POLÍTICAS

S.E.S. Hospital Universitario de Caldas, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de **S.E.S. Hospital Universitario de Caldas**.
- Los activos dispuestos por el **S.E.S. Hospital Universitario de Caldas**. para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de **S.E.S. Hospital Universitario de Caldas**.
- **S.E.S. Hospital Universitario de Caldas** identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Los colaboradores que tengan asignado un equipo de cómputo deberá cerrar la sesión cuando no este trabajando o se pare de su puesto de trabajo.
- Se establecerá una política de cierre de sesión automático 15 minutos después de inactividad del equipo.

CRIPTOGRAFÍA

o **S.E.S. Hospital Universitario de Caldas** implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo/Oficina de Tecnológica de Información y las Comunicaciones determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- **S.E.S. Hospital Universitario de Caldas** adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- **S.E.S. Hospital Universitario de Caldas** definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de **S.E.S. Hospital Universitario de Caldas** deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. **S.E.S. Hospital Universitario de Caldas** planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Grupo de Tecnológica de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes del **S.E.S. Hospital Universitario de Caldas**, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- El **S.E.S. Hospital Universitario de Caldas** definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- El Grupo/Oficina de Tecnológica y Comunicaciones, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- **S.E.S. Hospital Universitario de Caldas** establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.

- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- **S.E.S. Hospital Universitario de Caldas** establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
- El Grupo/Oficina de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

POLÍTICAS DE GESTIÓN DE INCIDENTES

La entidad se compromete a mantener un entorno de seguridad de la información sólido y eficaz. Para lograrlo, se ha establecido esta política de gestión de incidentes en seguridad de la información, que aborda responsabilidades y procedimientos relacionados con la identificación, notificación, valoración, respuesta y aprendizaje de incidentes de seguridad.

Responsabilidades y Procedimientos

a) Responsabilidades: Se designarán roles y responsabilidades claras para la gestión de incidentes de seguridad de la información. Esto incluirá un Equipo de Respuesta a Incidentes de Seguridad (CSIRT).

b) Procedimientos: Se establecerán procedimientos documentados para la identificación, notificación y gestión de incidentes de seguridad de la información.

- **Notificación de Eventos de Seguridad de la Información**

Se requerirá que todos los empleados notifiquen inmediatamente al CSIRT cualquier evento que sospechen que podría ser un incidente de seguridad de la información. Se proporcionarán canales de comunicación seguros y un procedimiento de notificación específico.

- **Notificación de Puntos Débiles de la Seguridad**

La entidad promoverá la cultura de la notificación proactiva de puntos débiles de la seguridad. Se establecerá un mecanismo para que los empleados informen de cualquier debilidad de seguridad identificada sin temor a represalias.

- **Valoración de Eventos de Seguridad de la Información y Toma de Decisiones**

Se implementará un proceso de valoración de incidentes de seguridad que incluirá la categorización, evaluación de impacto y determinación de la respuesta apropiada. La alta dirección estará involucrada en la toma de decisiones clave.

- **Respuesta a los Incidentes de Seguridad**

La entidad se compromete a responder de manera oportuna y eficaz a los incidentes de seguridad. Se definirán procedimientos de respuesta que incluirán la contención, erradicación, recuperación y lecciones aprendidas.

- **Aprendizaje de los Incidentes de Seguridad de la Información**

La entidad buscará el aprendizaje continuo de los incidentes de seguridad de la información. Se realizarán análisis posteriores a los incidentes para identificar debilidades en la seguridad y se implementarán medidas correctivas para evitar futuros incidentes similares.

- **Capacitación y Concientización**

La entidad proporcionará capacitación y concientización en seguridad de la información a todos los empleados, con un enfoque especial en la importancia de la notificación y gestión de incidentes.

POLÍTICAS DE CUMPLIMIENTO

- **S.E.S. Hospital Universitario de Caldas** velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

ESCRITORIO LIMPIO:

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a **S.E.S. HOSPITAL UNIVERSITARIO DE CALDAS**, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números) y deberán contener una longitud mínimo de 8
- No se permite repetir contraseñas anteriores.
  - El umbral de bloqueo por intentos fallido es de 5 intentos.

