Contenido

1. Objetivos y alcance

- Definir las políticas de seguridad de la información enfocadas en mantener la Confidencialidad, Integridad y Disponibilidad de la información empresarial para el desarrollo de las actividades del negocio.
- Comunicar y crear conciencia de seguridad de la información en todo el personal vinculado con la empresa y partes interesadas con relación con recursos y activos de información.
- Mantener y mejorar continuamente la seguridad de la información para asegurar la disponibilidad de los recursos tecnológicos y la protección de la información del negocio.

2. Compromiso de la Gerencia

La gerencia de la E.S.E Hospital San Vicente de Paul, siguiendo los lineamientos empresariales y las definiciones estratégicas del negocio, muestra su compromiso hacia la seguridad de la información desde la revisión, aprobación, comunicación, ejecución y asignación de recursos necesarios para el desarrollo de las actividades necesarias para lograr la implementación, promoción y mantenimiento de una cultura organizacional enfocada a la seguridad de la información con base en la implementación de un SGSI según la NTC ISO 27001:2013.

3. Objetivos de medición

Se realizarán evaluaciones y análisis de los resultados de las mediciones de puntos críticos en el sistema que permitan evidenciar la evolución del SGSI.

- Atención oportuna a Incidentes de Seguridad en Mesa de Ayuda.
- Disponibilidad de la plataforma tecnológica instalada.
- implementación de mejoras hacia el SGSI.

- Formación personal en SGSI.

4. Responsabilidades

El Comité de Seguridad de la Información es el organismo responsable del desarrollo e implantación de las actividades enfocadas al SGSI, así como de definir y aprobar, las directrices y políticas que la E.S.E Hospital San Vicente de Paul, debe implementar para asegurar la aplicación, evaluación y seguimiento al cumplimiento de las políticas de seguridad de la información definidas.
El comité de seguridad de la información se encarga de realizar revisiones anuales de la política del SGSI, para validar su conveniencia, adecuación, eficacia y mejora continua hacia el SGSI. Se debe dejar registro de la revisión en acta del comité de SGSI.

5. Comunicación de la política

Publicación del documento en la intranet institucional.

Desde la gerencia general en apoyo con el Comité de Seguridad de la información y las áreas requeridas, se definirán los, procedimientos de comunicación apropiados, tanto internos como externos, que posibiliten la correcta divulgación y ejecución de la política, así como el suministro oportuno de información a todas las partes interesadas.
Se deben desplegar comunicaciones a todo el personal con relación a sus responsabilidades y los procedimientos que le competen dentro del SGSI, en pro de la aplicación y cumplimiento del presente documento.

6. Requisitos para la información

Como requisitos para la información E.S.E Hospital San Vicente de Paul, define las necesidades de información con que se debe contar al interior de cada proceso y las actividades propias del negocio para todo tipo de información que incluya el alcance del presente documento.

Identificación: Todos los procesos deben realizar la identificación y registro de los activos de información dentro de los repositorios organizacionales definidos para tal fin y con ello entregar cada uno de los atributos allí solicitado con el fin de lograr la identificación correcta del activo y la información relacionada.

Clasificación: La información contenida en cada activo de información identificado, debe estar clasificada, esta clasificación debe obedecer a los parámetros establecidos por la E.S.E Hospital San Vicente de Paul con la finalidad de contar con el tratamiento adecuado a cada una de ellas.

Asignación: Debe identificarse un responsable de cada activo de información dentro de la lista maestra, este responsable, es un elemento activo dentro del SGSI.

Localización: La información empresarial, debe contar una localización real de cada elemento a través de la identificación de sus activos de información, esto debe estar diligenciado en el repositorio de activos definido por la empresa.

Controlada: Con base en la política del control de acceso, toda la información empresarial, debe estar protegida con relación a su acceso según la definición de la política de control de acceso.

Respaldo: La información debe contar con un medio de respaldo y recuperación de la información, el cual debe estar identificado en la política de respaldo y recuperación, los procesos de backup y los planes de contingencia que se tengan definidos dentro de la organización.

7. Control para la seguridad de la información

Se definen los controles de la seguridad de la información dentro de la E.S.E Hospital San Vicente de Paul indispensables en la disposición de herramientas de TI.

Acceso autenticado: Se debe conservar el control de acceso desde la autenticación de los usuarios a los equipos de cómputo, como el acceso a la información según los perfiles de acceso definidos en cada activo de información.

