LA VERSIÓN DIGITAL Y ORIGINAL DE ESTE DOCUMENTO SE ENCUENTRA BAJO CUSTODIA DE LA OFICINA ASESORA DE PLANEACIÓN Y CALIDAD, LA LEGALIZACION DE ESTE DOCUMENTO SE REALIZA MEDIANTE LA IMPRESIÓN Y FIRMA DE LA PRIMERA HOJA DE DICHA VERSION; LA PRESENTE ES UNA COPIA IDÉNTICA DE LA ORIGINAL Y ES UN DOCUMENTO COPIA CONTROLADA DE CONSULTA.

LA OFICINA DE PLANEACIÓN Y CALIDAD ES RESPONSABLE DE PUBLICAR LAS ACTUALIZACIONES REALIZADAS POR EL PROCESO.

ESTA PUBLICACIÓN SE REALIZA CONFORME SE DESCRIBE EN EL DOCUMENTO: "PC-PR-007 PROCEDIMIENTO PARA LA ELABORACIÓN Y CONTROL DE LOS DOCUMENTOS DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN".

TABLA DE CONTENIDO

INTRODUCCION

EL Hospital Federico Lleras Acosta de Ibague – Tolima E.S.E. (En Adelante HFLLERAS), con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información que crea, custodia y almacena, se acoge al Modelo de Seguridad y Privacidad de la Información, MSPI, con el fin de implementar lineamientos para la adopción de buenas prácticas de seguridad de la información y cumplir con los lineamientos que el Ministerio de Tecnologías de la Información y las comunicaciones (MinTic).

Este documento se genera como base y guía de los temas más importantes en los que se tiene que trabajar en la entidad para el fortalecimiento de la gestión de TI, tomando como guía el Decreto 1008 del 14 de junio de 2018 – Política de Gobierno Digital, Manual de Gobierno Digital Versión 7 - abril de 2019, La metodología del Modelo de Seguridad y Privacidad de la Información y sus respectivos manuales y guías técnicas para la implementación de este.

Con las acciones de implementación no solo se identifican y clasifican los activos (inventario de activos de información) sobre los cuales se aplican diferentes controles para preservar la confidencialidad, integridad y disponibilidad de la información, sino que se evalúan los riesgos, amenazas, vulnerabilidades, se establecen responsables de la seguridad y se hacen las primeras mediciones. Vienen luego los indicadores, la valoración de los resultados y la mejora continua.

1. OBJETIVO

Establecer los lineamientos y políticas que regulan la seguridad de la información en el HFLLERAS, y presentar de forma clara y coherente a todas las unidades funcionales que componen la institución los elementos que conforman la política de seguridad para su conocimiento, y cumplimiento tanto de los funcionarios, contratistas, visitantes y terceros que prestan o consumen los servicios relacionados con el HFLLERAS, bajo el liderazgo del área de Tecnologia de la Información, en todos los procesos internos o externos vinculados a la institución para cada una de las tareas que se desempeñen.

1.1. OBJETIVOS ESPECIFICOS

- Proteger, preservar y administrar objetivamente la información del HFLLERAS, junto con las tecnologías utilizadas para su procesamiento frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de funcionalidad, integridad, disponibilidad, legalidad, y confiabilidad de la información.

- Establecer directrices, lineamientos relacionados con la seguridad de la información para su cumplimiento por parte de todas las partes interesadas del sistema en el HFLLERAS.

- Generar una cultura y concientización de la seguridad de la Informacion dentro del HFLLERAS enfocada a la apropiación de la protección y el uso adecuado de la información por parte de las partes interesadas.

- Establecer mecanismos de control para la protección de los activos de información del HFLLERAS y los recursos asociados que los soportan.

- Cumplir con los requisitos legales, normativos o contractuales aplicables y relativos a la seguridad de la información.

- Mantener la Política de Seguridad de la Información vigente y operativa.

2. ÁMBITO DE APLICACIÓN

El documento aplica a todos los procesos de la institución.

