# POLITICA DISPOSITIVOS MOVILES, EQUIPOS PORTATILES Y MEDIOS INFORMÁTICOS

Esta política ha sido diseñada para establecer un marco integral de protección que garantice la confidencialidad, integridad y disponibilidad de nuestros datos, así como la seguridad de nuestros activos tecnológicos. Al adherirnos a esta política, buscamos fortalecer nuestra postura de seguridad y mitigar los riesgos asociados con el uso de equipos móviles, equipos portátiles y medios informáticos en el ámbito laboral.

## 1. OBJETIVO

El propósito de esta política es establecer directrices claras para proteger la información sensible y los activos de nuestra organización cuando se utilizan equipos móviles, portátiles o medios informáticos como discos duros y memorias USB.

## 2. ALCANCE

Esta política se aplica a todos los empleados, contratistas y terceros que utilicen equipos móviles, equipos portátiles y medios informáticos propiedad de la organización o que accedan a recursos corporativos en sus dispositivos personales. La política también se extiende a cualquier información confidencial o recursos de TI que se almacenen o procesen en estos dispositivos.

## 3. RESPONSABLE

- Coordinador de TI
- Líder de infraestructura
- Oficial de seguridad de la información
- Usuarios finales

## 4. DEFINICIONES

**Acuerdo de nivel de servicio (SLA)(ANS):** Service Level Agreement (SLA). Un acuerdo entre un proveedor de servicios de Tecnologías de la Información (TI) y un cliente que en este caso será la Oficina de Tecnología e Informática.
**Auditoria:** La auditoría se refiere a la evaluación sistemática, independiente y documentada para obtener evidencia objetiva y evaluarla de manera imparcial con el fin de determinar en qué medida se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).
**Capacidad**: El máximo rendimiento que se puede obtener de un Ítem de configuración o Servicio de TI con el objetivo de cumplir los niveles de servicio acordados.
**Ciberseguridad:** La ciberseguridad se refiere a la protección de los sistemas y datos informáticos contra el acceso no autorizado, el uso malintencionado, la modificación, el robo o la destrucción. La ciberseguridad incluye medidas técnicas, físicas y administrativas para proteger la información. (ISO/IEC 27001:2022).
**Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (mintic, s.f.)
**Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (mintic, s.f.)
**Incidente de seguridad de la información:** Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.
**Información:** Datos relacionados que tienen significado para la entidad1. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (mintic, s.f.)
**Riesgos:** Los riesgos se refieren a la posibilidad de que ocurra un evento que pueda tener un impacto negativo en un proyecto, una organización o una persona. Los riesgos pueden ser internos o externos, y pueden ser gestionados mediante la identificación, evaluación y mitigación. (ISO/IEC 27001:2022).
**Sistema de Información:** Conjunto de aplicaciones, servicios, tecnología de información u otros componentes de manejo de información. (ISO/IEC 27001:2022).
**Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. (mintic, s.f.)
**Id.:** Un Id. de usuario es un identificador único de cliente mediante el cual un anunciante elige identificar a un usuario que visita su sitio web. (Ayuda de Google Ads, s.f.)
**TI.:** El concepto de tecnología de la información refiere al uso de equipos de telecomunicaciones y computadoras (ordenadores) para la transmisión, el procesamiento y el almacenamiento de datos. (Pérez Porto, 2014).

## 5. DIRECTRICES GENERALES

- Todos los empleados, contratistas y usuarios que utilicen equipos móviles, portátiles y medios informáticos deben cumplir con esta política y ser responsables de proteger la información y activos de la ESE ISABU – Instituto de Salud de Bucaramanga.
- Todos los empleados, contratistas y usuarios que utilicen equipos móviles, portátiles y medios informáticos son responsables de su cuidado y custodia deberán presentar según sea el caso el paz y salvo emitido por el Almacenista general, en constancia de entrega total de los bienes asignados por la ESE ISABU
- Todos los empleados, contratistas y usuarios que utilicen equipos móviles, portátiles y medios informáticos una vez finalizado contrato o cuando se retiren definitivamente deberán presentar al jefe inmediato o supervisor del contrato
- Cualquier dispositivo utilizado fuera de las instalaciones que almacene o procese información ya sean corporativos o equipos personales y que sean usados para actividades de la ESE ISABU - Instituto de Salud de Bucaramanga debe contar con autorización de su jefe inmediato.
- No se debe dejar equipos desatendidos ni medios de almacenamiento fuera de las instalaciones en lugares públicos y no seguros.
- Proteger los equipos en todo momento frente a temas como, por ejemplo: agua, calor, humedad, polvo, o cualquier elemento que pueda dañar o deteriorar el equipo.
- Para retirar los equipos de cómputo de la entidad, se requiere la respectiva autorización por parte del jefe inmediato.
- Donde técnicamente sea posible se habilitará en equipos móviles la opción de geolocalización y borrado seguro por medio de una herramienta tecnológica.