Uso adecuado recursos: El uso adecuado de los recursos informáticos dispuestos, como equipos de cómputo, accesos servicio empresariales y otros dispuestos por personal de TI, son de uso exclusivo de las actividades propias del negocio, su adecuado uso evita problemas de seguridad y compromisos de la información institucional.

Uso conectividad segura: Se debe conservar la conectividad segura cuando se requiera por medio de los servicios dispuestos de VPN Empresariales y conservar las condiciones de manejo seguro de la información.

Software licenciado: Los equipos de cómputo empresarial, deben contar con software instalado cumpliendo con la normatividad legal vigente en todas las herramientas de software instaladas y para uso de las actividades propias del negocio.

Implementación respaldos: Conservar respaldos de información a nivel de los servicios de sistemas de información, para mantener salvaguardar la continuidad el negocio en la conservación de la información, implementando planes de respaldo y recuperación en todos los sistemas de información aplicables.

8. Continuidad del negocio

- La protección y seguridad de las personas es la primera premisa y el objetivo prioritario, tanto en situaciones normales como en situaciones de crisis derivada de una calamidad.
- Se deben nombrar representantes de las distintas áreas con la debida experiencia y conocimiento, para que participen activamente en la elaboración, implantación, revisión, prueba y actualización de los Planes de Continuidad de Negocio.
- En caso de contratar servicios de seguridad y fiabilidad se deben considerar criterios que garanticen de forma razonable la continuidad de los servicios críticos que son proporcionados.

ESE Hospital San Vicente de Paul, diseñará y socializará los planes de contingencia de los diferentes procesos aplicables, a fin de consolidar un plan de continuidad de negocio apropiado a la necesidad de la compañía.

9. Políticas de seguridad del SGSI

9.1 Política de control de acceso

La política de control de acceso es una definición organizacional, conforme a la postura de seguridad de la información y con base en la infraestructura. Esta política, se aplica con apoyo del personal de TI.

Para cumplimiento de lo anterior se define:

9.1.1 Acceso a equipos de computo

La accesibilidad a los equipos de cómputo institucionales está definida bajo los criterios configurados en el aprovisionamiento inicial de las máquinas y en la definición de control de identidades dentro de la infraestructura de TI. Se debe conservar lo siguiente:

- Acceder a nivel de usuario de dominio, usando únicamente las credenciales del dominio empresarial asignado en el usuario desde el área de TI.

- Los accesos con usuarios administradores en los equipos de cómputo quedan restringidos, solo al dominio y uso del personal autorizado de TI y para tareas de soporte y administración de los equipos de cómputo.

- No se permite la creación de usuario locales de ningún tipo en los equipos de cómputo a personal ajeno al área de TI, esta tarea debe ser solicitada a la Mesa de Ayuda y soporte cuando se requiera.

- Los equipos de cómputo no pueden estar incluidos en dominios ajenos a los autorizados por el personal de TI
- Cada usuario debe hacer uso del equipo de cómputo, bajo las credenciales propias asignadas desde el personal de TI.

9.1.2 Control de claves y nombres de usuario

9.1.2.1 Obligaciones de los usuarios

- Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves.
- No se deben divulgar las claves a otras personas, incluyendo los lideres y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el área de TI.
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio de comunicación, estas son de uso exclusivo.
- El usuario debe implementar claves seguras cumpliendo con los niveles de complejidad definidos por el área de TI, cuando aplique, se sugiere tener en cuenta lo siguiente:
  - Incluir al menos ocho caracteres.
  - Incluir al menos un carácter numérico.
  - Uso de carácter alfabético en mayúscula y minúscula.
  - Usar un carácter especial.
  - No debe ser una palabra común del diccionario.
  - No relacionar, nombres propios, parentescos o información personal conocida.
  - No repetir clave en ningún momento.
  - Atender la periodicidad de cambio de clave.

- En cualquier caso, el usuario debe procurar, construir claves complejas, en todos los sistemas de información que use, aun cuando estos, no obliguen a su construcción.

9.1.2.2 Gestión de claves de usuarios y servicios

Los empleados y colaboradores de la E.S.E Hospital San Vicente de Paul, tiene la obligación de mantener sus claves en forma confidencial, de acuerdo con lo establecido en este documento.

