidad y buenas prácticas, **CLINALTEC** deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que **CLINALTEC** actúe en caso de ser necesario. Este Plan de Continuidad deberá ser actualizado y probado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, este plan abarca la continuidad del funcionamiento de las tecnologías de información y comunicación.
CLINALTEC deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

10.7. Cumplimiento de Políticas, Normas y Estándares de Seguridad de la Información: CLINALTEC establece las siguientes consideraciones.

El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente y se abordará con prontitud cualquier problema de incumplimiento identificado a través de auditorías u otros medios, tomando acciones correctivas para remediar la situación y prevenir futuras ocurrencias.

11. CONTROLES DE PERSONAS.

11.0. Selección: La Jefatura Departamento de Gestión Humana aplicará los controles de verificación de antecedentes de todos los candidatos para convertirse en personal que se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y la riesgos percibidos.

11.1. Términos y Condiciones de Empleo: El Gerente Legal y de Cumplimiento incluirá obligaciones de seguridad en los contratos de trabajo para definir claramente las

responsabilidades del empleado en la protección de los activos de información, incluida la confidencialidad, el manejo de datos y el reporte de incidentes de seguridad.

11.2. Concientización, Educación y Capacitación en Seguridad de la Información: El área de seguridad de la información capacitará al personal de la organización y las partes interesadas relevantes formación y concienciación regulares y eficaces para educar acerca de los riesgos de seguridad de la información, sus responsabilidades individuales y el comportamiento adecuado para proteger la información confidencial.

11.3. Proceso Disciplinario: Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información, ayudando a proteger los activos de información al minimizar el riesgo de violaciones de seguridad causadas por comportamientos no conformes y a su vez refuerza la importancia de la seguridad de la información dentro de la organización al demostrar la gravedad del incumplimiento.

11.4. Responsabilidades Después de la Terminación o Cambio de Empleo: Se deberán establecer procedimientos claros para administrar el acceso a los activos de información y devolver la propiedad de **CLINALTEC** cuando finaliza el vínculo laboral de un empleado o cambia su función. Este control tiene como objetivo minimizar el riesgo de acceso no autorizado, filtraciones de datos y pérdida de información confidencial durante las transiciones de los empleados.
Tras la terminación o un cambio significativo de rol, se debe revocar o restringir inmediatamente por parte del área TICs el acceso del empleado a los sistemas de información, redes y activos físicos para evitar el acceso no autorizado.

11.5. Acuerdos de Confidencialidad o No Divulgación: El Gerente Legal y de Cumplimiento establecerá acuerdos formales con colaboradores y terceros para proteger la información confidencial cuando se comparte o divulga. Este control tiene como objetivo minimizar el riesgo de acceso no autorizado, filtraciones de datos y uso indebido de información confidencial.
Estos acuerdos deben ser identificados, documentados, revisados y firmados por el personal y otras partes interesadas relevantes.

11.6. Trabajo remoto: Se deberá controlar el acceso remoto a la red de **CLINALTEC** en la modalidad de trabajo a distancia, esto es, desde fuera de las instalaciones propias.
Los servicios de conexión al trabajo remoto estarán destinados exclusivamente a personal de **CLINALTEC**. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del área de seguridad de la información. (Véase, Política Trabajo Remoto)

11.7. Informe de Eventos de Seguridad de la Información: Todos los empleados de **CLINALTEC** tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad de la información de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, **CLINALTEC** deberá implementar procedimientos para la correcta gestión de los incidentes detectados.
Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

12. CONTROLES FÍSICOS.

12.0. Escritorio Limpio y Pantalla Limpia: Se establecen los siguientes requisitos con el objetivo de mantener la seguridad en los puestos de trabajo:

Se deberá bloquear la sesión de los equipos cuando el empleado deje el puesto, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.

Se deberá dejar recogido el entorno de trabajo al finalizar la jornada. Esto incluye la necesidad de que todo documento o soporte de información quede fuera de la vista, guardando bajo llave los que por su clasificación sean confidenciales o secretos.

Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

12.1. Seguridad de los Activos Fuera de las Instalaciones: Identificar y clasificar todos los activos de información que puedan sacarse de las instalaciones, como computadoras portátiles, dispositivos móviles, medios extraíbles y documentos.
Implementar medidas de seguridad física para proteger los activos fuera de las instalaciones del acceso no autorizado, robo o daño. Esto puede incluir almacenamiento seguro, contraseñas seguras, cifrado y mecanismos de rastreo.

13. CONTROLES TECNOLÓGICOS.

13.0. Dispositivos de Punto Final de Usuario: enfatiza la importancia de proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final de usuario (PC Portátil, laptop, notebook, tablet, dispositivos móviles, etc).
Este control tiene como objetivo salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.

