PROCEDIMIENTO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2023-2025

E.S.E HOSPITAL SAN JOSÉ
SAN BERNARDO DEL VIENTO

TABLA DE CONTENIDO

1. Introducción

La E.S.E Hospital San José de San Bernardo del Viento busca afrontar los retos del negocio con una infraestructura digital moderna, robusta y segura, capaz de sacar provecho de la llamada cuarta revolución industrial "La transformación digital", En general, el cambio obligatorio desde la simple digitalización a la innovación basada en combinaciones de tecnologías está obligando a las empresas a reexaminar la forma de hacer negocios. Por lo que para el hospital se debe dar prioridad a la seguridad de la información, cumpliendo los lineamientos de los estándares ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines y el ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls como complemento a los requisitos de seguridad, los cuales consisten en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de gestión de riesgo, para lo cual, se busca estar alineados con las exigencias del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, (MinTic).

El grupo de necesidades de información lo conforman el conjunto de requerimiento de información, activos y datos que se necesitan para la ejecución de las estrategias, el cumplimiento de sus objetivos y metas del negocio. Existen diferentes fuentes de información a tener en cuenta en la construcción del Plan Estratégico de Tecnologías de la Información y Comunicación – PETIC, finalmente en éste se consignan todas las iniciativas y oportunidades tecnológicas de la institución, considerando su estado actual y definiendo un estado futuro que se construye a partir de la puesta en marcha de diferentes esfuerzos, proyectos, programas, iniciativas y compromisos.

La información es un activo vital para el éxito y la continuidad de negocio del Hospital, el aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización; siendo necesario planear e implementar un sistema de gestión de seguridad de la información que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que están sometidos los activos de información del hospital.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, permite alinearse a los siguientes componentes y habilitadores:

TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las TIC. Así mismo, busca fortalecer las competencias T.I. de los servidores públicos, como parte fundamental de la capacidad institucional.

TIC para la Sociedad: tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, políticas y normas, y la identificación de soluciones a problemáticas de interés común.

Arquitectura: Busca fortalecer las capacidades de gestión de T.I. de las entidades públicas, a través de la definición de lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.

Seguridad y Privacidad: Busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Servicios Ciudadanos Digitales: Busca facilitar y brindar un adecuado acceso a los servicios de la administración pública haciendo uso de medios digitales, para lograr la autenticación electrónica, interoperabilidad y carpeta ciudadana, esto será posible a través de la implementación del Modelo de Servicios Ciudadanos Digitales.

El presente documento es el resultado de la actualización correspondiente a la vigencia 2021.

2. Objetivo

Planear e implementar las estrategias para la gestión de seguridad y privacidad de la Información en el Hospital San José de San Bernardo del Viento que permitan minimizar los riesgos de pérdida de activos de la información, alineadas a las directrices emanadas por MinTIC y acordes con las necesidades del hospital.

2.1. Objetivos específicos

- Realizar un diagnóstico de la situación actual de seguridad de la información mediante auditorías para identificar las brechas del sistema y los aspectos a mejorar.
- Definir un plan de trabajo para lograr la implementación del modelo de seguridad y privacidad de la información en el hospital.
- Comunicar e implementar la estrategia de seguridad de la información.
- Definir las responsabilidades relacionadas con el manejo de la seguridad de la información.
- Establecer una metodología de gestión de la seguridad de la información clara y estructurada.

- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Reducir el riesgo de pérdida de confidencialidad, integridad y disponibilidad de los activos de información.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios y de las operaciones necesarias de negocio tras incidentes de gravedad.
- Definir el plan para la transición de lPv4 a IPv6.

3. Alcance

El MSPI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de la información en los procesos que se ejecutan en el Hospital, aplica a todos los niveles del hospital, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del hospital compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

Este documento indica cuáles serán las labores que realizará el hospital con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos del hospital, definiendo plazos anuales.

4. Glosario de términos

- **Activo de información**: aquello que es de alta validez y que contiene información vital del hospital que debe ser protegida.
- **Amenaza**: Es la causa potencial de un daño a un activo de información. Es toda aquella acción o elemento capaz de atentar contra la seguridad de la información.
- **Análisis de riesgos**: Utilización sistemática de la información disponible, para

identificar peligros y estimar los riesgos.

- **Antivirus**: Software encargado de detectar, bloquear y eliminar virus informáticos o código malicioso.
- **Ataque**: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad; también se puede afirmar que es cuando se materializa una amenaza de seguridad.
- **Causa**: Razón por la cual el riesgo sucede.
- **Código malicioso**: Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos y spyware. Puede utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo, pen-drives).
- **Controles**: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
- **Diseño de Red Segura**: Definición de un esquema de red aplicando medidas de seguridad informática, que una vez implementadas minimizan los riesgos de una intrusión
- **Disponibilidad**: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.
- **DMZ**: Una DMZ o una zona desmilitarizada, es un segmento de red específico, en el cual se ubican servicios específicos de red que son públicos a redes poco seguras como Internet.
- **Estándar de seguridad**: Conjunto de normas o modelos diseñados con la finalidad de brindar soluciones de sistemáticas a un área del conocimiento específico.
- **Firewall**: Un firewall o también llamados corta fuego, es un software o hardware que restringe el acceso a sitios web o una red sin autorización de acceso.

- **Impacto**: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
- **Incidente de seguridad de la información**: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
- **Incidente de seguridad**: Un incidente de seguridad es cualquier acción que atente
- **Ingeniería social**: es la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas.
- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Intrusos**: Es una Persona que intenta acceder a un sistema informático sin autorización, a través de técnicas y/o métodos informáticos que se lo permitan. ISO: (International Organization for Standardization). Organización internacional de estándares
- **Metodología**: Es un conjunto de reglas o métodos organizados de forma sistémica con el objetivo de lograr el cumplimiento de una norma o un estándar.
- **Plan de contingencia**: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.
- **Pphishing**: Wi-phishing, sustracción de datos personales a través de falsas redes públicas de acceso Wi-Fi.
- **Probabilidad de ocurrencia**: Posibilidad de que se presente una situación o evento específico.
- **Propietario del riesgo sobre el activo**: Persona responsable de gestionar el riesgo.
- **Red de Datos**: Es aquella infraestructura o red de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.
- **Red Privada virtual VPN**: Sistema de telecomunicación consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente los recursos de una red de acceso público, es decir, es una

extensión de la red privada de una organización usando una red de carácter público.

- **Repudio**: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación.
- **Responsables del Activo**: Personas responsables del activo de información.
- **Riesgo Inherente**: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- **Riesgo Residual**: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.
- **Riesgo**: Grado de exposición de un activo que permite la materialización de una amenaza.
- **Riesgos**: Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información. Departamento de seguridad.
- **Seguridad de la Información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO/IEC 27000:20184). SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.
- **Seguridad física**: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, entre otros. SGSI: Sistema de gestión de la seguridad de la información,
- **Seguridad lógica**: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.
- **Sistema de Gestión de Seguridad de la información SGSI**: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001:2013.
- **Teletrabajo**: El teletrabajo es un nuevo sistema de organización del trabajo en que la persona trabajadora desarrolla una parte importante de su trabajo fuera de la empresa y por medios telemáticos.
- **Vulnerabilidad**: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por

ausencia en controles de seguridad que permite ser explotada.

- **Wi-Fi (wireless fidelity o fidelidad sin cables)**: Es una red de ordenadores sin utilización de cables equivalente a la tecnología inalámbrica 802.11 para comunicación a distancia.

5. Marco normativo

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 527 de 1999. Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1273 de 2009. Ley la cual se crea y se protege el bien jurídico de la información y los datos personales.

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

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1581 de 2012. Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales.

Decreto 2609 de 2012. Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica.

Decreto 2693 de 2012. Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Decreto 103 de 2015. Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información.

Resolución 2710 de 2017. Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
CONPES 3995 de 2020. Política nacional de confianza y seguridad digital, política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

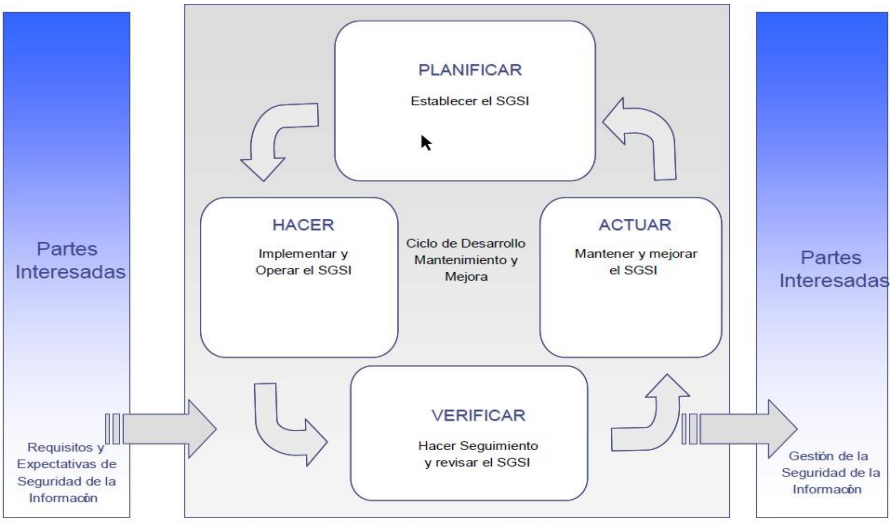
6. Política de Gerencia Tecnologías de Información y Comunicación

Estamos comprometidos en satisfacer las expectativas tanto de los usuarios externos como internos de la tal manera que los diferentes procesos adopten buenas prácticas que permitan garantizar la confiabilidad, oportunidad, confidencialidad, seguridad y acceso a la información.

7. Requisitos generales

El procedimiento para garantizare la seguridad y confidencialidad de la información es presentado a los miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal al hospital, y que no dependa exclusivamente de la oficina o área de TI.