Para cumplimiento de lo anterior se define que:

- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos que corresponda y los sistemas de información lo permitan
- Los usuarios y claves de usuarios administradores, así como claves de super usuarios en aplicaciones, servicios de TI, Servicios de terceros y portales de servicio o autoservicio, que están dispuestos en la organización, deben ser de conocimiento único y exclusivo del personal Administrador de TI.
- Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, de forma que no sean de fácil identificación que permitan suplantaciones tempranas.
- El acceso a información empresarial debe estar controlado y se deben cambiar periódicamente las claves de acceso bajo una política general de cambio de contraseñas dispuesta desde la plataforma tecnológica empresarial.

- Cuando el sistema de información lo permita, debe requerir que el usuario modifique la clave de primer acceso o que el usuario haga su asignación propia desde el primer acceso.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión de los usuarios a los sistemas de información.
- Si un usuario ingresa una clave incorrecta hasta 3 veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión, aplica para las aplicaciones que lo permitan.
- Para el control de claves sensibles, como claves de administración de las herramientas de gestión de la información, Son manejadas exclusivamente por el personal de mesa de ayuda.
- Las claves de acceso deben conservar un nivel de complejidad, tanto a nivel de dominio como de aplicaciones cuando estas permitan su configuración.

9.1.2.3 Acceso a sistemas y aplicaciones

- El líder de cada área solicitara los accesos a los sistemas de información del equipo de personas que tenga a cargo diligenciando el formato definido desde TI. La solicitud será realizada a TI y a la Subgerencia de Servicios de salud, subgerencia Administrativa y financiera o Gerencia. La aprobación será dada por alguna de las Subgerencias o Gerencia de acuerdo con el área que lo requiera y la respectiva ejecución será realizada por el área de TI.
- Los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y una contraseña única por cada colaborador o tercero.
- Cuando se retire cualquier colaborador o tercero, se deberá inactivar el usuario en todos los sistemas de información.

- El área de TI deberá realizar revisiones de permisos de acceso a los diferentes sistemas de información, dejando registro de las revisiones y los hallazgos.
- Las contraseñas deben cumplir con un mínimo de 8 caracteres y contar con definición de complejidad requerida desde el servicio de administración de dominio o de control de identidades.
- Todos los empleados deben cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima mensual, para lo cual se enviarán alertas automáticas periódicas, de acuerdo con las facilidades que ofrezcan las herramientas para este efecto.
- El acceso al sistema Dinámica Gerencial de la E.S.E Hospital San Vicente de Paul se bloqueará para los usuarios luego de 3 intentos fallidos de autenticación. Para las demás herramientas de gestión de información se seguirán los esquemas de bloqueo definidos en las mismas en caso de que los posean.

9.1.2.4 Cambio de estado o finalización de un contrato

- Cuando el personal se retire de la empresa, los lideres, Subgerencias, Gerencia o la Dirección de Talento humano debe notificar lo más pronto posible a la mesa de ayuda (área de TI) o al correo electrónico sistemas@esehospicaldas.gov.co con el fin de retirar accesos a los sistemas de información.
- Cuando se modifican las relaciones contractuales con entidades externas que tienen acceso a sistemas, servicios e instalaciones el gestor del servicio a nivel interno debe informar a la mesa de ayuda.
- Cuando finaliza el contrato, el propietario del contrato debe informar inmediatamente a las personas que autorizaron los privilegios de acceso del

contrato y a la mesa de ayuda para correcta gestión de los accesos disponibles.

- Cuando se generen cambios de cargo y/o funciones, se deben ajustar de los derechos de accesos según lo requiera el nuevo perfil o área del usuario.
- El personal de Talento Humano debe notificar sobre el retiro del personal a mesa de ayuda, a fin de que se haga el retiro de los derechos de acceso asignados.

9.1.2.5 Revisiones periódicas de los derechos de acceso

- El área de TI será responsable de generar reportes de los roles asignados en el sistema Dinámica Gerencial y de enviarla a los lideres de procesos periódicamente con el fin de validar los mismos.
- Los lideres de los sistemas de información en los procesos de revisiones periódicas deben reportar como incidente de seguridad si encuentra alguna desviación sobre en la asignación de privilegios.
- La revisión debe realizarse periódicamente e informarse a la mesa de ayuda para registro como incidente del SGSI.