## 5.1 POLITICA DE SEGURIDAD DE LA INFORMACION DE DISPOSITVOS MOVILES Y EQUIPOS PORTATILES

### 5.1.1 REQUISITOS MINIMOS DE SEGURIDAD

- Los equipos móviles y equipos portátiles deben contar con un software de antivirus.
- Se debe establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital para dispositivos móviles
- Se debe establecer un mecanismo de control de acceso como contraseña mínima de 8 caracteres, alfanumérica, caracteres especiales, mayúsculas y minúsculas en equipos portátiles.
- Se debe configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Se debe configurar la opción de borrado remoto de información en los dispositivos móviles corporativos, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.
- Se debe realizar cifrado del dispositivo móvil.
- Está prohibido descargar e instalar aplicaciones no autorizadas o de fuentes no confiables en los dispositivos móviles y equipos portátiles.
- Está prohibido almacenar información personal en los dispositivos móviles o equipos portátiles asignados por la ESE ISABU- Instituto de salud de Bucaramanga
- Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.

### 5.1.2 GESTIÓN DE ACTIVOS

- Se debe mantener un inventario actualizado de todos los equipos móviles y portátiles de propiedad de la ESE ISABU – Instituto de salud de Bucaramanga por parte Almacén incluyendo información sobre su estado y asignación a usuarios específicos.
- Al dar de baja o reasignar equipos móviles o portátiles, se debe informar al proceso de Gestión de TICS vía correo electrónico para que se borren de manera segura todos los datos y configuraciones de ser necesario

## 5.2 POLITICAS DE DISPOSITIVOS MOVILES O EQUIPOS DE CÓMPUTO PRIVADOS CON ACCESO A INFORMACION CORPORATIVA

El acceso a la información del ESE ISABU - Instituto de Salud de Bucaramanga a través de dispositivos móviles o equipos portátiles de propiedad de trabajadores, contratistas y/o terceros está sujeto a ciertas restricciones y directrices para garantizar la seguridad y confidencialidad de los datos de la entidad.

### 5.2.1 ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

No se permite transferir ni almacenar información Publica Clasificada, Publica reservada o sensible de la entidad en dispositivos móviles privados y equipos de cómputo privados, ni en sitios o redes públicas como café internet, servicios de nube gratuitos, correos electrónicos personales, WhatsApp, OneDrive, Google Drive, Dropbox, ni cualquier otro medio no autorizado por la Oficina de Gestión de las TICS.

### 5.2.2 USO DE HERRAMIENTAS OFICIALES

Los trabajadores y contratistas deben hacer uso exclusivo de las herramientas y medios suministrados por la oficina de Gestión de las TICS para almacenar, transmitir, procesar y gestionar la información a la que tengan acceso mediante el uso de dispositivos móviles privados y portátiles privados.

### 5.2.3 ELIMINACIÓN DE ACCESOS AL TERMINAR LA VINCULACIÓN LABORAL O CONTRATUAL

En el momento de finalizar la vinculación laboral o relación contractual que permitió el acceso a la información de la ESE ISABU – Instituto de Salud de Bucaramanga a través de dispositivos móviles privados o equipos portátiles privados, los usuarios deben eliminar los accesos a aplicaciones de la entidad en las que se almacene o transmita información corporativa, como por ejemplo el correo electrónico institucional, entre otros.

## 5.3 POLITICAS DE DISPOSITIVOS MOVILES Y EQUIPOS PORTATILES CON ACCESO A INFORMACION CORPORATIVA DE PROPIEDAD DE LA EMPRESA

### 5.3.1 ALMACENAMIENTO DE INFORMACIÓN PERSONAL

Está estrictamente prohibido almacenar información personal en los dispositivos móviles o equipos portátiles asignados por la ESE ISABU - Instituto de Salud de Bucaramanga. Estos dispositivos deben utilizarse exclusivamente para fines laborales y acceso a la información institucional.

### 5.3.2 CONFIGURACIÓN Y SOFTWARE AUTORIZADO

Los empleados, contratistas o terceros deben abstenerse de realizar cambios en la configuración de seguridad o instalar aplicaciones o software no autorizados por la Oficina de Gestión de las TICS de la empresa.

### 5.3.3 PROTECCIÓN FÍSICA Y LÓGICA

Los trabajadores, contratistas o terceros a quienes se les haya asignado dispositivos móviles o portátiles de propiedad de la ESE ISABU - Instituto de Salud de Bucaramanga, deben protegerlos física y lógicamente para prevenir el hurto, acceso no autorizado o divulgación de información institucional sensible.