3. RESPONSABLE

Profesional Universitario de Tecnología de la Información.

4. DEFINICIONES

- **ACTIVO DE INFORMACIÓN:** Es todo aquello que, en el Hospital, es considerado importante o de alta validez para el mismo, porque información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.
- **AMENAZA:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en un equipo, como por ejemplo un virus.
- **AUTENTICACIÓN:** es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser). La autenticación por sí sola no verifica derechos de acceso del usuario; estos se confirman en el proceso de autorización. (Comisión Interamericana de telecomunicaciones, 2006)
- **AUTORIZACIÓN:** Un procedimiento por el cual se define a qué recursos de sistema el usuario autenticado podrá acceder. (RZ Redes Zone, 2020)
- **CONTROL DE ACCESO:** es un sistema automatizado que permite de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad establecidos por una empresa, comercio, institución o cualquier otro ente. (Sistemas Integrales de Seguridad, 2015)
- **CARPETA COMPARTIDA:** Carpeta cuyo contenido es accesible por todos los usuarios que pertenecen a un mismo grupo de trabajo.
- **CONFIDENCIALIDAD:** La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información. (Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán, 2013)
- **COPIAS DE RESPALDO (BACKUP):** Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Suele conservarse en un lugar seguro, generalmente en un dispositivo distinto de aquel en el que se encuentra el original y lejos de este. De esta forma, si la información original se daña es posible reconstruirla a partir de la copia.

- **CUOTA (QUOTA):** Límite, establecido por el administrador a cada usuario, para la asignación de espacio en el disco duro para almacenamiento de la información de la institución.
- **DATO:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **DISPONIBILIDAD:** Es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. (INFOSEGUR, 2013)
- **DISPOSITIVOS MÓVILES:** son aquellos dispositivos (portátiles, tablets y teléfonos móviles) que facilitan trabajar fuera de las instalaciones del Hospital.
- **FILE SERVER:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos del Hospital.
- **GOOGLE DRIVE:** Plataforma en la nube de Google que permite guardar los archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet.
- **HARDWARE:** Se denomina hardware a todos los componentes físicos internos de un ordenador, es decir, la parte tangible del equipo, como son: la placa base o placa madre, la CPU o procesador (unidad central de procesamiento), la memoria principal o memoria RAM (Random Access Memory), el disco duro (HD, SSD...), tarjetas gráficas, tarjeta de red, las entradas (USB, Serial), las salidas, fuente de alimentación, chasis, entre otros. (Tecnológicas, 2020)
- **INFORMACIÓN:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **INFORMACIÓN CONFIDENCIAL O CRÍTICA:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en el HFLL.
- **INTEGRIDAD:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **INVENTARIO DOCUMENTAL:** es un registro que sirve para indicar la cantidad de los expedientes que existen en un archivo, y tiene como principal utilidad, el poder expedientar correctamente los documentos existentes o nuevos. (Congreso de la República, 2000).
- **METODOLOGÍA:** Hace referencia al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. (Concepto Definición, 2020)

- **MSPI**: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MINTIC.
- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **SERVIDOR:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta apropiada.
- **SHAREPOINT:** Sitio web que ofrece un espacio central de colaboración y almacenamiento de documentos, información e ideas.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SEGURIDAD:** se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información. (Gerencial, 2016)
- **SEGURIDAD DIGITAL:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante, incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).
- **SISTEMA DE INFORMACIÓN:** es un conjunto de elementos que interactúan entre sí con un fin común; que permite que la información esté disponible para satisfacer las necesidades en una organización, un sistema de información no siempre requiere contar con recurso computacional, aunque la disposición de este facilita el manejo e interpretación de la información por los usuarios. (Panamá, s.f.)
- **SOFTWARE:** son los programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador. Por ejemplo, los sistemas operativos, aplicaciones, navegadores web, juegos o programas. (GcfGlobal, s.f.)
- **TELETRABAJO:** Todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".
- **VULNERABILIDAD:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5. MARCO LEGAL