9.2 Política de borrado seguro

9.2.1 Eliminación de información digital

- Los activos de información como plantillas, formatos, guías y documentos que no estén en uso son pasados a la librería de obsoletos una vez sean reemplazados o se defina que no seguirá siendo usados, de acuerdo con los lineamientos establecidos en el sistema de gestión documental.

- La información electrónica generada debe ser conservada por los periodos indicados en el sistema de gestión documental de la ESE Hospital San Vicente de Paul Caldas.
- Toda información almacenada en PCs, portátiles, y dispositivos móviles como celulares debe ser borrada en caso de que dichos dispositivos cambien de usuario.

9.2.2 Eliminación de información física

- Todos los equipos físicos que almacenen información dentro de la E.S.E, como computadores, portátiles, celulares, discos duros y memorias externas que sean dejados de usar, deben pasar por un proceso de borrado de datos y reacondicionamiento, de acuerdo con los lineamientos definidos al respecto por el área de TI o Mesa de ayuda.
- Conforme a lo anterior, la E.S.E no realiza destrucción física de equipos físicos de almacenamiento de información.

9.3 Política de uso aceptable

Esta política aplica al uso de información, dispositivos electrónicos e informáticos, recursos de red para realizar actividades propias del negocio, acceso a las redes internas y sistemas de información empresariales y todos los recursos dispuestos por la organización.

Todos los empleados de la ESE Hospital San Vicente de Paul Caldas, colaboradores, clientes y partes interesadas con relación con la compañía, son responsables de ejercer el buen juicio con respecto al uso apropiado de información, dispositivos electrónicos y recursos de la red de acuerdo con las políticas y estándares de la empresa, así como la normatividad legal vigente.

Para cumplir lo anterior, se define lo siguiente:

9.3.1 Uso aceptable de los activos de información

9.3.1.1 Generales

- Toda actividad de gestión y operación que se lleve a cabo con los activos de información deben ser encaminada a garantizar el correcto cumplimiento de la misión y objetivos organizacionales de **la ESE.**
- Los colaboradores responsables del SGSI de **la ESE** son responsables del uso adecuado de los activos de la información que son de vital importancia para el desarrollo de los procesos misionales.
- Todos los colaboradores deben reportar, a Gerencia, subgerencias, directores o lideres de procesos en los cuales ejecutan las funciones, cualquier acción que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información.
- Cualquier cambio que se vaya a hacer a los activos de la información y que implique una afectación del servicio, debe seguir el **proceso de cambios definido por la ESE**, a fin de tener una trazabilidad de las modificaciones realizadas en los activos.
- Todos los colaboradores deben aplicar los controles de seguridad de la Información definidos en el SGSI de la **ESE** para reducir los riesgos que afectan a la seguridad de la información.
- Los colaboradores de **la ESE Hospital San Vicente de Paul Caldas** no podrán almacenar información confidencial o restringida en sus computadores personales o cualquier dispositivo de almacenamiento sin el conocimiento previo de área de TI.
- Está prohibido utilizar los activos de información para fines diferentes a los asignados para cada uno de ellos.

9.3.1.2 Uso de activos por fuera de las instalaciones

- Los colaboradores de la **ESE Hospital San Vicente de Paul Caldas** no podrán instalar ningún programa o software propio de la Organización en otros equipos diferentes a los asignados para su uso.
- El uso y seguridad de cualquier dispositivo físico por fuera de la Organización debe estar a cargo de su responsable y debe contar con el visto bueno y autorización del área de TI.
- El usuario es responsable de la protección de los equipos a su cargo para reducir el riesgo no autorizado de acceso a la información y para protegerlo contra pérdida o robo.

9.3.1.3 Devolución de Activos de Información empresarial

- Los empleados y asociados con actividades laborales con **la ESE Hospital San Vicente de Paul Caldas** deben devolver todos los activos asociados a sus actividades.
- El personal de la Mesa de Ayuda debe registrar la devolución de los activos para conservar el registro correcto para exclusión de responsabilidades de los usuarios salientes.
- La información empresarial contenida en dispositivos de TI, debe ser respaldada y almacenada según la disposición de respaldos de información existente.
- Los equipos de cómputo de alquiler deben borrarse completamente sus dispositivos de almacenamiento antes de hacer la devolución al proveedor.
- El personal de Mesa de Ayuda debe entregar equipos sin ningún tipo de información de usuarios anteriores cuando aplique la reutilización de algún equipo de cómputo siempre y cuando sean para funciones diferentes.