### 5.3.4 NOTIFICACIÓN DE PÉRDIDA O HURTO

En caso de pérdida o hurto de un dispositivo móvil o equipo portátil de propiedad de la empresa, el trabajador, contratista o tercero responsable del dispositivo debe informar urgentemente a su jefe inmediato en la entidad y a la Oficina de Gestión de las TICS a través de los canales de comunicación autorizados.

Esta política tiene como objetivo proteger la integridad de la información de la entidad y garantizar el uso adecuado y seguro de los dispositivos móviles proporcionados por la ESE ISABU. El incumplimiento de esta política puede tener consecuencias disciplinarias y legales.

Todos los empleados, contratistas y terceros involucrados en el uso de estos dispositivos deben adherirse a estas directrices para salvaguardar la confidencialidad y privacidad de la información corporativa. La Oficina de Gestión de

las TICS supervisará la implementación y cumplimiento de esta política para garantizar la protección de los activos tecnológicos de la entidad.

## 5.4 POLITICA DE SEGURIDAD DE LA INFORMACION PARA MEDIOS INFORMATICOS

La entidad define controles de seguridad para medios extraíbles como discos duros externos, memorias USB y otros dispositivos con el objetivo de proteger la información sensible. Para ello se defines los siguientes lineamientos:

- El uso de medios extraíbles debe ser autorizado y justificado según las necesidades laborales.
- Se prohíbe el uso de medios no autorizados o de origen desconocido.
- Se mantiene un registro de los medios extraíbles utilizados, incluyendo el propósito, el usuario responsable.
- Se cuenta con un seguimiento para asegurarse de que los medios sean devueltos y desinfectados después de su uso.
- Todos los medios extraíbles que contengan información sensible cuentan con cifrado de datos.
- Cualquier medio extraíble se debe escanear en busca de malware antes de conectarse a los sistemas internos.
- Los medios extraíbles se deben almacenar y transportar de manera segura para prevenir pérdidas y robos.
- Donde sea apropiado, se cuenta con la función de bloqueo de escritura en los medios extraíbles para prevenir cambios no autorizados en los datos.
- Se cuenta con procedimientos para la eliminación segura de datos de medios extraíbles que ya no sean necesarios
- En caso de pérdida o hurto de un dispositivo móvil o equipo portátil de propiedad de la empresa, el trabajador, contratista o tercero responsable del dispositivo debe informar urgentemente a su jefe inmediato en la entidad y a la Oficina de Gestión de las TICS a través de los canales de comunicación autorizados.

## 5.5 CAPACITACIÓN Y CONCIENTIZACIÓN

Los empleados, contratistas y usuarios que utilicen equipos móviles deben recibir capacitación periódica, mínimo 1 vez al año en seguridad de la información y en el cumplimiento de esta política, de igual forma se llevarán a cabo campañas de concientización para promover buenas prácticas de seguridad en el uso de dispositivos móviles.

## 5.6 AUDITORÍA

En cualquier momento el oficial de seguridad de la información de la entidad o el equipo de la oficina de gestión de las TICS podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles. Las Auditorías internas o de tercera parte pueden realizar la verificación de las configuraciones de los equipos móviles y su cumplimiento con los lineamientos de esta política.

## 5.7 CUMPLIMIENTO Y AUDITORÍA

El cumplimiento de esta política será verificado mediante auditorías periódicas. Las violaciones a esta política pueden conllevar medidas disciplinarias, incluyendo acciones legales según corresponda.

## 5.8 REVISIONES DE LA POLÍTICA

Esta política será revisada y actualizada según sea necesario para adaptarse a los cambios en la tecnología y las mejores prácticas de seguridad de la información.

Al adherirnos a esta Política, estamos comprometidos a proteger nuestros activos y salvaguardar la información confidencial de nuestra organización. Cada miembro es responsable de cumplir con estas directrices y contribuir a la seguridad de nuestra infraestructura tecnológica. Juntos, fortaleceremos la resiliencia de nuestra organización frente a las amenazas cibernéticas y garantizaremos un entorno seguro y protegido para el uso de la tecnología en beneficio de todos.

## 6 DOCUMENTOS REFERENCIADOS


-, M. D.-M. (2022). NTC ISO/IEC 27001:2022 ANEXO A GTC ISO/IEC 27002:2022, CONTROLES FÍSICOS 7.10 MEDIOS DE ALMACENAMIENTO


## 7 CONTROL DE MODIFICACIONES

| CONTROL DE MODIFICACIONES | | | |
|---|---|---|---|
| **Versión** | **Fecha** | **Descripción de la Modificación** | **Realizada por** |
| 1 | 13-09-2023 | Emisión inicial del documento | Ingeniero de seguridad y privacidad de la información – Proceso de gestión de TI |