Para llevar a cabo este propósito, se basará la estrategia en el modelo PHVA como se muestra en la siguiente imagen:



Modelo **PHVA aplicado al MSPI**

FASE	DESCRIPCION
PLANIFICAR (establecer el MSPI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
HACER (implementar y operar el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI
VERIFICAR (hacer seguimiento y revisar el MSPI)	Evaluar donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, reportando los resultados a la dirección para su revisión.
ACTUAR (mantener y mejorar el MSPI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

Para planear y gestionar la implementación del MSPI se contará con un grupo interdisciplinario que será liderado por el responsable de seguridad de la información del hospital quien deberá entregar y dar a conocer los perfiles y responsabilidades de cada persona al grupo de trabajo e identificar las personas idóneas para asignar cada rol.

A continuación, se muestra un modelo tomado de la guía de MinTIC correspondiente a los miembros del equipo de seguridad y privacidad de la información.

8. Establecimiento y gestión del MSPI

8.1. Establecimiento del MSPI

El hospital realizará esfuerzos para:

- Definir el alcance y límites del MSPI en términos de las características del servicio que presta el organismo, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
- Definir una política de MSPI en términos de las características del servicio que presta el organismo, su estructura interna, sus activos de información y tecnología; que:
  - Incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad de la información.
  - Tenga en cuenta los requisitos del organismo, los legales o reglamentarios y las obligaciones de seguridad contractuales.
  - Este alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del MSPI.
  - Establezca los criterios contra los cuales se evaluará el riesgo.
  - Haya sido aprobada por la dirección.
- Definir el enfoque organizacional para la valoración del riesgo, teniendo en cuenta:
  - Identificar una metodología de valoración del riesgo que sea adecuada al MSPI y a los requisitos reglamentarios, legales y de seguridad de la información de la organización, identificados.

- Desarrollar criterios para la aceptación de riesgos e identificar los niveles de riesgo aceptables.
- Seleccionar una metodología para la valoración de riesgos que asegure que las valoraciones produzcan resultados comparables y reproducibles.

- Identificar los riesgos
  - Identificar los activos dentro del alcance del MSPI y los propietarios de estos activos de información.
  - Identificar las amenazas a estos activos.
  - Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas.
  - Identificar los impactos que la perdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos.
- Analizar y evaluar los riesgos.
  - Valorar el impacto que podría causar una falla en la seguridad, sobre el organismo, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad
    o disponibilidad de los activos.
  - Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.
  - Estimar los niveles de los riesgos.
  - Determinar la aceptación del riesgo o la necesidad de su tratamiento a partir de los criterios previamente establecidos.
- Identificar y evaluar las opciones para el tratamiento de los riesgos. Las posibles acciones incluyen:
  - Aplicar los controles apropiados
  - Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la

organización para la aceptación de riesgos.

- Evitar riesgos
- Transferir a otras partes los riesgos asociados con el negocio ej. Aseguradoras, proveedores, etc.

- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
- Los controles a seleccionar e implementar deben cumplir los requisitos identificados en el proceso de valoración y tratamiento de riesgos.
- Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
- Obtener autorización de la dirección para implementar y operar el MSPI.
- Elaborar una declaración de aplicabilidad, la declaración de aplicabilidad debe incluir:
  - Los objetivos de control y los controles.
  - Los objetivos de control y los controles que ya se hayan implementado.
  - La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión.
- Elaborar un plan de sensibilización y apropiación del MSPI para toda la entidad.

8.2. Implementación y operación del MSPI

El hospital:

- Formulará un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.
- Implementará el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.
- Implementará los controles seleccionados para cumplir los objetivos de control.
- Definirá cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar cómo se van a usar estas mediciones con el

fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.

- Implementará programas de formación y de toma de conciencia.
- Gestionará la operación del MSPI.
- Gestionará los recursos del MSPI.
- Implementará procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

8.3. Seguimiento y revisión del MSPI

El hospital deberá:

- Ejecutar procedimientos de seguimiento, revisión y otros controles para:
  - Detectar rápidamente errores en los resultados del procesamiento
  - Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
  - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
  - Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
  - Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política y objetivos del MSPI, y la revisión de los controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

- Revisar las valoraciones de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:
  - El hospital
  - La tecnología
  - Los objetivos y procesos del hospital
    - Las amenazas identificadas.
    - La eficacia de los controles implementados.
    - Eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.
- Realizar auditorías internas del MSPI a intervalos planificados.
- Emprender una revisión del MSPI, realizada por la dirección, en forma regular para asegurar que el alcance siga siendo suficiente y que se identifiquen mejoras al proceso de MSPI.
- Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
- Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.

8.4. Mantenimiento y mejora del MSPI

Regularmente el hospital deberá:

- Implementar las mejoras identificadas en el MSPI.
- Emprender las acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
- Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.

- Asegurar que las mejoras logran los objetivos previstos.

9. Requisitos de documentación

La documentación del MSPI incluirá registros de las decisiones de la dirección, asegurar que las acciones sean trazables a las decisiones y políticas de la alta dirección, y que los resultados registrados sean reproducibles.

Esta documentación se realizará conforme a las guías dispuestas por MinTIC para el MSPI.

10. Responsabilidades de la dirección

La dirección del hospital brindará evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del MSPI de la siguiente manera:

- Estableciendo la política del MSPI.
- Asegurando que se establezcan los objetivos y planes del MSPI.
- Estableciendo funciones y responsabilidades de seguridad de la información.
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.
- Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un MSPI.
- Decidiendo los criterios para aceptación de riesgos y los niveles de riesgo aceptables.
- Asegurando que se realizan auditorías internas del MSPI.
- Efectuando las revisiones por la dirección, del MSPI.

10.1. Gestión de recursos

Provisión de recursos

El hospital determinará y suministrará los recursos necesarios para:

- Establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el MSPI.

- Asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos de la institución.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- Llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente a los resultados y en donde se requiera mejorar la eficacia del MSPI.

Formación, toma de conciencia y competencia.

El hospital debe asegurar que todo el personal al que se le asigne responsabilidades definidas en el MSPI sea competente para realizar las tareas exigidas, mediante:

- La determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el MSPI.
- El suministro de formación o realización de otras acciones (ej. Contratación de personal competente) para satisfacer las necesidades.
- La evaluación de la eficacia de las acciones emprendidas.
- El mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones.

11. Auditorías internas del MSPI

El hospital deberá llevar a cabo auditoria internas del MSPI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos del MSPI:

- Cumplen los requisitos de la presente norma y de la legislación o reglamentaciones pertinentes.
- Cumplen los requisitos identificados de seguridad de la información.
- Están implementados y se mantienen eficazmente.
- Tienen un desempeño acorde con lo esperado.

12. Revisión del MSPI por la dirección

La dirección del hospital deberá revisar el MSPI del hospital una vez al año, para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad.

Información para la revisión

Las entradas para la revisión por la dirección incluirán:

- Resultados de las auditorias y revisiones del MSPI.
- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del MSPI.
- Estado de las acciones correctivas y preventivas.
- Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Resultados de las mediciones de eficacia.
- Acciones de seguimiento resultante de revisiones anteriores por la

dirección.

- Cualquier cambio que pueda afectar el MSPI.
- Recomendaciones para mejoras.

Resultados de la revisión

Los resultados de la revisión por la dirección incluirán cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que pueden tener impacto en el MSPI, incluidos cambios a:
- Los requisitos de la organización
- Los requisitos de seguridad
- Los procesos del organismo que afectan los requisitos del negocio existentes.
- Los requisitos reglamentarios o legales.
- Las obligaciones contractuales.
- Los niveles de riesgo y/o niveles de aceptación de riesgos.
- Los recursos necesarios.
- La mejora a la manera en que se mide la eficacia de los controles.

13. Mejora del MSPI

Mejora continua

El hospital deberá mejorar continuamente la eficacia del MSPI mediante:

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- Los resultados de la auditoría.
- El análisis de los eventos a los que se les ha hecho seguimiento.
- Las acciones correctivas y preventivas y la revisión por la dirección.

Acción correctiva

El hospital deberá emprender acciones para eliminar la causa de no conformidades asociadas con los requisitos del MSPI, con el fin de prevenir que ocurran nuevamente.

El procedimiento documentado para la acción correctiva debe definir requisitos para:

- Identificar las no conformidades
- Determinar las causas de las no conformidades.
- Evaluar la necesidad de acciones que aseguren que las no conformidades no vuelven a ocurrir.
- Determinar e implementar la acción correctiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción tomada.

Acción preventiva

El hospital determinará acciones para eliminar la causa de no conformidades potenciales con los requisitos del MSPI y evitar que ocurran. Las acciones preventivas tomadas deben ser apropiadas al impacto de los problemas potenciales.

El procedimiento documentado para la acción preventiva debe definir requisitos para:

- Identificar no conformidades potenciales y sus causas.
- Evaluar la necesidad de acciones para impedir que las no conformidades ocurran.
- Determinar e implementar la acción preventiva necesaria.
- Registrar los resultados de la acción tomada.
- Revisar la acción preventiva tomad

14. DESARROLLO

14.1. Política de seguridad de la información

El Hospital San José de San Bernardo del Viento, considera la información como un activo fundamental para la gestión administrativa y para la prestación de servicios de salud; por lo cual asigna un compromiso expreso de la protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad de la información.

Consciente de las necesidades actuales, el Hospital San José de San Bernardo del Viento implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se exponen la información, ayudar a la reducción de costos operativos y financieros, establecer una cultura de seguridad y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del Hospital San José de San Bernardo del Viento, deberán adoptar los lineamientos contenidos en el presente documento y en los

demás relacionados, con el fin de mantener la confidencialidad, la integridad y disponibilidad de la información.

La política global de seguridad de la información del Hospital San José de San Bernardo del Viento se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información del hospital. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

Esta política deberá ser revisada de manera periódica (por lo menos una vez al año, cuando se adicione un nuevo servicio TIC o se identifiquen cambios en el contexto interno o externo en la institución). Los responsables de realizar la revisión de la presente política será el comité de seguridad de la información o el responsable definido para tal labor.