9.3.1.4 Instalación de antivirus

- La instalación y administración del software antivirus es controlada por el área de TI. No se deben instalar otros programas antivirus diferentes a los dispuestos por el área de TI. El acceso al personal autorizado a carpetas específicas está limitado sólo para personal que tenga antivirus instalado en sus equipos.

9.3.1.5 Control de cuentas y claves de usuario

- Todo usuario debe acceder siempre a los sistemas de Información autorizados con el nombre de usuario que le ha sido asignado a cada sistema.
- La contraseña es personal e intransferible, por lo que nunca debe cederse o compartirse a terceras personas ni comunicarse por ningún medio escrito.
- Toda acción registrada en la red y en cualquier sistema de información, es única responsabilidad del usuario propietario de la cuenta.
- Las credenciales de acceso a la red y los sistemas de información no deben ser compartidos, el mal uso de la información es responsabilidad del dueño de la cuenta.
- Las contraseñas no se transmitirán de forma oral o escrita cuando exista el riesgo de que terceras personas puedan llegar a conocerlas.
- Cuando un usuario olvide su contraseña se le deberá asignar otra nueva, este deberá solicitarla a través de la Mesa de Ayuda al personal de área de TI.
- Las contraseñas deben ser cambiadas periódicamente, según lo requiera el sistema de seguridad empresarial mediante información desde el propio sistema o cuando el usuario por algún motivo requiera su cambio.

- El acceso al sistema de información ERP/HIS se bloqueará para los usuarios luego de 3 intentos fallidos de autenticación.

9.3.1.6 Manejo escritorio limpio y equipos desatendidos

- Impedir acceso a terceras personas al equipo de cómputo corporativo, acción que puede vulnerar políticas de acceso a la información.
- Evite almacenar información relevante en el escritorio de su equipo de cómputo, esto llamara la atención de un atacante o dejara vulnerable su confidencialidad.
- Al retirarse de su equipo de cómputo en lugares con presencia de terceras personas, bloquee su pantalla para proteger el acceso a la información.
- Ejecutar con frecuencia, mínimamente mensual, la depuración del escritorio a fin de no almacenar información en este sitio.
- En el escritorio, solo deben estar los accesos directos de aplicaciones de uso común.

9.3.1.7 Acceso y uso del internet

- Se debe mantener el acceso a internet exclusivamente a la ejecución de las actividades propias de la organización.
- No descargar música ni videos, ni acceder a ningún tipo de sitio de entretenimiento que distraiga la atención de las actividades laborales.
- No es permitido acceder a sitio de pornografía, drogas, alcohol, webproxys o hacking o cualquier otro sitio que ponga en riesgo la seguridad de la información empresarial.
- No está permitido el uso de correos electrónicos personales dentro de los equipos de cómputo corporativos.

- No se permite, envío o recepción de ningún tipo de información de carácter corporativo por medio de correos electrónicos personales.
- No está permitido revisión, acceso o uso de redes sociales personales dentro de los equipos de cómputo corporativos.
- No está permitido la descarga de software desde internet, sin la previa autorización del personal del área de TI.
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos.

9.3.1.8 Manejo de correos electrónicos y programas de comunicación

- Utilizar la cuenta de correo electrónico corporativo para fines laborales y los estrictamente relacionados con las actividades propias de su trabajo.
- No abrir correos con mensajes en inglés (a menos que los esté esperando) y sospechar de correos que no se espera sean recibidos.
- Todos los mensajes enviados por medio de correo electrónico son de propiedad de la organización, la cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.
- Está prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico, estos mensajes sólo pueden ser enviados por usuarios debidamente autorizados por el área de TI.
- Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores de este, tales como comentarios sobre sexo, raza, religión o preferencias sexuales, tendencia política entre otras que generen algún tipo de discriminación.

- Es responsabilidad del usuario reportar al responsable de TI sobre este tipo de mensajes, quien a su vez deberá reportarla al área que corresponda, en caso de comprometer la seguridad de la información de la entidad.
- Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros.
- Es responsabilidad del Usuario evitar que la información confidencial y/o sensible sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa y escrita del dueño de la información, en cuyo caso los archivos deben viajar en forma Segura (encriptados).
- Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.
- El usuario no está autorizado a eliminar ningún elemento del correo electrónico, sin la autorización expresa de su jefe inmediato o del personal del área de TI.
- La información del correo electrónico corporativo no puede ser extraída de los repositorios organizacionales que disponga el área de TI.
- No está permitido usar la cuenta de correo electrónico corporativa, para suscripciones de carácter personal enfocadas a; redes sociales, periódicos, revistas, ventas por catálogo, recepción de notificaciones o publicidad comercial ajena a la actividad de la empresa, cuentas de recuperación de contraseñas o información de contacto de actividades de carácter personal del empleado, así como ninguna actividad de este que no esté alineadas con la actividad empresarial.