USO DEL DISPOSITIVO MÓVIL

● En cualquier momento el área de Seguridad de la Información podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles.

● **CLINALTEC** pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos.
● Con el fin de dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir las directrices consignadas en el Reglamento de uso de Dispositivos móviles.

USUARIO DE DISPOSITIVO MÓVIL

El personal que haga uso del dispositivo móvil asignado por **CLINALTEC**, deberá:

a. Antes de empezar a usar el equipo, el usuario deberá leer y aceptar la **política de seguridad y privacidad de la información y sus políticas asociadas al reglamento.**

b. Mantener la configuración del dispositivo, los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

c. No almacenar información personal en los dispositivos móviles asignados.

d. Está prohibido realizar instalación de aplicaciones no autorizadas.

e. Se autoriza el uso de WhatsApp, sin embargo, no se permite por esta aplicación el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

f. Configurar sólo las cuentas organizacionales en los dispositivos de **CLINALTEC** que tendrán acceso a la información de la Entidad.

g. En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de **CLINALTEC**, se debe reportar la pérdida a la Gerencia TICs y al área de seguridad de la información lo más pronto posible por medio de los canales de atención autorizados.

13.1. Gestión de Dispositivos BYOD o Dispositivos Personales: CLINALTEC permitirá la política conocida como BYOD (Bring Your Own Device), que permite a los empleados utilizar sus recursos o dispositivos móviles personales para acceder a recursos o información de la entidad; Adicionalmente, los usuarios deberán tener en cuenta una serie de requisitos establecidos en esta Política:

a. Se deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos BYOD que tratan información igual que al resto de dispositivos de **CLINALTEC**.

b. El usuario será responsable de los equipos BYOD.

c. Los usuarios deberán mantener actualizado el dispositivo BYOD personal donde traten información de cualquier tipo de **CLINALTEC**.

d. Los empleados deberán recibir autorización de su responsable de área para utilizar dispositivos BYOD.

e. Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos debe ser reportada al responsable de seguridad de la información por medio de los canales autorizados.

13.2. Control y Derechos de Acceso: Enfatiza la importancia de restringir y gestionar la asignación y el uso de los derechos de acceso a los diferentes sistemas de información de la entidad y que dicho acceso se utilice de manera adecuada y para fines legítimos.

● Cada usuario debe tener una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y “contraseña” deben ser únicos.

● Los nombres de usuario y “contraseña” son personales e intransferibles, y solamente deben ser utilizados por el funcionario al que le fueron asignados. Está totalmente prohibido que un funcionario autorice el uso de clave a terceros o que preste sus credenciales de acceso.

● Todo funcionario será responsable de las actividades y transacciones que sean realizadas con su “usuario y contraseña” de carácter confidencial.

● Los derechos de acceso de los usuarios a las transacciones específicas de cada uno de los sistemas de información deben estar formalmente autorizados por **CLINALTEC** a través del área Gerencia TICs.

● Siempre que sea posible, se deberá de disponer de un doble factor de autenticación (MFA) para el acceso a los sistemas de información, siendo obligatorio para aquellos que puedan ser accesibles desde redes públicas

● Notificar de acuerdo a lo establecido en la política de **reporte de Incidentes** de seguridad de la información, cualquier incidente relacionado con sus contraseñas:
a. Pérdida
b. Robo
c. Indicio de pérdida de confidencialidad.

● El área Gerencia TICs es responsable de dejar deshabilitados los derechos de acceso de manera inmediata a aquellos funcionarios que presenten novedades de personal (retiro, incapacidad, permisos, traslados y otros), basándose en la información o novedades reportadas por la Jefatura Departamento de Gestión Humana. En caso de requerir el acceso a la cuenta del usuario, el Jefe Directo autorizará si así lo requiere los nuevos accesos del personal de reemplazo de los privilegios que fueron suspendidos temporalmente hasta el regreso del titular.

13.3. Eliminación de la Información: Se centra en la eliminación segura y adecuada de la información que ya no es necesaria o que ha alcanzado el final de su ciclo de vida útil. Esto implica establecer procedimientos y controles para garantizar que la información sensible no se divulgue accidentalmente o sin autorización, y para proteger la privacidad de los datos.

Por lo tanto **CLINALTEC** se deben implementar las siguientes medidas para la información confidencial se proteja:

● Definir criterios para determinar qué información ya no es necesaria o ha alcanzado el final de su ciclo de vida útil.

● Implementar un proceso de autorización formal para la eliminación de información, asegurando que solo las personas autorizadas puedan aprobar la eliminación.