14.2. Política de Clasificación de la Información

Objetivo

Gestionar las acciones necesarias para que la información reciba el nivel de protección apropiada de acuerdo con el tipo de clasificación establecido por el Hospital.

Directrices

- Se deberán definir cuáles son los niveles de clasificación de la información (Pública, uso interno, confidencial o restringida) para la información que se maneja en la institución.

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales escritos en cualquier medio, ya sea magnético, papel u otro que genere el Hospital (Ej: historias clínicas, exámenes de laboratorio, patologías, imágenes diagnósticas, entre otras).

- El propietario de la información o a quien delegue, será el responsable de clasificar la información que tiene bajo su responsabilidad teniendo en cuenta los riesgos, amenazas e impactos en caso de materialización de éstos.

14.3. Política de Seguridad para los usuarios de activos de información

Objetivo

Verificar que los funcionarios, contratistas y demás colaboradores del Hospital San José de San Bernardo del Viento, entiendan sus responsabilidades y funciones, con el fin de reducir el riesgo de hurto, fraude o usoinadecuado de la información y de las instalaciones.

Directrices:

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores del Hospital San José de San Bernardo del Viento, entiendan sus responsabilidades en relación con las políticas de seguridad de la información y cumplan las mismas actuando de manera consistente frente a estas, con el fin de reducir el riesgo de hurto, fraude o uso inadecuado de la información o de los equipos empleados para el tratamiento de la información.

- Los recursos tecnológicos y de software asignados a los funcionarios del Hospital son responsabilidad de cada uno.

- Los usuarios son los responsables de la información que administren en sus equipos personales; deberán abstenerse de almacenar en ellos información no institucional.

- Los usuarios solo tendrán acceso a los datos y recursos autorizados por el Hospital y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

- Es responsabilidad de cada usuario proteger la información que esté contenida en documentos, formatos, listados, etc.; los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entradas de estos procesos.

- Los dispositivos electrónicos de propiedad del hospital (computadoras, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

- Cualquier evento o posible incidente que afecte la seguridad de la información, deberá ser reportado inmediatamente a la mesa de ayuda (Técnico Operativo sistema de información) del Área TIC del Hospital.

- Los jefes de las diferentes áreas del Hospital en conjunto con el Comité de Seguridad de la información propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial.

14.4. Políticas específicas para funcionarios y contratistas del Área de TIC.Objetivos

Garantizar que funcionarios y contratistas del área TIC aseguren una adecuada protección de la información de la cual son responsables de su administración.

Directrices

- El personal del área TIC no debe dar a conocer sus claves de usuario a personal ajeno a su área.
- Los usuarios y claves de los administradores de sistemas y del personal del área TIC son de uso personal e intransferible.
- El personal del área TIC debe emplear obligatoriamente claves o contraseñas con un alto nivel de complejidad.
- Los medios de instalación y seriales del software adquirido por el Hospital San José de San Bernardo del Viento deben mantenerse custodiados para evitar el acceso a personal no autorizado.
- Para el cambio o retiro de equipos de cómputo por daño u obsolescencia, se deben seguir políticas de saneamiento; es decir, llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. (Ej. formateo o borrado seguro de información).
- Los funcionarios encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.
- El personal del área TIC no otorgará privilegios especiales a usuarios sobre las estaciones de trabajo sin la autorización correspondiente del Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- El personal del área TIC está obligado a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- El personal del área TIC no utilizará la información del hospital para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar por quien designe el Jefe Oficina Asesora Sistemas de Información Hospitalaria, de tal forma que asegure su protección y disposición en un futuro.
- El software licenciado y registrado como software adquirido, será únicamente instalado en equipos y servidores de propiedad del hospital, excepto aquellas empresas que mantengan un convenio contractual con el Hospital San José de San Bernardo del Viento para la ejecución de las actividades requiera el acceso al software.
- El Hospital San José de San Bernardo del Viento, instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados y en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización por parte del Jefe Oficina Asesora Sistemas de Información Hospitalaria puede implicar amenazas legales y de seguridad de la información para la entidad, por lo cual esta práctica no está autorizada. La persona o empresa encargada de redes e infraestructura, deberá llevará el control de las cantidades de licencias disponibles.
- El acceso al software y la documentación de éste solamente podrá ser consultada y usada en el ejercicio de las actividades contractuales.
- Cumplir siempre con el registro en la bitácora de acceso al DataCenter de las personas que ingresen y que hayan sido autorizadas previamente por el Jefe Oficina Asesora Sistemas de Información Hospitalaria o por quien éste delegue.
- Por defecto deben ser bloqueados todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de Seguridad de la Información o el Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los servidores deben ser configurados con el mínimo de servicios posibles y asociados para el desarrollo de las funciones designadas.

14.5. Políticas específicas para Web master

Objetivo

Proteger la integridad de la página Web institucional, el software y la información contenida en ellas.

Directrices

- Los responsables de áreas que requieran publicar información institucional en la página Web deben preparar y depurar la información de su área o dependencia y reportar a la Oficina de Mercadeo y Comunicaciones para su revisión quien será responsable de verificar ortografía, redacción e imagen corporativa de la información a publicar. Posteriormente la Oficina de Mercadeo y Comunicaciones generará una solicitud a la mesa de ayuda del área TIC para efectuar los cambios correspondientes.
- El responsable de redes e infraestructura realizará las copias de seguridad de la página web y mantendrá el histórico respectivo.
- Se deberá tener especial cuidado en la información que es publicada en la web y debe ser la autorizada por las áreas y con nivel de clasificación pública.

14.6. Política de Tercerización u Outsourcing

Objetivo

Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por esta.

Directrices

- Se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas. El análisis de los riesgos será la base para el establecimiento de los controles y deben ser presentado al Comité de Seguridad de la Información y área TIC antes de firmar el contrato de Outsourcing.
- Con el fin de proteger la información por ambas partes, se debe formalizar un acuerdo de confidencialidad en donde se defina claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir. Si la información intercambiada lo amerita teniendo en cuenta la clasificación de la información de acuerdo con los niveles de seguridad, se debe preparar y legalizar un acuerdo de confidencialidad entre la entidad y el Outsourcing de acuerdo al objetivo y al alcance del contrato; el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad de la información y con los objetivos de la entidad.

14.7. Política de disposición de información, medios y equipos

Objetivo

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de

información o contra desastres y propender por su recuperación oportuna.

Directrices

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
-

14.8. Política de respaldo y restauración de información

Objetivo

Asegurar que la información crítica para la entidad se encuentre disponible en situaciones de contingencia y poder asegurar la continuidad del negocio.

Directrices

- La información de cada sistema debe ser respalda regularmente en medios de almacenamiento como discos externos, servidores de almacenamiento o el medio que disponga el hospital.
- Los administradores de los servidores son los responsables de la realización y custodia de las copias de seguridad según el procedimiento establecido.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada con los controles ambientales aplicables y con control de acceso físico.
- Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal, entre otros.
- El plan de Contingencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; para lo cual el Hospital San José de San Bernardo del Viento dispone de un espacio para el almacenamiento de la información en los servidores.

- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera del edificio en donde se encuentre el Data Center del Hospital.
- Las restauraciones de copias de respaldo en ambientes de producción deben estar debidamente aprobada por el propietario de la información.
- Periódicamente desde el área TIC se verificará la correcta ejecución de los procesos de backup ejecutados.
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. Este proceso deberá ser controlado y aprobado por las áreas de Revisoría Fiscal y/o Control Interno.
- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización de los recursos de almacenamiento que entrega el Hospital a los usuarios.
-

14.9. Política de gestión de activos de información

Objetivo

Establecer la forma en que se logra mantener la protección adecuada de los activos de información.

Directrices

- El Hospital San José de San Bernardo del Viento mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el área TIC.
- El Hospital San José de San Bernardo del Viento, es el propietario (En cabeza de sus líderes de áreas) de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de la información y comunicaciones (TIC).

14.10. Política de uso de los activos

Objetivo

Proteger de forma adecuada los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

Directrices

- Los activos de información pertenecen al Hospital y el uso de estos deben emplearse exclusivamente con propósitos laborales. Los activos de información de Hardware proveídos por el contratista o de terceras partes, serán administrados y estarán bajo la supervisión del personal TIC del Hospital y deberán cumplir con políticas de seguridad de la información, tal como control de acceso a redes y aplicativos, entre otros.
- Los usuarios deberán utilizar únicamente software, programas y equipos autorizados por el área de TIC del Hospital San José de San Bernardo del Viento.
- El Hospital proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad del Hospital, los funcionarios o usuarios solo podrán realizar backup de información pública. Para copiar cualquier tipo de información clasificada como confidencial o restringida debe pedir autorización a su jefe inmediato, de acuerdo con las normas sobre clasificación de la información.
- Periódicamente, el personal de redes e infraestructura efectuará una auditoria a los computadores para revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como violación a las Políticas de Seguridad de la Información del Hospital.
- El Hospital no se hará responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios contratistas.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos que requieran un nivel de aprobación, deben ser solicitados, analizados y aprobados por el Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- Estarán bajo custodia de la Oficina Asesora Sistemas de Información

Hospitalaria, los medios magnéticos/electrónicos (CD, DVD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso; adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet.

- Los Password de administración de los equipos informáticos, sistemas de información o aplicativos estarán bajo la responsabilidad del funcionario que tenga la administración de los servicios TIC.
- En caso de ser necesario y previa autorización del Comité de Seguridad de la Información o de la oficina asesora de sistemas de información hospitalaria, los funcionarios del Hospital podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban a través de internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
- Los recursos informáticos no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenidos personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos.
- Los usuarios no podrán efectuar ninguna de las siguientes actividades:

  - Instalar software en cualquier equipo instalado en áreas físicas del Hospital.
  - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo del Hospital.
  - Modificar, revisar, transformar o adaptar cualquier software propiedad delHospital.
  - Descompilar o realizar ingeniería inversa en cualquier software de propiedad del Hospital.
  - Copiar o distribuir cualquier software de propiedad del Hospital.