9.3.1.9 Derechos de autor

- En caso de requerirse material o información registrada con derechos de autor no se debe copiar sin la autorización del propietario.
- Los equipos de cómputo empresariales solo pueden usar aplicaciones o software de terceros, que cuenten con el debido licenciamiento en protección de la legalidad del software.
- No está permitido reproducir de forma ilegal, copias de aplicaciones propiedad de la compañía a nivel de licenciamiento para ser extraída a terceras personas.

9.3.1.10 Atención y cuidados equipos de computo

- La mesa de ayuda atiende todos los incidentes y solicitudes relacionadas con el mantenimiento y reparación de equipos de cómputo.
- La mesa de ayuda recibe, clasifica y atiende el incidente
- Los reportes a la mesa de ayuda deben hacerse por parte de los usuarios cuando su equipo presente alguna falla, con la mayor oportunidad posible.
- El usuario, está en la obligación de cuidar el equipo de cómputo, para conservar la perfecta integridad física del mismo, así como toda la información contenida en él.
- El usuario responsable del equipo debe asegurar las siguientes condiciones de cuidado para los equipos de cómputo.

  Permanecer en espacios seguros libres de caída de agua.

  No exponer los equipos a altas temperaturas.

  No exponer el equipo a polvo o suciedad directa.

9.4 Política de almacenamiento de información local

El almacenamiento de la información corporativa, como parte fundamental de los activos de la organización, esta estandarizada desde el área de TI (para los casos que apliquen) en repositorios organizacionales, lo cual, permite su adecuada conservación manteniendo su Confidencialidad, Integridad y Disponibilidad.

Para cumplimiento de lo anterior se define que:

- No está permitido el almacenamiento de información corporativa en los repositorios locales de los equipos de cómputo lo cual deja en riesgo la disponibilidad de la información.
- Si el equipo es portátil y tiene información almacenada localmente, el usuario debe solicitar un respaldo de la información al personal del área de TI.
- La información contenida en los repositorios empresariales drive de usuario, almacenamientos compartidos y equipos de cómputo, es de propiedad exclusiva de la **ESE Hospital San Vicente de Paul Caldas.**
- No se autoriza el almacenamiento de información personal del empleado en los medios de almacenamiento corporativos ni en los equipos de cómputo.
- La empresa no se hace responsable del uso malintencionado, pérdida o daño de la información no corporativa almacenada dentro de los equipos de cómputo empresariales.

9.5 Política de uso dispositivos móviles.

Los dispositivos móviles son activos de información sensibles para el desarrollo de actividades empresariales. El manejo desatendido de sus políticas y su usabilidad pueden comprometer la seguridad de la información corporativa y requiere mayor compromiso del personal a cargo.

Para cumplimiento de lo anterior se define que:

- Se emplearán los recursos móviles solo para las actividades propias del negocio.
- El usuario responsable, mantendrá reserva de la información que por razón de su actividad laboral maneje, y no podrá compartirla, destruirla, alterarla u ocultarla.
- La información empresarial debe estar almacenada en los repositorios corporativos dispuestos para tal fin.
- Los dispositivos móviles son para uso exclusivo de actividades empresariales por lo cual la **ESE Hospital San Vicente de Paul Caldas** no se hace responsable por perdida o uso no intencionado de información de terceros almacenada allí.
- El usuario es responsable de los registros que se generen desde el dispositivo móvil
- No está permitido aparear o suministrar servicio de internet al dispositivo desde ninguna fuente externa a la empresa, llámese, wifi, bluetooth o cualquier medio que permita su exposición a internet o ambientes externos no seguros.
- Toda instalación o desinstalación de software en el dispositivo y en lo posible, ejecutadas por el mismo personal a cargo de este, requiere autorización expresa del personal de soporte de Gestión TI.
- Los únicos autorizados para realizar modificaciones a la configuración original del dispositivo, así como para destapar sus componentes, son los funcionarios de Gestión de TI.
- El usuario debe salvaguardar su equipo y la información contenida del uso de personal no autorizado dentro o fuera de la empresa.