El marco legal aplicable está de acuerdo con lo establecido en el Normograma institucional el cual se encuentra en el portal web de transparencia del HFLLERAS en la siguiente ruta:

- https://www.hflleras.gov.co/transparencia-0/4-normatividad/4-2

6. APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las políticas del sistema de gestión de seguridad y privacidad de la Informacion aplican y son de obligatorio cumplimiento para la alta dirección, gerentes, directores, jefes de Oficina, jefes de Área, funcionarios, contratistas, terceros, y en general a todos los usuarios de la información que permitan el cumplimiento de los propósitos generales del HFLLERAS.

7. POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

Para el Hospital Federico Lleras Acosta de Ibagué E.S.E, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos que se identifican de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica al HFLLERAS según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de HFLL.
- Garantizar la continuidad del negocio frente a incidentes.
- HFLLERAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

8. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar

cumplimiento de la política.

A continuación, se establecen los lineamientos de seguridad que soportan el SGSI del HFLLERAS:

- HFLLERAS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- HFLLERAS protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

- HFLLERAS protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- HFLLERAS protegerá su información de las amenazas originadas por parte del personal.

- HFLLERAS protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- HFLLERAS controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- HFLLERAS implementará control de acceso a la información, sistemas y recursos de red.

- HFLLERAS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- HFLLERAS garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- HFLLERAS garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- HFLLERAS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

9. ROLES Y RESPONSABILIDADES

El HFLLERAS definirá una estructura de roles y asignación formal de responsabilidades orientados a la seguridad y privacidad de la información en diferentes niveles del Hospital para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información

9.1. COMPROMISO DE LA ALTA DIRECCIÓN

La Gerencia General con el apoyo de la Junta Directiva son responsables de brindar su compromiso en la asignación de recursos y de fomentar la concientización sobre la importancia y la necesidad de la implementación, control y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información para el HFLL.

Su compromiso se demostrará a través de:

- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad de la información para los colaboradores definidos.

- Revisar y aprobar las políticas y lineamientos de seguridad de la información.

- Promocionar la cultura y concientización de la seguridad de la información dentro de la organización y a las partes interesadas.

- Manifestar liderazgo y apoyo continuo para la implementación del SGSI.

- Realizar actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

9.2. RESPONSABLE DE LA ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La responsabilidad de la gestión del sistema está a cargo de la Dirección de Tecnologia, las funciones que debe cumplir son:

- Promover la concientización y formación de los empleados en materia de seguridad de la información.

- Realizar revisiones periódicas del Sistema de Gestión de Seguridad y Privacidad de la Información (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes para su actualización.

- Controlar y revisar los indicadores definidos para el Sistema de Gestión de Seguridad y Privacidad de la Información.

- Generar un cronograma que incluya el desarrollo y actualización de la documentación del Sistema de Gestión de Seguridad y Privacidad de la Información.

- Trabajar de manera integrada con las áreas del alcance de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información.

- Contribuir al enriquecimiento del sistema de gestión del conocimiento en cuanto a la documentación de las lecciones aprendidas.

- Revisar los informes de auditoría y definir planes de trabajo con los dueños de los activos para la remediación de no conformidades.

- Definir y comprobar la aplicación del procedimiento de notificación y gestión de incidentes de Seguridad de la Información.

- Liderar la gestión de riesgos de seguridad de la información en el HFLLERAS

- Establecer los requerimientos mínimos de seguridad que deberán cumplir los proyectos en donde se afecten los activos de información.

9.3. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

La dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre la seguridad de la información van a ser tratados en el Comité de Gestión y desempeño.

En este comité se tratarán los siguientes temas:

- Aprobación de la política de seguridad de la información.
- Seguimiento a la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en HFLLERAS
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos institucionales.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.

Estas actividades se irán presentando dentro de la agenda del Comité.