- El usuario deberá informar al jefe inmediato de cualquier violación de las políticas de seguridad o uso indebido del cual tenga conocimiento.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los servicios de TIC, utilizando una cuenta de usuario o clave de otro usuario.
- Cada usuario es responsable de asegurar que el uso de redes externas, tal como internet, no comprometa la seguridad de los recursos informáticos del Hospital. El área de redes e Infraestructura es responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad.
- Todos los archivos provenientes de equipos externos del Hospital deben ser revisados para detención de virus antes de ser utilizados en la red del Hospital.
- La información del Hospital debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se puede garantizar que la información sea segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

14.11. Política de uso de estaciones cliente

Objetivo

Asegurar que los usuarios usen correctamente las estaciones de trabajo como parte integral de los activos de información institucional.

Directrices

- La instalación de software en los computadores suministrados por el Hospital es una función exclusiva del área TIC. Se mantendrá una lista actualizada delsoftware autorizado para instalar en los computadores.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos

que no sean de carácter institucional.

- Los programas instalados en los equipos son de propiedad del Hospital; la copia no autorizada de programas o de su documentación, implica una violación a la política general del Hospital. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las sanciones disciplinarias establecidas por el Hospital o las sanciones que especifique la ley. (Dichas copias no autorizadas deberán ser eliminadas).
- El Hospital se reserva el derecho de proteger su buen nombre y sus inversiones de hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad intelectual. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorias anunciadas y no anunciadas.
- En el disco o unidad C: de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
- Los usuarios podrán trabajar sus documentos institucionales en borrador en las estaciones cliente asignado y deberá ubicar copias y documentos finales en las carpetas virtuales centralizadas que se establezca para cumplir con las tablas de retención documental del Hospital.
- Los equipos que ingresan temporalmente al hospital y que sean de propiedad de terceros, deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización; el Hospital no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
- El área TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean del Hospital dentro de sus instalaciones y horario laboral.

14.12. Política de uso de Internet

Objetivo

Establecer lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando perdida, modificaciones no

autorizadas o uso inadecuado de la información en las aplicaciones web.

Directrices

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborares.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del Hospital o que representen peligro para la entidad como: pornografía, terrorismo, segregación racial, música, redes sociales u otras fuentes.
- El acceso a sitios WEB con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad de la Información ó Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- La descarga de archivos de Internet debe ser con propósitos labores y de forma razonable para no afectar el servicio de Internet.
- Los documentos o software que se descarguen de Internet deben tener las debidas licencias o permisos de uso, respetando siempre la propiedad intelectual del mismo.

14.13. Política de uso de mensajería instantánea y redes sociales

Objetivos

Definir las pautas generales para asegurar una adecuada protección de la información del Hospital San José de San Bernardo del Viento, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios.

Directrices

- El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones con el fin de facilitar canales de comunicación con la

ciudadanía.

- No se permite el envío de mensajes con contenido que atente la integridad de las personas o instituciones o cualquier contenido que presente riesgo de código malicioso.
- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del hospital, que sea creado a nombre personal en redes sociales (twitter, Facebook, YouTube, blog, etc.) se considera fuera del alcance del SGSI y por lo tanto su confiablidad, integridady disponibilidad, así como los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya publicado.

14.14. Política de uso de discos de red o carpetas virtuales

Objetivo

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Directrices

- Para que los usuarios tengan acceso a la información en los discos de red, el jefe inmediato deberá enviar una solicitud a la mesa de ayuda del área TIC del Hospital, autorizando el acceso y permisos correspondientes al rol y funciones a desempeñar. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- El hospital suministrará una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de daños en el equipo asignado.
- La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
- Está prohibido almacenar en las estaciones de trabajo (computadores de escritorio o portátiles, tablets, celulares inteligentes, etc.), o en los discos de red de propiedad de la entidad, archivos con contenido que atente contra la

moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso.

- Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización del jefe inmediato.
- Se prohíbe el uso de información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

14.15. Política de uso de impresoras y del servicio de Impresión

Objetivo

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión en las diferentes áreas del hospital.

Directrices

- Los documentos que se impriman en las impresoras del Hospital deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras (y/o cualquier equipo de cómputo). En caso de presentarse alguna falla, esta se debe reportar al área TIC por medio de su mesa de ayuda.
- Agregar o alinear la presente política con la de política de cero papeles, si existe.

14.16. Política de uso de puntos de red de datos

Objetivo

Asegurar la operación correcta y segura de los puntos de red instalados en la entidad.

Directrices

- Los usuarios deberán emplear los puntos de red para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no sean de propiedad del Hospital, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el área de redes e infraestructura. Se deberá identificar el equipo por medio de la MAC.

- La instalación, activación y gestión de los puntos de red es responsabilidad del área de infraestructura y redes.

14.17. Política de seguridad del centro de datos (DataCenter)

Objetivo

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Directrices

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visite el centro de datos.
- El área de redes e infraestructura debe garantizar que el control de acceso al centro de datos del Hospital cuente con dispositivos de control necesarios (electrónicos de autenticación o sistemas de control biométrico) para asegurar accesos autorizados.
- El área de redes e infraestructura deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del área de redes e infraestructura. En caso contrario, deberá ser supervisado por personal de esta área si el aseo lo llegase a realizar personal ajeno a ésta.
- En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

- El centro de datos debe estar provisto de:

  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuarcon la refrigeración
  - Unidades de potencia ininterrumpida UPS, que proporcione respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
  - Alarma de detención de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán se probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar prevista en los procedimientos de mantenimiento y control.
  - Extintores de incendios o un sistema contra incendios debidamente probado y con la capacidad de atener el fuego generado por equipo eléctrico, papel o químicos especiales.

- El cableado de la red debe ser protegido de interferencias a través del uso de canaletas.

- Los cables de potencia deben estar separados de los de comunicaciones (datos), siguiendo las normas técnicas.

- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizadas por el comité de seguridad de la información o Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista de redes e infraestructura.

- Las puertas de acceso al centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el

funcionario de la actividad se ubicará dentro del centro de datos.

- Cuando se requiera realizar actividad sobre algún armario (rack), este deberá siempre estar y/o quedar ordenado, cerrado y con llave cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que se requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

14.18. Políticas de seguridad de los equipos de cómputo

Objetivo

Asegurar la protección de la información procesada en los equipos de cómputo.

Directrices

- Dar cumplimiento a las siguientes normas de seguridad:
  - Encender y apagar correctamente el equipo de cómputo.
  - No colocar encima de los equipos de cómputo ningún objeto que pueda caer y dañarlos.
  - Toda CPU que se encuentre en servicio no debe estar en el piso sin ningún tipo de soporte.
  - No consumir alimentos ni bebidas cerca al equipo de cómputo.
  - Limpiar regularmente el equipo de cómputo asignado.
- Conectar a la red de energía regulada únicamente equipos de cómputo y tecnológicos de propiedad del hospital. Equipos ajenos al hospital y autorizados para su uso dentro de la institución se deben conectar a la red noregulada.
- Seguridad del cableado: los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

- Deben existir planos que describan las conexiones del cableado
- El acceso a los centros de cableado, deben estar protegidos.

➢ Mantenimiento de los equipos de cómputo:

- El Hospital debe mantener contratos de soporte y mantenimiento de los equipos de cómputo.
- Las actividades de mantenimiento tanto preventivo como correctivo debe registrarse para cada equipo de cómputo.
- Las actividades de mantenimiento de los servidores, comunicación,energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones del Hospital para reparaciones o mantenimientos deben estar debidamente autorizados y se deben garantizar que en dichos elementos no se encuentre información confidencial.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información confidencial contenida en ella. Realizar copia de información.

➢ El retiro e ingreso de todo activo de información de propiedad de los usuarios del Hospital utilizados para fines personales, se realizará mediante los procedimientos establecidos por la entidad. El Hospital no se hace responsable de los daños ocasionados a los bienes del usuario al haberse conectado a la red eléctrica del Hospital. El retiro e ingreso de todo activo de información de los visitantes (consultores, pasantes, visitantes, pacientes y sus familias), será registrado y controlado en las porterías. El personal de vigilancia registrará las características de la identificación del activo de información en el formato destinado para tal fin.

➢ El traslado entre dependencias del Hospital de todo activo de información

(equipos de cómputo), está a cargo del área Administrativa (Activos Fijos) parael control de Inventarios.

14.19. Política de escritorio, pantalla limpia y de equipos desatendidos

Objetivo

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de información durante y fuera del horario de trabajo normal de los usuarios.

Directrices

- El personal del Hospital o contratistas debe conservar su escritorio libre de información confidencial, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal del Hospital debe bloquear la pantalla de su computador con el protector de pantalla en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba ausentarse del puesto de trabajo.
- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- Almacenar bajo llave y cuando corresponda, los documentos en físico y/o medios informáticos en gabinetes u otro tipo de mobiliario seguro, cuando no estén siendo utilizados, especialmente fuera del horario de trabajo.
- No se deben utilizar fotocopiadoras, escáners, equipos de fax, cámaras digitales y en general equipos tecnológicos que no se encuentren configurados a la red del hospital.

14.20. Política de uso de correo electrónico

Objetivo

Establecer una serie de directrices para el uso responsable del correo electrónico

institucional.