- No está permitido visitar en internet sitios de pornografía, redes sociales, contenido ilegal, mensajería instantánea, descarga masiva, reproducción de música, videos, bolsas de empleo o cualquier sitio que pueda poner en riesgo la información empresarial.
- No abrir ningún tipo de mensaje desconocido, en internet, correos desconocidos o ingresar a sitios donde te exijan información confidencial, personal o empresarial.
- No está permitido descargar ningún tipo de software, sea cual sea su finalidad o uso, las herramientas de este tipo serán proporcionadas por el área de Gestión de TI.

9.6 Política de respaldo, retención y recuperación

ESE Hospital San Vicente de Paul Caldas, define la presente política con el fin de establecer un control de seguridad, que aporte a la conservación de la información del negocio para su posible recuperación, que defina intervalos de procesamiento y verificación que cubran la información empresarial, definida en el alcance del Sistema de gestión de Seguridad de la información.

Para cumplimiento de lo anterior se define que:

- Debe **implementarse un servicio** de **respaldo, retención y recuperación** de la información que permita la conservación de la Integridad, Confidencialidad y disponibilidad de la información.
- El procedimiento de respaldo debe **incluir** toda la información definida en el **alcance del SGSI.**
- La información respaldada dentro del proceso **debe cumplir con pruebas de recuperación** de la información para garantizar la idoneidad de los medios almacenados.

- Las **pruebas** deben ser **documentadas y ejecutadas** para valorar la disponibilidad de cada medio de respaldo y su información.
- La documentación mensual de los procesos de pruebas, deben ser enviados mensualmente al Comité del SGSI.

Se debe cumplir con las siguientes directrices para la administración del servicio descrito en la presente política:

9.6.1 Directrices para el respaldo

- Implementar proceso de respaldo automático de información diariamente para el sistema de información Dinámica Gerencial y Digital Logic (Sistema de información para gestión documental) **.**
- Implementar respaldos totales de los recursos solicitados de forma individual y requeridos por los usuarios de la **ESE Hospital San Vicente de Paul caldas.**
- Por parte de TI, mantener un cuadro detallado de las tareas programas de forma automática de respaldos.

9.6.2 Directrices para la retención

- Definir tiempos de retención dentro de cada tarea programada.
- Desde el área de TI, se debe comunicar los tiempos de retención definidos para cada recurso o tipo de información procesada en los respaldos.
- Cada líder de proceso puede solicitar un tiempo de retención para los respaldos de su información según se requiera por necesidad propia de su proceso.
- El área de TI debe valorar y acordar con el líder del proceso el tiempo adecuado o la estrategia de retención a implementar cuando se requiera.

9.6.3 Directrices para la recuperación

- La recuperación de información granular, debe ser, solicitada a través de la mesa de ayuda.
- Las solicitudes de recuperación solo deben realizarse por el propietario de la información dentro de cada proceso asociado.

9.7 Política de continuidad del negocio

El plan de continuidad de negocio permite actuar de forma diligente y oportuna ante una situación de crisis o de emergencia y que facilite la recuperación oportuna de nuestros servicios en el menor tiempo posible, priorizando la seguridad de las personas, la prestación del servicio, el patrimonio y la reputación organizacional.

Para cumplimiento de lo anterior, se define que:

- Se debe diseñar y mantener un plan de continuidad de negocio.
- Procurar por su divulgación, actualización y mejora.
- Confirmar, liderar y mantener un comité de continuidad del negocio.
- Mantener programas que permitan probar la eficacia de su aplicación.
- Disponer recursos necesarios para su mantenimiento, actualización e implementación.
- Definir objetivos claros de recuperación, que se enmarquen en estrategias que permitan la continuidad del negocio.
- Incluir en la iniciativa de continuidad, la prestación de los servicios a terceros y partes interesadas.
- Capacitar continuamente al personal en estrategias de continuidad de negocio a nivel empresarial y proyectos.
- Desarrollar revisión del plan de continuidad por lo menos una vez al año.

9.8 Política de gestión del cambio

Esta política, define el flujo de trabajo y la forma como se controlan los cambios a nivel organizacional **donde se puedan presentar impactos dentro de los procesos de negocio y la seguridad e la información**.