9.4. USUARIOS DE LA INFORMACIÓN DEL HFLLERAS

Se entiende por usuario de la información cualquier funcionario, contratista, proveedor o tercero, que utiliza la información procesada y suministrada por el HFLLERAS para ejercer sus funciones. Entre las responsabilidades de los usuarios de la información se encuentran:

- Conocer, comprender y aplicar las políticas de seguridad de la información establecidas por el HFLLERAS.
- Garantizar la confidencialidad, Integridad y disponibilidad de la información que reciben, generan y procesan del HFLLERAS
- Cumplir con sus funciones y responsabilidades contractuales asegurándose de que sus acciones no afecten la seguridad de la información.
- Comunicar al responsable de Seguridad de la información, los incidentes de seguridad de la información que detecte durante el desarrollo de sus actividades.
- Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con seguridad de la información.
- Implementar las medidas de seguridad de la información necesarias en su área para evitar fraudes, robos o interrupción en los servicios o activos de información.
- Cumplir con las Políticas de Seguridad de la Información establecidas por el HFLLERAS.

10. POLITICAS Y LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

10.1. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

El HFLLERAS en cumplimiento al compromiso del Sistema de Gestión de Seguridad y Privacidad de la Información, crea una estructura de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información.

El Área de Tecnologías de la Información debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información del HFLLERAS a los funcionarios disponibles en el HFLLERAS, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

Los roles y responsabilidades de seguridad de la información se encuentran descritos las funciones de cada funcionario.

10.2. SEGURIDAD EN EL RECURSO HUMANO

El HFLLERAS a través del programa GA-PG-018 PLAN ESTRATEGICO DE TALENTO HUMANO para el personal de planta y para los contratistas de acuerdo con el GJ-MN-001 MANUAL DE CONTRATACIÓN, implementa controles para asegurar que todos los funcionarios, contratistas, proveedores y demás colaboradores del Hospital se les aplique los controles de seguridad de la información definidos en el proceso de selección, ingreso, y retiro. Durante su vinculación se les presente las responsabilidades en seguridad de la información.

Los funcionarios que se vinculen al HFLLERAS son seleccionados de acuerdo con los requisitos del manual de funciones y competencias del hospital y según los requerimientos específicos para la seguridad de la información definidos.

10.2.1. CAPACITACION Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACION

Al momento de la vinculación, el proceso de gestión humana también realizará la inducción a los funcionarios y contratistas en los temas relacionados con la

seguridad de la información, de acuerdo con los temas suministrados por el responsable de seguridad de la información.

El área de Gestión de Talento Humano, con el apoyo del responsable de seguridad de la Información, incluye lo pertinente del tema de seguridad de la información en el plan de capacitación anual y será divulgado a los funcionarios y contratistas de la organización.

La política de seguridad de la información y las relacionadas serán socializadas de acuerdo con las actualizaciones que puedan llevarse a cabo, y se publicara en la intranet del hospital para conocimiento de todo el personal objetivo.

El manual y los documentos relacionados están publicados en la Intranet del Hospital.

El plan de socialización de la seguridad y privacidad de la información se encuentra en más detalle en el instructivo, GA-IN-053 INSTRUCTIVO PARA LA CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

10.2.2.CAMBIO DE ESTADO O FINALIZACIÓN DE UN CONTRATO

En los procesos de desvinculación y/o retiro del Hospital, el funcionario, contratista, proveedor o colaborador debe hacer entrega de los activos de información entregados y generados durante su vinculación laboral y diligenciar el formato GA-FR-189 PAZ Y SALVO DE SERVICIOS DE TECNOLOGÍA con el fin de hacer la devolución formal de los activos de información a cargo.

Cuando el funcionario o contratista se retira del hospital, se recomienda realizar las siguientes acciones:

- Inhabilitar el acceso del usuario a todos los sistemas y recursos organizacionales relacionados.
- Hacer una copia de seguridad de todos los archivos del usuario (según solicite el jefe Inmediato y/o supervisor del contrato).
- Coordinar el acceso a los archivos del usuario para el jefe inmediato.
- Hacer eliminación segura de la información del hospital del dispositivo del contratista.