Directrices

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de correo institucional; toda información o contenido que sea transmitido por las cuentas de correo de este sitio, son responsabilidad únicamente del dueño de la cuenta.
- La cuenta de correo es personal e intransferible, siendo su responsabilidad salvaguardar la clave de acceso, cambiándola en forma periódica, ni prestar la clave en ninguna circunstancia, pues su uso recae bajo su responsabilidad. Así mismo, el usuario se compromete a notificar personalmente al administrador de correo electrónico de manera inmediata la pérdida de su contraseña o acceso no autorizado por parte de terceros a su cuenta.
- Se requiere que la primera vez que el usuario ingrese a su cuenta de correo cambie su clave. Por motivos de seguridad, es recomendable cambiar la clave, como mínimo, cada tres meses. El correo electrónico es una herramienta de trabajo para uso exclusivamente de la Institución, no es una herramienta de difusión masiva e indiscriminada de información.
- Los miembros del Hospital deben ser cuidadosos cuando decidan abrir los archivos adjuntos en mensajes de remitentes desconocidos o sospechosos, para evitar descarga de algún virus informático o programa sospechoso.
- Será responsabilidad del administrador de las https://www.esehospitalsanjose.com:2083/ respaldo (Backups) de los mensajes de las carpetas de correo electrónico.
- Es responsabilidad del propietario de la cuenta mantener el buzón por debajo de su capacidad para evitar que se sature (eliminando regularmente mensajes antiguos, etc.). Si el buzón llega a saturarse no podrán recibirse mensajes nuevos mientras permanezca saturado. No se deben distribuir listas de direcciones de Correos de la Institución sin expresa autorización del Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- El usuario es responsable de difundir su cuenta de correo, por lo tanto, la publicación de esta en sitios web, listas de correo, inscripciones a sitios de interés, provocara probablemente, el ataque continuo de correo basura (Spam) con publicidad en internet, por lo tanto, no se puede divulgar la cuenta de

correo en estos medios.

Condiciones de uso

- Podrán tener correo electrónico Institucional todas aquellas personas de las diferentes áreas administrativas y asistenciales que se considere tenga necesidad de este servicio y tengan un vínculo laboral con el Hospital San José de San Bernardo del Viento, las cuales serán asignadas con previa autorización del Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- Los usuarios podrán tener correo institucional siempre y cuando cumplan con los términos de condiciones y las normas internas de la Institución; como también deberá tener claro que es para uso exclusivo del Hospital mas no para uso de tipo personal o comercial.
- Los usuarios serán completamente responsables del uso y manejo de las actividades realizadas con la cuenta de correo asociada a nuestra Institución, así como de la información enviada a través de este servicio.
- Se deberá usar lenguaje apropiado para los mensajes y manejar conductas de cortesía al momento del uso.
- Están completamente prohibidas las siguientes actividades:

  - Utilizar el correo electrónico para cualquier propósito personal de índole comercial o financiero.
  - No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.
  - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados.
  - Distribuir mensajes ofensivos, con palabras inapropiadas o que vulneren la integridad o buen nombre de la institución o de las personas.
  - Leer correos ajenos, generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- Violar los derechos de cualquier persona o Institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
- Usar el correo con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil o maliciosa.
- Enviar por correo electrónico material que contenga virus de software, o cualquier otro código de computadora, archivos o programas diseñados para, destruir o limitar el funcionamiento de algún software o disco duro de computadora o equipo de telecomunicaciones.
- Usar el Servicio con fines fraudulentos o inapropiados.
- Causar daño a menores de edad.

- El usuario se responsabiliza de mantener la confidencialidad de su contraseña y cuenta y de todas las actividades que se efectúen bajo éstas, con el fin de que en toda información o contenido se mantenga su seguridad.
- Cada usuario se compromete a informar inmediatamente a la administración del correo institucional de cualquier acceso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad y se compromete asegurarse de que su cuenta sea cerrada al final de cada sesión.
- El usuario se obliga a cumplir las normas sobre protección de la información y de los datos que consagre la Constitución y la ley.

Caducidad de las cuentas de correo

El uso inapropiado, el abuso en el servicio de correo electrónico o no uso del mismo pueden ocasionar la desactivación temporal o permanente de las cuentas. La desactivación de una cuenta de correo electrónico supone la pérdida automática de la capacidad de enviar y recibir mensajes. Si existe evidencia de que el usuario está haciendo mal uso del servicio, no está respetando los lineamientos establecidos en esta política o está incurriendo en actividades ilícitas mediante el servicio de correo, el Hospital se reserva el derecho de tomar acciones disciplinarias, incluyendo las medidas pertinentes, de acuerdo con la normativa de la institución y a la legislación vigente. Como norma general, las cuentas de correo electrónico se mantendrán activas mientras la relación laboral de la persona con el

Hospital esté vigente.

Buzón de correo

Todas las cuentas de correo tienen asignado un espacio de 25 Gb para almacenar los mensajes recibidos (buzón). Si se sobrepasa la capacidad máxima el usuario no podrá recibir ni enviar correos.

El usuario deberá asegurarse de que su cuenta sea cerrada al final de cada sesión con el fin de evitar perdida de la información o suplantación.

14.21. Políticas de asignación de nombres de usuario para las cuentas decorreo institucional

El nombre de usuario asignado será el primer nombre de la oficina o de la dependencia. Por ejemplo, para área de sistemas sería sistemas@esehospitalsanise.com.

Recomendaciones para la asignación de contraseña

- Para la asignación de la contraseña, los usuarios deben utilizar al menos 8 caracteres para crear la contraseña. Se recomienda o se exigirá utilizar en una misma contraseña dígitos, letras y caracteres especiales.
- Es recomendable que las letras se alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
- Elegir una contraseña que pueda recordarse fácilmente y que pueda escribirse rápidamente.

Acciones que deben evitarse en la gestión de contraseñas seguras

- Evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas.

- No utilizar información personal en la contraseña: nombre del usuario o de familiares, ni apellidos, ni fecha de nacimiento, y por supuesto, en ninguna ocasión utilizar datos como el número de cedula o número de teléfono.
- Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”), ni repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
- Evitar utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
- No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de esta. Tampoco se deben guardar en documentos de texto dentro del propio computador o dispositivos móviles.
- No enviar nunca la contraseña por correo electrónico o en mensajes de texto; tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
- Tener especial cuidado al ingresar las contraseñas en computadores que se desconozca su nivel de seguridad y puedan estar monitorizados, o en computadores de uso público (Ej.: bibliotecas, cibercafés, telecentros, etc.).

14.22. Política de control de acceso a sistemas y aplicativos

Objetivo

Definir las pautas generales para asegurar un acceso controlado lógico, a la información de la plataforma informática del Hospital, así como el uso de medios de computación móvil.

Directrices:

- El Hospital proporcionará a los funcionarios y contratistas todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las

cuales fueron contratados; por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, agendas electrónicas, celulares inteligentes, access point, entre otros que no estén autorizados por la Oficina Asesora Sistemas de Información Hospitalaria.

- Todo equipo de cómputo ajeno al hospital debe cumplir con los siguientes criterios para la conexión a la red interna de la institución:

  - Sistema operativo licenciado que permita unirse al dominio del hospital.
  - Sistema operativo en su versión Windows 7 o 10 Professional.
  - Sistema operativo actualizado, con todos los parches de seguridad.
  - Antivirus actualizado.
  - Escaneo total con el antivirus con un día de anticipación al ingreso del dominio del hospital.
  - Licencias de todo el software que esté instalado en el equipo.
  - Todo equipo que no cumpla con alguno de estos criterios, por seguridad de la información no podrá ser instalado a la red, recursos y sistemas internos del hospital.

- El hospital suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se le dé a las claves asignadas.

- El área de TIC será el responsable de generar el usuario y la contraseña de primer acceso para el ingreso a los aplicativos institucionales del personal autorizado por el área de talento humano.

- El área TIC será el responsable de mantener los registros de cada uno de los usuarios a los cuales se les han concedido permisos de acceso o eliminación de estos.

- El propietario de los activos de información o a quien delegue debe autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

- El propietario de los activos de información o a quien delegue debe monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

- Cada usuario es responsable de los mecanismos de control de acceso que le han sido proporcionados; esto es usuario y contraseña de primer acceso, por lo que se deberá mantener de forma confidencial.

- Cada usuario que tenga acceso a sistemas y aplicativos debe contar con un único usuario para el aplicativo asignado.

- Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tiene prohibido utilizar el ID de otros usuarios.

- No se podrá realizar ninguna actividad de tipo remoto sobre los equipos, servidores principales sin la debida aprobación del Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- La conexión remota a la red área local del Hospital debe ser hecha a través de una conexión IP4 Dinámico segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

- Solo usuarios del área TIC, están autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones.

- Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación se hará con números, letras mayúsculas y minúsculas, y caracteres especiales.

- Los usuarios con acceso a los diferentes sistemas de información deberán cambiar su contraseña de acceso con una frecuencia mínima de 3 meses.

- Los usuarios deben cumplir las siguientes normas para la creación de contraseñas:

    - Mantener los datos de acceso en secreto.
    - Contraseñas fáciles de recordar y difíciles de adivinar.
    - Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente.
    - Notificar cualquier incidente de seguridad relacionado con sus

contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

14.23. Política para dispositivos móviles

Objetivo

Proveer las condiciones de seguridad para el manejo de los dispositivos móviles (memorias USB, Discos duros externos, teléfonos inteligentes y tabletas, entre otros) institucionales y personales autorizados que hagan uso de activos de información en los servicios del hospital.

Directrices:

- El área TIC debe implementar las medidas de protección física y lógica sobre los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el hospital.
- El uso de dispositivos de almacenamiento externo (D.D externos, DVD, CD, memorias USB, agendas electrónicas, celulares, entre otros) pueden generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar algunos de los dispositivos de almacenamiento externo enunciados anteriormente, se debe obtener aprobación formal e individual del Jefe Oficina Asesora Sistemas de Información Hospitalaria.
- El área TIC debe establecer las configuraciones de seguridad de acceso para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el hospital, previamente autorizados.
- El área TIC deberá configurar el control de bloqueo automático de sesión de usuarios por inactividad.
- El área TIC debe activar la opción de cifrado de discos en aquellos dispositivos móviles institucionales que almacenan información sensible y/o crítica.
- El área TIC debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- El área TIC debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales del hospital;

dichas copias deben acogerse a la política de respaldo y restauración de la Información.