USO ADECUADO DE DISPOSITIVOS MÓVILES

- Seguridad de la información: Proteger los dispositivos con contraseñas seguras, cifrado y evitar almacenar información crítica sin autorización.
- Acceso a redes: Usar redes seguras o VPN al acceder a información institucional, evitando Wi-Fi públicas no seguras.
- Instalación de aplicaciones**:** Descargar solo aplicaciones necesarias y aprobadas, evitando fuentes no confiables.
- Uso responsable: Utilizar dispositivos solo para tareas laborales, evitando redes sociales y aplicaciones no autorizadas en horario laboral.
- Sincronización y respaldo: Sincronizar y respaldar datos en la nube corporativa autorizada.
- Responsabilidad del usuario**:** Reportar pérdidas o robos de inmediato y cumplir con las políticas de seguridad de la institución.

CONEXIONES A LA RED

- Acceso autorizado: Solo dispositivos y usuarios aprobados pueden conectarse a la red institucional, usando credenciales seguras.
- Seguridad: Es obligatorio usar VPN para conexiones remotas y evitar redes Wi-Fi públicas no seguras.

- Monitoreo: La red será supervisada constantemente, con registros de accesos auditables.
- Uso adecuado: La red debe usarse solo para actividades laborales, evitando sitios no relacionados con el trabajo.
- Actualizaciones: Los dispositivos deben estar actualizados para evitar vulnerabilidades.

SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN
SENSIBILIZACIÓN Y COMUNICACIÓN

S.E.S. Hospital Universitario de Caldas, definirá un "**Plan de Comunicación en Seguridad de la Información"** a través de su oficina de comunicación interna y externa y el Grupo/Oficina TIC, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

CAPACITACIONES EN SEGURIDAD

S.E.S. Hospital Universitario de Caldas, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de **S.E.S. Hospital Universitario de Caldas.**

SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de **S.E.S. Hospital**

Universitario de Caldas de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c. El Grupo TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario **S.E.S Hospital Universitario de Caldas** las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

TABLA DE CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN U ORIGEN DEL CAMBIO	FECHA
00	Elaboración del documento	02/10/2023
01	Se agrega lo siguiente USO DE USUARIOS Y CONTRASEÑAS: Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña. Las credenciales son personales e intransferibles. Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números) y deberán contener una longitud mínimo de 8 No se permite repetir contraseñas anteriores. El umbral de bloqueo por intentos fallido es de 5 intentos. **USO ADECUADO DE DISPOSITIVOS MÓVILES** Seguridad de la información: Proteger los dispositivos con contraseñas seguras, cifrado y evitar almacenar información crítica sin autorización.	26/09/2024

	Acceso a redes: Usar redes seguras o VPN al acceder a información institucional, evitando Wi-Fi públicas no seguras. Instalación de aplicaciones: Descargar solo aplicaciones necesarias y aprobadas, evitando fuentes no confiables. Uso responsable: Utilizar dispositivos solo para tareas laborales, evitando redes sociales y aplicaciones no autorizadas en horario laboral. Sincronización y respaldo: Sincronizar y respaldar datos en la nube corporativa autorizada. Responsabilidad del usuario: Reportar pérdidas o robos de inmediato y cumplir con las políticas de seguridad de la institución. **CONEXIONES A LA RED** Acceso autorizado: Solo dispositivos y usuarios aprobados pueden conectarse a la red institucional, usando credenciales seguras. Seguridad: Es obligatorio usar VPN para conexiones remotas y evitar redes Wi-Fi públicas no seguras. Monitoreo: La red será supervisada constantemente, con registros de accesos auditables. Uso adecuado: La red debe usarse solo para actividades laborales, evitando sitios no relacionados con el trabajo. Actualizaciones: Los dispositivos deben estar actualizados para evitar vulnerabilidades.	