10.2.3.PROCESO DISCIPLINARIO

El adelantamiento de los procesos disciplinarios corresponde al área de Control Interno Disciplinario y de la Procuraduría General de la Nación, de acuerdo con las competencias señaladas en la ley.

Para los casos internos en que se violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad sin justificación alguna, el HFLLERAS tiene implementado un proceso disciplinario documentado en el procedimiento CD-PR-001 PROCEDIMIENTO PARA LA GESTION DE CONTROL INTERNO DISCIPLINARIO.

10.3. GESTION DE ACTIVOS DE INFORMACIÓN

Con el fin de mantener un control de la información, el HFLLERAS cuenta con un inventario de los activos de información, teniendo en cuenta los niveles de clasificación como Confidencialidad, integridad, disponibilidad y ubicación para lo cual debe realizar asignación de los responsables de los activos de información. Además, implementa directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.

10.3.1.RESPONSABILIDAD DE LOS ACTIVOS DE INFORMACIÓN

Se identifican los activos de información asociados a cada uno de los respectivos procesos del HFLLERAS, con su respectivo responsable y ubicación y se registra en el formato GA-FR-184 FORMATO DE IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACION.

El Inventario se deberá identificar, documentar y actualizar ante cualquier modificación de la información o su responsable y debe ser revisado en un periodo no mayor a un año.

El propietario del activo es el responsable de garantizar la confidencialidad, integridad y disponibilidad de la información del activo a cargo.

La responsabilidad de realizar y mantener actualizado el inventario de activos de información es del dueño del proceso correspondiente con el acompañamiento del

responsable de seguridad de la información.

La información, sistemas, servicios, activos físicos, equipos tales como computadores, equipos de impresión, servidores, entre otros; propiedad del HFLLERAS son activos que el hospital proporciona para el desarrollo de sus funciones y actividades, y su uso por parte de los usuarios se debe restringir a ejecutar actividades o funciones vinculadas con la organización y a satisfacer las necesidades del hospital.

10.3.2.CLASIFICACION DE LOS ACTIVOS DE INFORMACIÓN

La clasificación de los activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, es por eso que el HFLLERAS establece un sistema de clasificación con base a los lineamientos recomendados de la guía 5 del Modelos de Seguridad y Privacidad de la Información, la Norma ISO IEC 27005 – 2009, y la 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, para la clasificación de los activos de información ya que con base en su valor y de acuerdo a otras características particulares requiere un tipo de manejo especial.

El HFLLERAS mantiene un inventario actualizado de sus activos de información de acuerdo con el instructivo GA-IN-049 - INSTRUCTIVO PARA IDENTIFICACION Y REGISTRO DEL LOS ACTIVOS DE SEGURIDAD DE LA INFORMACION, quedando bajo la responsabilidad de cada propietario de información hacer el registro y actualización de los activos en el formato GA-FR-184 FORMATO DE IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACION por cada proceso.

Los niveles de clasificación de la información del Ministerio permiten identificar las características de protección, manejo y tratamiento de la información en cuanto a: niveles de acceso, métodos de distribución, restricciones en la distribución, almacenamiento, archivado, disposición y destrucción.

Se establecen los siguientes niveles de clasificación en el Ministerio (MINTIC):

- **Información Pública:** Se permite cualquier medio de divulgación o trasmisión que normalmente utilice el HFLLERAS, Se almacena en cualquier medio físico o magnético sin ningún tipo de protección. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014. Solo deben tener acceso los funcionarios explícitamente autorizados.

- **Información Pública Reservada:** Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley (1712 de 2014). Para su transmisión por medios electrónicos es obligatorio solicitar acuse de recibo al destinatario. Se debe mantener guardar en un medio protegido con controles de acceso o si se encuentra en medio físico debe estar bajo llave de manera que solo esté para el acceso al propietario

- **No Clasificada**: Es aquella información que no ha sido clasificada y por tal razón se le debe dar la misma protección de Información Publica Reservada.