- El área TIC debe instalar un software de antivirus tanto en los dispositivos móviles institucionales como en los personales que hagan uso de los servicios provistos por el hospital.
- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de software no autorizado y/o desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados mientras se encuentren en lugares diferentes al hospital.
- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de bibliotecas o cafés internet, entre otros.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

14.24. Política de transferencia de información

Objetivo

Presentar los lineamientos orientados para la protección de la información tanto del Hospital como de los pacientes en aquellas situaciones en las cuales sea necesario o se requiera realizar su transferencia a terceros, asegurando que la información sensible y crítica del Hospital y de los pacientes sea transferida a su destino a través de los medios disponibles y autorizados, de manera adecuada para prevenir su posible interceptación, acceso y/o uso no autorizado.

Directrices generales:

- El propietario de los activos de información o a quien él delegue debe velar porque la información del hospital o de sus usuarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información.

- El propietario de los activos de información o a quien él delegue debe asegurar que los datos requeridos de los usuarios sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- El propietario de los activos de información o a quien él delegue, debe verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- El propietario de los activos de información o a quien él delegue debe autorizar los requerimientos de solicitud/envío de información del hospital por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- El propietario de los activos de información o a quien él delegue debe asegurar que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a la presente política.

- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando carpetas, archivos compartidos, discos virtuales, medios removibles, entre otros que no estén controlados ni auditados por el área TIC.

- El área de correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el hospital y que estos permitan ejecutar rastreo de las entregas.

- El área TIC debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

- No está permitido el intercambio de información sensible del hospital ni de sus usuarios o pacientes por vía telefónica o fax.

Contacto vía telefónica

- Realizar la transferencia de información únicamente a través de líneas telefónicas internas.
- Al realizar contacto telefónico, marcar el número registrado en la base de dato por parte del paciente o familiar.
- Siempre se deberá preguntar por el nombre completo del paciente para asegurar que se está comunicado con la persona indicada y a través del uso de validación de información.
- No se deberán dejar mensajes con información sensible con personas diferentes al paciente, en equipos de respuesta automática o mensajes de voz, siempre y cuando el mensaje sea demasiado urgente y sin datos sensibles.
- Asegurese de dejar el mensaje en la máquina de respuesta correcta y de uso permanente por el paciente.

Contacto vía correo electrónico

- Únicamente información NO sensible podrá ser enviada a cuentas de correo electrónico de pacientes.
- Los usuarios (asistenciales – administrativos) bajo ninguna circunstancia deben utilizar el correo electrónico personal como medio para enviar o recibir información propia del hospital, de sus usuarios o pacientes (salvo aquellos autorizados).
- Información sensible solamente podrá ser entregada o compartida a los pacientes a través de medio conversación telefónica o de manera personal y no a través de correo electrónico.

Comunicación electrónica de información a terceros

- Bajo ninguna circunstancia información o datos personales de usuarios o pacientes podrán ser enviados sin los controles de encriptación necesarios.
- El intercambio de información sensible a través de redes públicas o links con entidades del sector o terceros autorizados, deberá ser protegida mediante el uso de mecanismos criptográficos que garanticen su confidencialidad y autenticidad.

Transporte de información digital en medio físico

- La información sensible de pacientes o del Hospital que requiera ser entregada físicamente, deberá ser protegida mediante el uso de mecanismos criptográficos que garanticen su confidencialidad y autenticidad en cualquier dispositivo de almacenamiento que se establezca para su transporte (discos duros, USB, entre otros, que estén autorizados por la Oficina Asesora Sistemas de Información Hospitalaria).

14.25. Política para revisión de los derechos de acceso a usuarios

Objetivo:

Verificar y validar que el acceso lógico asignado a los sistemas de información y aplicaciones, se encuentran debidamente aprobados y acceden a la información y/o recursos apropiados de acuerdo con sus roles y responsabilidades del funcionario dentro de la institución.

Directrices:

- Para administrar los accesos a los Sistemas de información se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización presenten necesidades de acceso.

- Los líderes de procesos o área deben revisar en forma periódica los perfiles de usuarios del personal a su cargo y solicitar al área TIC la actualización de éstos cada vez que ocurra un cambio en la definición de funciones.

- Se mantendrá registro de los intentos de acceso fallidos a sistemas considerados críticos, el cual será revisado periódicamente por el responsable de los sistemas de información.

- Constituirá falta grave el intento de obtener accesos no autorizados a los aplicativos institucionales.

- De forma periódica se suspenderán las cuentas de usuarios que no fueron accedidas durante un lapso determinado de tiempo; para ello, se deberá asegurar la copia de respaldo con información de registro de actividades de usuarios en los diferentes sistemas de información o aplicaciones.

14.26. Política para disposición final de medios cuando no se requieranObjetivo:

Establecer las directrices y actividades necesarias para el manejo, almacenamiento y disposición final de los medios de almacenamiento de información usados por la institución.

Directrices:

- La disposición final de documentos se hará de acuerdo con el programa de gestión documental, procesos y procedimientos internos para el archivo, conservación y disposición final de documentos.
- La disposición final de los documentos se realizará en las mejores condiciones, procurando siempre fomentar la transparencia, el acceso y el cumplimiento de los lineamientos que al respecto puedan ser aplicados.
- Todo documento en físico que se requieran dar de baja se debe coordinar con la Oficina de Seguridad y Salud en el Trabajo para la destrucción y disposición final de los mismos, dando cumplimiento a las siguientes actividades:

    - Separar el papel que se encuentre en buen estado para disponer de forma final.
    - Realizar destrucción manual del papel que va a ser dispuesto de forma final.
    - Comercializar (venta de material reciclable) con empresas que tengan licencia ambiental para disposición y tratamiento de residuos sólidos.

- El hospital garantizará la consulta, utilización y conservación de la documentación de la entidad para satisfacer necesidades de información de los usuarios.
- Los equipos de cómputo que ya no se requieran por su obsolescencia o daño, serán revisados por personal del área TIC, quienes emitirán el reporte técnico respectivo para la disposición final por parte del hospital.
- Toda disposición final de medios electrónicos que ya no se usen (equipos de cómputo y/o periféricos) se debe ejecutar de acuerdo con lo establecido en el procedimiento interno del hospital para baja de equipos y a la normatividad vigente emitida por el gobierno colombiano para la disposición de aparatos electrónicos.

Algunas de las estrategias para disposición final son las siguientes:

- Subastar mediante un intermediario, aquellos equipos en funcionamiento y que para el hospital sean considerados obsoletos.
- Comercializar todo equipo dañado con empresas que tengan licencia ambiental para disposición y tratamiento de equipos electrónicos.

- Aquellos medios de información que ya no se requieran por obsolescencia (PC portátil y de escritorio), deben cumplir con las condiciones de borrado y/o formateo seguro antes de su disposición final (instructivo para borrado y/o formateo seguro).

14.27. Política de devolución de activos

Objetivo

Asegurar que los activos de información de propiedad del hospital sean devueltos de forma íntegra por funcionarios, contratistas y demás personas quienes hayan tenido responsabilidad de propiedad sobre los mismos.

Directrices

- Los funcionarios, contratistas y todos aquellos que se vinculen directa o indirectamente con el hospital, tienen como responsabilidad final realizar la devolución de los activos de información de la institución a su cargo y responsabilidad (software, documentos corporativos, equipamiento,

dispositivos de computación móvil, entre otros) al jefe de área respectiva; que a lo largo de su vida laboral se le asignó una vez que se dé por concluida toda relación o vínculo laboral.

- En los casos donde el funcionario, contratista y demás tengan bajo su administración información importante generada o accedida durante su desempeño en las funciones del cargo; dicha información deberá ser entregada al hospital a través de cada jefe de área para su almacenamiento y/o respaldo; la devolución de la información y demás activos será tenida en cuenta para el concepto de paz y salvo para con el hospital.

- Si un funcionario, contratista y demás con autorización de la Oficina Asesora Sistemas de Información Hospitalaria utiliza su equipo de cómputo personal, éste es responsable de transferir toda la información de propiedad del hospital al área de interés; dicha información deberá ser eliminada de manera confiable de su equipo como resultado de la finalización de su relación laboral.

- Al momento que un funcionario termine su vínculo laboral con el hospital o sea reasignado de área, éste debe hacer entrega formal de los activos de información que estaban a su cargo al jefe inmediato.

- Al momento que un funcionario termine su vínculo o relación laboral, las áreas responsables de gestionar los permisos de acceso físico y/o lógico a través de medios electrónicos o similares, deberán inactivar de manera oportuna dichos permisos.

- Toda devolución de activos tangibles de información se debe realizar mediante el área de activos fijos a través del formato de traslado generado por esta área.

- El área de recursos humanos y aquellas que gestionen contratistas o similares, deben ser las fuentes de información de los retiros de funcionarios, contratistas y demás externos.

14.28. Política de seguridad para relación con proveedores

Objetivo

Establecer pautas para identificar y mantener relaciones claras y fortalecidas con los proveedores del Hospital San José de San Bernardo del Viento, orientadas a recibir servicios y/o productos con calidad, oportunos y/o continuos teniendo en cuenta los acuerdos establecidos con ellos, garantizando de esta formala aplicación de medidas de seguridad adecuadas que aseguren el cumplimiento delos objetivos institucionales.

Directrices

La política de relación con proveedores, indica aquellas buenas prácticas que el Hospital San José de San Bernardo del Viento deberá tener en cuenta para establecer una relación clara y bien establecida con respecto al apoyo y soporte que debe tener en cuanto a la protección de seguridad de la información.