Para cumplimiento de lo anterior, se define que:

- Los cambios organizacionales son propuestos por lideres de procesos y personal de gerencia en todos los niveles de la organización.
- Las solicitudes de gestión de cambio deben seguir las actividades de control descritas en el procedimiento de gestión del cambio definido en la ESE Hospital San Vicente de Paul de Caldas
- Todos los procesos de gestión de cambio deben cumplir con la totalidad de requisitos validados por las partes interesadas.
- El encargado de gestión del cambio debe ejercer seguimiento y control de las actividades propias de los cambios autorizados.
- Todo proceso de cambio debe contar con un cronograma aprobado.
- Terminada la implementación del cambio, el área de procesos debe validar la eficacia de la implementación para proceder el cierre.

9.9 Política de acceso remoto

Las conexiones remotas desde el exterior de las compañías, dadas por los mismos empelados o por terceros como proveedores y partes interesadas, deben ser autorizadas y controladas por personal de TI para garantizar uso de herramientas apropiadas y la protección de la información corporativa.

Para cumplimiento de lo anterior se define que:

- Las conexiones remotas solo son admitidas a proveedores con servicios de soporte activos mediante contrato con alguna solución de software contratada.

- Las conexiones remotas, se autorizan exclusivamente por el personal de TI teniendo en cuenta conservar la seguridad de la información corporativa.

- Si el usuario lo requiere, puede solicitar acompañamiento en la sesión de trabajo al personal de TI durante el tiempo que dure la sesión de soporte remoto del proveedor.

- Ningún empleado de la organización, ajeno al área de área TI, está autorizado para establecer en cualquier dirección, comunicación con acceso remoto a los equipos de cómputo empresariales.

- Las conexiones remotas de los empleados hacia los recursos organizacionales deben hacerse a través de los equipos corporativos asignados.

- Según el requerimiento de servicio y las disposiciones de TI, deben usarse expresamente las aplicaciones que el área de TI suministra a nivel de VPN, Google Meets entre otras dispuesta en la plataforma tecnológica empresarial.

- No usar redes públicas para conectar los equipos de cómputo empresariales, ni para el acceso a los servicios dispuestos por la organización.

- Use siempre conexiones de su red de hogar, o conexiones de confianza en términos de acceso de terceras personas para evitar ataques informáticos.

9.10 Política de creación de usuarios

El área de TI permitirá el acceso a los recursos tecnológicos, mediante la creación de una cuenta de usuario de dominio, que permita su identificación dentro de la red y con este el acceso a otros recursos empresariales dispuestos.

Para cumplimiento de lo anterior se define que:

- El Jefe inmediato, hace la solicitud de creación de usuario en la red, especificando en el formato para solicitud de creación de usuarios cuando sea necesario; datos del usuario, rol o perfil de acceso, listado especifico de los sistemas de información y/o equipos que requiere (Dinámica gerencial, correo electrónico, internet, telefonía, portátil, equipo de cómputo, entre otros) para el desarrollo de las actividades del cargo.
- La aprobación de la creación de los usuarios debe ser realizada por las Subgerencias (Servicios de Salud o Administrativa y financiera) o la Gerencia.
- El personal del área de TI debe asegurar la transferencia de archivos del proceso con relación al usuario anterior del cargo si existe, así como los contenidos de los archivos del correo electrónico cuando el cargo así lo requiera.
- El personal del área de TI debe asegurar la conservación de los archivos de los usuarios salientes y generar los repositorios individuales del nuevo usuario durante la creación del perfil.
- El personal del área de TI debe asegurar que los usuarios creados, se asignan correctamente a los perfiles de usuario definidos en los niveles de seguridad y distribución desde el AD (Directorio Activo).
- Se debe asegurar, que los usuarios creados cumplen con las necesidades del jefe inmediato con relación a las herramientas y servicios requeridos para las actividades empresariales.

- El usuario creado, solo debe contar con el licenciamiento de software estricto que fue solicitado por su jefe inmediato o líder de proceso.

10. Control de cambios

Versión	Ítem	Descripción del cambio	Razón del cambio	Elaborado por	Revisado por	Aprobado por	Fecha
01		Creación de las políticas del SGSI		Diana Isabel Posada Villada Posada Director técnico Gobierno Digital, Tecnología e Información	Oficina asesora de planeación	Subgerencia administrativa y financiera	31/05/2022