● Establecer métodos de eliminación seguros y efectivos para diferentes tipos de información, como trituración de documentos físicos, eliminación segura de archivos electrónicos y borrado de datos en medios de almacenamiento.

● Implementar procedimientos para verificar que la información se haya eliminado de manera efectiva y que no se pueda recuperar.

● Documentar el proceso de eliminación de información y mantener registros de las actividades de eliminación.

13.4. Gestión de copias de seguridad: Se centra en la implementación de un proceso de copia de seguridad de la información eficaz para proteger los datos y sistemas de **CLINALTEC** contra pérdidas o daños. Las copias de seguridad permiten restaurar la información y los sistemas en caso de un incidente, como un ataque cibernético, un desastre natural o una falla del sistema.

Por lo tanto **CLINALTEC** se deben implementar las siguientes medidas para restaurar la información ante un incidente de seguridad:

- Establecer una política formal que defina los tipos de información que se deben respaldar, la frecuencia de las copias de seguridad, los métodos de respaldo y los procedimientos de restauración.

- Utilizar soluciones de copia de seguridad adecuadas para diferentes tipos de información y sistemas, como copias de seguridad locales, copias de seguridad remotas y copias de seguridad en la nube.

- Realizar pruebas periódicas de las copias de seguridad para verificar su integridad y capacidad de restauración.

- Documentar los procedimientos de copia de seguridad y mantenerlos actualizados para garantizar su correcta ejecución.

- Capacitar a los empleados sobre la importancia de las copias de seguridad y los procedimientos de respaldo adecuados.

13.5. Prevención de fugas de información

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.
Se deberán analizar los vectores de fuga de información, en función de las condiciones y operativa de trabajo. Para ello, se deberán identificar los activos cuya fuga supone mayor riesgo para **CLINALTEC**, basándose en la criticidad del activo y el nivel de clasificación que la información tenga. Además, se deberán identificar las posibles vías de robo, pérdida o fuga de cada uno de los activos en sus diferentes estados del ciclo de vida.

CLINALTEC deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Se deberá asegurar la formación y capacitación de todos los empleados en torno a buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Proceso para el manejo de dispositivos de alta criticidad conocidos
- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares
- Uso del correo electrónico
- Impresión de documentación
- Salida de documentación
- Uso de dispositivos móviles
- Uso de Internet
- Escritorios limpios y ordenados (Política de mesas limpias)
- Equipos desatendidos

14.0. CUMPLIMIENTO REGULATORIO:

CLINALTEC deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

14.0. Auditorías de Seguridad y Gestión de Vulnerabilidades:

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la **CLINALTEC**, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado. Una vez identificadas las vulnerabilidades, se deberán aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

14.1. Gestión de Excepciones:

Cualquier excepción a la presente Política de Seguridad y Privacidad de la Información deberá ser registrada e informada al responsable del área de Seguridad de la Información de **CLINALTEC** que corresponda. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir en base su categorización del riesgo, definiendo la viabilidad de la excepción o negación de la misma.

Cualquier tipo de excepción debe contar con la aprobación adicional de la Alta Gerencia.

14.2. Comunicación y Socialización de Políticas: Todo(a) funcionario(a) o contratista que ingrese a **CLINALTEC**, deberá recibir capacitación sobre las políticas establecidas en el presente manual en el momento de su inducción.
La Jefatura Departamento de Gestión Humana remitirá con la debida anticipación a oficina de seguridad de la información, la información de fecha, hora y lugar de las jornadas de inducción.

14.3. Sanciones Disciplinarias:

Cualquier violación de la presente Política puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de **CLINALTEC**. Es responsabilidad de todos los empleados de **CLINALTEC** notificar al responsable del área de Seguridad de la Información de cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

14.4. Revisión de la Política:
La aprobación de esta Política implica que su implantación contará con el apoyo de la Alta Gerencia para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.
La presente Política de Seguridad de la Información, será revisada y aprobada anualmente por el comité de Seguridad de la información. No obstante, si tuvieran lugar cambios relevantes o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de **CLINALTEC**.

15. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO	PARTICIPANTES
12-06-2024	00	Emisión del documento	Carlos Andrés Cano Guzmán Oficial de seguridad de la información.

16. APROBACIÓN DEL DOCUMENTO

ELABORÓ	REVISÓ FONDO	REVISO FORMA	APROBÓ

Carlos Andrés Cano Guzmán Oficial de seguridad de la información.	Comité de Seguridad de la Información	Margarita Villanueva Ref. Planeación y Mejoramiento Continuo	Juan Camilo Arbeláez Vicepresidente General
FECHA Junio de 2024	**FECHA** Junio de 2024	**FECHA** Junio de 2024	**FECHA** Junio de 2024