Por esta razón y para la protección de seguridad de la información, la relación con proveedores se define teniendo en cuenta las siguientes directrices:

- Calidad; seleccionar proveedores que ofrezcan productos y/o servicios que cumplan con estándares de calidad determinados por las mejores prácticas del sector y en lo posible que demuestre buenas prácticas de gestión mediante la presentación de certificaciones que evidencien su gestión de calidad, seguridad de la información u otro afín.
- Proveedor competente; determinar que el personal contratista sea calificado y competente para brindar los servicios que ofrecen dentro de sus propuestas.
- Idoneidad del proveedor; instaurar relaciones con proveedores legalmente constituidos, íntegros, formales y éticos en su accionar, sin ningún tipo de inhabilidad.
- Competitividad**;** que ofrezcan productos y/o servicios en las condiciones más competitivas del mercado a los intereses del Hospital San José de San Bernardo del Viento.
- Capacidad técnica y logística**;** que el proveedor cuente con la capacidad técnica, administrativa, logística y financiera para entregar los bienes y servicios en las condiciones negociadas.

- Respaldo; que la atención del proveedor sea directa y con mayor flexibilidad para adaptarse a las necesidades del Hospital San José de San Bernardo del Viento.
- Referencias; calificación en el sector o mercado como organización prestadora de servicios o proveedora de bienes o productos.
- Validación; todo acuerdo establecido formalmente entre el Hospital San José de San Bernardo del Viento y el proveedor, deberá estar soportado por medio de un contrato y/u orden de compra donde se valide elobjeto del contrato
- Seguimiento; todo servicio contratado por parte del Hospital San José de San Bernardo del Viento deberá estar bajo permanente monitoreo de su desempeño, calidad y oportunidad.
- Acceso a información; todo acceso a información a ser asignado a un tercero deberá estar previamente autorizado por el propietario del activo de información del área respectiva.

14.29. Política para la gestión de proyectos

Objetivo

Definir las reglas de seguridad para el resguardo de los activos de información sensibles para la gestión de los proyectos que se lleven a cabo dentro de la institución.

Directrices:

- Dentro de los objetivos del proyecto se deben incluir objetivos de seguridad de la información en concordancia con los activos de información a tratar.
- Identificar los activos de información sensibles que estarán involucrados en el diseño y desarrollo del proyecto.
- Incluir en la gestión del proyecto una evaluación de los riesgos para la protección de los activos de información y de esta forma identificar los controles necesarios.
- Definir los responsables en cada una de las etapas del proyecto a fin de que bajo su responsabilidad se implementen los controles relacionados al uso y/o tratamiento de los activos de información.
- La seguridad de la información debe ser parte de todas las etapas del

proyecto, independiente de la metodología utilizada.

14.30. Política para desarrollo externo de software

Objetivo

Velar porque el desarrollo externo de software cumpla con los requerimientos de seguridad esperados, con buenas prácticas para desarrollo seguro, así como con metodologías para la realización de pruebas de aceptación y seguridad. Además, asegurar que todo software desarrollado externamente cuente con el nivel de soporte requerido por el hospital.

Directrices:

- El propietario de los sistemas de información o a quien delegue es responsable de realizar las pruebas para asegurar que los sistemas de información cumplan con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- El área TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del hospital.
- El área TIC debe asegurar que los sistemas de información desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El área TIC, a través de sus funcionarios, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- Validar que los desarrolladores de los sistemas de información empleen buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- El área de TIC debe contar con un contrato de soporte vigente o asegurar la prestación de soporte por parte del proveedor de software (SLA). Los

desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo del hospital; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Validar que los desarrolladores construyan los aplicativos de tal manera que se efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable.

- Verificar que en los desarrollos efectuados se asegure la validación de la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Validar que en los desarrollos ejecutados existan los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecucióna los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Validar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

14.31. Política para seguridad de equipos y activos fuera de las instalaciones

Objetivo:

Proteger los activos y equipos de la organización que se encuentren fuera de las instalaciones.

Directrices:

- La asignación de equipos de cómputo debe ser realizada por el jefe de área y esta debe quedar documentada detallando el equipo asignado y usuario a quien se responsabiliza.

- El uso de equipos de cómputo y activos de información fuera de las instalaciones del hospital, debe ser autorizado por el jefe del área respectiva.

- Todo equipo de cómputo que sea retirado del hospital por aprobación del jefe de área para funciones del cargo, debe ser registrado en las bitácoras llevadas por la empresa de vigilancia al momento de ser retirado e ingresado de las instalaciones.

- Todo equipo que sea retirado del hospital no debe ser desatendido en áreas de acceso público y deben seguirse las directrices de la política de escritorio, pantalla limpia y equipos desatendidos.

- Cuando el usuario viaje con un equipo de cómputo portátil de propiedad del hospital, éste debe ser transportado como equipaje de mano y de forma disimulada.

- Se deben observar siempre las instrucciones del fabricante para proteger los equipos contra exposiciones a campos electromagnéticos, fuertes entradas de polvo, humedad, entre otros.

14.32. Política para seguridad de oficinas, recintos e instalaciones

Objetivo:

Proveer mecanismos de control y seguridad física en aquellas áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren equipos y demás infraestructura de soporte a los sistemas de información que se consideren áreas seguras y de acceso restringido.

Directrices:

- Mantener de manera discreta el centro de datos, las oficinas TIC y demás áreas donde se almacene información sensible, sin señales externas o internas de tal manera que las actividades de procesamiento de información se mantengan reservadas.

- No dejar solos en las oficinas o áreas seguras a personal ajeno al área (visitantes, proveedores, entre otros).

- Las puertas y ventanas de oficinas y recintos se deben mantener cerradas

cuando se termine la jornada laboral (en áreas que aplique) o cuando no haya vigilancia y se debe contar con protección externa para las ventanas ubicadas en niveles bajos.

- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos.
- Almacenar los equipos redundantes y la información de resguardo (Backup) en un sitio seguro y distante del lugar de procesamiento de información.
- Las visitas autorizadas para ingresar a áreas seguras donde se maneja información sensible, debe quedar registrado en bitácoras de control y durante la permanencia en éstas debe haber acompañamiento siempre por personal debidamente autorizado y que haga parte del área.
- El acceso a áreas seguras donde se procesa o almacena información sensible debe ser controlado y restringido solo a personas autorizadas.
- Todo lugar de trabajo en que exista algún riesgo de incendio, ya sea por la estructura del edificio o por la naturaleza del trabajo que se realiza, debe contar con extintores de incendio, de acuerdo al tipo de material combustible o inflamable.
- En áreas donde existan, se almacenen, trasvasijen o procesen sustancias inflamables o de fácil combustión, deberá establecerse una estricta prohibición de fumar.
- Almacenar los materiales peligrosos o combustibles en lugares seguros y bajo condiciones de seguridad.
- No se deben ingerir alimentos y/o bebidas en cercanías a los equipos y/o dispositivos de cómputo.
- Los funcionarios y terceros deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren dentro de las instalaciones.
- Mantener vigilancia continua dentro de las instalaciones del hospital.

14.33. Política de tratamiento y protección de datos personales

Introducción

En virtud de la Ley 1581 de 2012 (Art. 17 Lt. k y Art. 18 Lt. f) y del Decreto 1377 de 2013 (Art. 13.) mediante los cuales se dictan disposiciones para la protección de datos personales y en el desarrollo del derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, la ESE Hospital San José de San Bernardo del Viento en calidad de responsable del tratamiento de los datos personales de sus grupos de interés conformado por los usuarios y sus familias, colaboradores, contratistas, estudiantes, entidades responsables de pago y las entidades de inspección, vigilancia y control, información que se ha obtenido en el desarrollo de su actividad misional de prestar servicios de salud, por lo cual se compromete con el cumplimiento de la normativa mencionada y la protección de los derechos de las personas e informa a su grupo de interés que adopta las siguientes políticas sobre recolección, tratamiento y uso de datos personales.

Responsable del tratamiento de datos

La ESE Hospital San José de San Bernardo del Viento, identificada con NIT. 891000499-4, con domicilio en la ciudad de San Bernardo del viento , Km1 vía Lorica, Correo Electrónico: gerencia@esehospitalsanjose, teléfono (604) 7976500, es la responsable del tratamiento de los datos obtenidos de sus diferentes grupos de interés.

Directrices

La ESE Hospital San José de San Bernardo del Viento, en virtud de su objeto social, ha obtenido y conservado desde su creación, datos personales de sus grupos de interés, los cuales en adelante llamáremos titulares, los cuales son recolectados, almacenados, organizados, usados, transmitidos, actualizados, rectificados y en general administrados, de acuerdo con la respectiva relación y/o vinculación (civil, laboral, comercial o educativa) aplicando las siguientes directrices:

- La ESE Hospital San José de San Bernardo del Viento, está comprometida en dar un correcto uso y tratamiento de los datos personales y datos personales sensibles de sus titulares, evitando el acceso no autorizado a terceros que permita conocer, vulnerar, modificar, divulgar y/o destruir la

información, para lo cual cuenta con políticas de seguridad de la información que incluyen medidas de control de obligatorio cumplimiento.

- La ESE Hospital San José de San Bernardo del Viento, solicita a los titulares de la información los datos necesarios para administrar el riesgoen salud y dar cumplimiento a las funciones asignadas por la normativa vigente que regula el Sistema General de Seguridad Social en Salud. La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular.

- Salvo las excepciones previstas en la ley, el tratamiento de los datos personales sólo podrá realizarse con el consentimiento previo, expreso e informado de sus titulares, manifestado por escrito, de forma oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización.

- La ESE Hospital San José de San Bernardo del Viento, solicitará a las entidades responsables de pago, colaboradores, estudiantes y contratistas, los datos personales necesarios para establecer la respectiva relación y/o vinculación (civil, laboral, comercial o educativa). La información sensible requerida será de libre y voluntaria entrega por parte del respectivo Titular, quien deberá otorgar su consentimiento y autorización para su respectivo tratamiento.

- La ESE Hospital San José de San Bernardo del Viento, velará por el respeto y cumplimiento de los derechos fundamentales de los niños, niñas y adolescentes, observando los requisitos especiales establecidos para el tratamiento de sus datos personales y datos personales sensibles.

- El tratamiento de los datos personales proporcionados por los usuarios y sus familias de la ESE Hospital San José de San Bernardo del Viento, tendrá la siguiente finalidad:
  - Actualización de datos entregados por el Titular.
  - Para la prestación de los servicios asistenciales de sus usuarios y familias.
  - Caracterización y seguimiento a la población, para la gestión del riesgo en salud, utilizando la información derivada de los servicios asistenciales.
  - Entrega de reportes de Salud Pública de obligatorio cumplimiento.
  - Dar respuesta a requerimientos a entidades de control.

- Evaluación de indicadores de oportunidad y calidad de los servicios.
- Evaluación de la calidad de los productos y servicios de salud ofrecidos por la institución.
- Ejercer acciones legales y en la defensa de las mismas.
- Suministro de información a las autoridades competentes en caso de ser requerida.
- En general para cualquier otra finalidad que se derive de la naturaleza jurídica de la ESE Hospital San José de San Bernardo del Viento.

- El tratamiento de los datos personales proporcionados por los colaboradores de la ESE Hospital San José de San Bernardo del Viento, tendrá la siguiente finalidad:

  - Realización del proceso de selección de personal de acuerdo con suaptitud para un cargo o tarea.
  - Establecer una relación contractual.
  - Ofrecerle oportunidades de capacitación.
  - Evaluaciones de desempeño, satisfacción laboral, crecimiento personal, bienestar, seguridad y salud en el trabajo.
  - Cumplir el proceso de afiliación al Sistema General de Seguridad Social Integral (Entidades Promotoras de Salud, Administradoras deriesgos laborales, Fondos de pensiones y cesantías, Caja de Compensación)
  - Efectuar el proceso de Remuneración.
  - Ejercer acciones legales y en la defensa de las mismas.
  - Cumplir con exigencias judiciales.
  - Dar a conocer avances de la institución en aspectos investigativos, académicos y clínicos
  - Suministro de información a las autoridades competentes en caso deser requerida.

- En general para cualquier otra finalidad que se derive de la vinculación contractual.

➢ El tratamiento de los datos personales proporcionados por las entidades responsables de pago y contratistas de la ESE Hospital San José de San Bernardo del Viento, sean personas naturales o jurídicas, tendrála siguiente finalidad:

- Realizar la vinculación contractual.
- Efectuar el reconocimiento económico por la prestación del servicio.
- Suministro de información a las autoridades competentes en caso deser requerida.
- Ejercer acciones legales y en la defensa de las mismas.
- Cumplir con exigencias judiciales.

➢ El tratamiento de los datos personales de estudiantes que realizan prácticas en la ESE Hospital San José de San Bernardo del Viento, tendrá la siguiente finalidad:

- Presentar informes a las instituciones educativas
- Hacer invitación a eventos clínicos y académicos.
- Evaluar los conocimientos adquiridos durante su formación.
- Dar a conocer avances de la institución en aspectos investigativos,académicos y clínicos.
- Ejercer acciones legales y en la defensa de las mismas.
- Suministro de información a las autoridades competentes en caso deser requerida.
- En general para cualquier otra finalidad que se derive de la vinculación contractual.

Deberes de la ESE Hospital San José de San Bernardo del Viento

➢ Garantizar al usuario el pleno y efectivo derecho constitucional de habeasdata.
➢ Mantener la información en condiciones de seguridad y privacidad.
➢ Hacer uso de la información para los fines misionales y previstos en la ley.
➢ Tramitar de manera oportuna los reclamos que tengan los usuarios frente a la información consignada en la base de datos.
➢ No vender, circular o intercambiar la base de datos de sus usuarios, sin causa legal o contractual que lo justifique.
➢ Se debe conservar prueba del cumplimiento de la información suministrada al Titular, y cuando éste lo solicite, entregarle copia de esta.
➢ Al momento de solicitar al Titular la autorización la ESE Hospital San José de San

Bernardo del Viento deberá informar de manera clara y expresalo siguiente:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datosde las niñas, niños y adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

- El uso de los datos personales de los niños, niñas y adolescentes deberá cumplir con el requisito de responder y respetar los derechos prevalentes de este grupo poblacional, y sus derechos fundamentales.

- El representante legal del niño, niña o adolescente otorgará la autorización para el tratamiento de los datos personales del menor.

Derechos de los Titulares

El Titular de los datos personales y datos personales sensibles tendrá los siguientesderechos:

- Conocer, actualizar y rectificar los datos que aparezcan en la misma. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Conocer por qué y para qué la ESE Hospital San José de San Bernardo del Viento, recolecta información en base de datos.
- Revocar en cualquier momento la autorización dada para contener información personal en las bases de datos de la ESE Hospital San José de San Bernardo del Viento.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento considere que no se respetan los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a esta ley y a la constitución.
- Poner queja ante la Superintendencia de Industria y Comercio, cuando considere que le ha sido violado por parte de la ESE Hospital San José de San Bernardo del Viento, su derecho al Habeas Data.
- Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

Casos que no requieren autorización para el tratamiento de datos

La autorización del Titular no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

Entrega de información

La información que reúna las condiciones establecidas en el Art. 13 de la Ley 1581 de 2012, podrá suministrarse a las siguientes personas:

- A los Titulares, sus causahabientes o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el Titular o por la ley.

Área responsable de la atención de peticiones, consultas y reclamos.

El área responsable de la atención de peticiones, quejas, reclamos, sugerencias y felicitaciones será la oficina de Atención al Usuario (SIAU) de la ESE Hospital San José de San Bernardo del Viento, mediante la aplicación de su proceso: Gestión y tratamiento de PQRSF.

15. Capítulo II – Organización de la Seguridad de la Información

Compromiso de la dirección

La Junta Directiva del Hospital San José de San Bernardo del Viento aprueba el presente Manual de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información del hospital.

La Junta Directiva y la Gerencia del Hospital San José de San Bernardo del Viento

demuestran su compromiso a través de la:

- Revisión y aprobación de las políticas de seguridad de la información contenidas en este documento.
- Promoción de una cultura de seguridad de la información.
- Divulgación del presente manual a todas las partes interesadas.
- Disposición de los recursos adecuados para implementar y mantener laspolíticas de seguridad de la información.
- Verificación del cumplimiento de las políticas aquí mencionadas.
- Creación y seguimiento al Comité de Seguridad de la Información, con laparticipación de un representante de la alta gerencia.

Coordinación de la seguridad de la información

El Hospital San José de San Bernardo del Viento ha designado como representante de la alta dirección al Jefe Oficina Asesora Sistemas de Información Hospitalaria y responsable del Comité de Seguridad de la Información.
Dentro del Comité de Seguridad de la Información se definirán los responsables, roles y las funciones de los representantes de las otras áreas de la organización y quienes harán parte de dicho comité. Estas responsabilidades deben quedar inmersas en los contratos de trabajo, manual de funciones o el documento pertinente (para terceras partes).

15.1. Proceso de autorización para servicios de procesamiento de información

Al ingresar nuevos servicios, estos deben ser aprobados por la Oficina Asesora Sistemas de Información Hospitalaria y coordinados con el área que se encargará de la prestación del soporte y deben seguir el siguiente orden.

- Presentar la propuesta de la modificación o adición de un nuevo servicio TICal Líder de Sistemas de Información.

- Documento o acta de aprobación de la propuesta por parte del Jefe OficinaAsesora Sistemas de Información Hospitalaria.

La propuesta debe contener como mínimo:

- Descripción del problema a solucionar.
- Estudio de opciones con puntos a favor y en contra.
- Cotizaciones o presupuesto requerido
- Riesgos asociados antes, durante y después de la implementación.
- Diseño del plan de contingencia y temas relativos a la seguridad de la información

15.2. Acuerdos de confidencialidad

El departamento de Jurídica del Hospital San José de San Bernardo del Viento y el Jefe Oficina Asesora Sistemas de Información Hospitalaria, diseñaran los acuerdos de confidencialidad de acuerdo con los roles de todos los interesados (funcionarios de planta, contratistas, prestación de servicios, convenios docencia-servicios, etc.).
El área TIC NO podrá conceder permisos a ningún sistema de información sin que exista el debido acuerdo de confidencialidad y de no-divulgación firmado.
Los acuerdos de confidencialidad serán revisados como mínimo de forma anual por el departamento de Jurídica Hospital San José de San Bernardo del Viento y el Jefe Oficina Asesora Sistemas de Información Hospitalaria.

- **Autoridades y datos de contacto**

Entidad	Descripción	URL - Teléfono
Centro Cibernético Policial	Centro especializado de atención de delitos Cibernéticos de la policía Nacional de Colombia.	http://www.ccp.gov.co/ Tel: 57(1) 4266302 https://caivirtual.policia.gov.co/ Tel: 57(1) 5159700
Fiscalía general de la republica	Delitos Informáticos, dependencia adscrita al CTI de la Fiscalía General de la Nación	www.fiscalia.gov.co/colombia/tag/delitos-informaticos/
Dirección de Investigación Criminal “SIJIN”	Grupo de delitos investigativo informáticos	caivirtual@delitosinformaticos.gov.co Tel: 57(1)4266301 / 57(1)4266302 Delitos informáticos en el dpto. Huila Numero de celular 3112157043

3. EVALUACIÓN

Para evidenciar el nivel de comprensión y adherencia del Manual de Seguridad de la Información dentro de funcionarios, colaboradores, proveedores, contratistas y personas de interés general del Hospital San José de San Bernardo del Viento, se utilizará el instrumento: auditoria de adherencia en seguridad de la información. Los que se pretende

una vez realizado el proceso de sensibilización o capacitación, es medir el conocimiento y percepción de las políticas de seguridad de la información por medio de la lista de chequeo de la auditoria medir la adherencia y cumplimiento de las políticas por parte de funcionarios, colaboradores, proveedores, contratistas y personas de interés en general del hospital.