La Entidad debe realizar el tratamiento de información documental de acuerdo con lo establecido en el programa GA-PG-008 PROGRAMA DE GESTION DOCUMENTAL y realizar el proceso de etiquetado de acuerdo con el instructivo GA-IN-051 INSTRUCTIVO DE CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN.

10.4. POLITICA DE CONTROL DE ACCESO

El hospital define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma tecnológica del HFLLERAS, considerándolas como importantes.

El acceso a la información del HFLLERAS deberá ser otorgado sólo a usuarios autorizados, los permisos y niveles de acceso deben estar basados en concordancia a los cargos y necesidades expresadas para la realización de las tareas relacionadas bajo su responsabilidad. El HFLLERAS asignara inicialmente

acceso basado en mínimo privilegio. El acceso solo se asignará a aplicativos y sistemas autorizados en ambiente productivo, el ingreso a ambientes de desarrollo y pruebas están sujetos aprobación.

Si entes externos (Exceptuando entes de control y vigilancia) requieren acceso a información crítica del HFLLERAS, se deben suscribir el formato GA-FR-138 ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN para la seguridad de la información.

El acceso a la información se realiza de acuerdo con los niveles de clasificación de la información y perfil asignado al usuario.

10.4.1.CONTROL DE ACCESO CON USUARIO Y CONTRASEÑA

El usuario y contraseña es de uso personal e intransferible, por ninguna razón se deberá acceder a la red o a los servicios del HFLLERAS, utilizando una cuenta o clave de otro usuario.

Toda acción realizada usando el usuario es responsabilidad directa del usuario al que se le asignó.

En caso de ausencia prolongada por incapacidad o vacaciones los usuarios deben solicitar la desactivación de la cuenta.

Los derechos de acceso a los equipos, la información o las instalaciones del HFLLERAS deben ser removidos una vez que los acuerdos contractuales con los empleados, contratistas o usuarios de la información sean finalizados.

10.4.2.SUMINISTRO DEL CONTROL DE ACCESO

El HFLLERAS 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. Cuando se requiere la creación de un perfil de usuario, se debe diligenciar el formato GA-FR-015 CREACIÓN DE CUENTAS DE USUARIOS.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose al área de Tecnología, en donde se llevará a cabo la validación de los datos personales (ver GA-IN-006 INSTRUCTIVO PARA SOPORTE A

USUARIOS FINALES); en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte del jefe de Área de Tecnologías de la información). Algunas contraseñas pueden ser cambiadas por los mismos usuarios, (ver GA-IN-046 INSTRUCTIVO PARA EL CAMBIO DE CONTRASEÑAS EN LAS APLICACIONES INSTITUCIONALES).

Las cuentas con inactividad superior a un mes serán deshabilitadas y requerirán de una solicitud del usuario para su activación, adicionalmente anualmente se hace una revisión aleatoria de los derechos de acceso a los sistemas.

En el GA-MN-003 MANUAL DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION se encuentra en mayor detalle asignación de claves de acceso.

10.4.3.GESTIÓN DE CONTRASEÑAS

Con el fin de definir los estándares mínimos de calidad que deben tener las contraseñas el HFLLERAS establece lo siguiente:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas diez anteriores.
- Las contraseñas no deben ser visibles al digitarse en la pantalla
- La contraseña debe cumplir con tres de los cuatro requisitos:
  - Caracteres en mayúsculas
  - Caracteres en minúsculas
  - Base de 10 dígitos (0 a 9)
  - Caracteres no alfabéticos mínimo uno (Ejemplo: ¡, @, #, $, %, &. etc.)
- Las contraseñas deben ser cambiadas cada 30 días.

Con el fin de facilitar la gestión de cambio de contraseñas el HFLLERAS pone a disposición el Instructivo GA-IN-046 INSTRUCTIVO DE CAMBIO DE CONTRASEÑAS en las aplicaciones institucionales, donde se encuentra de forma detalla los cambios de contraseñas en las aplicaciones Spark, D.G.H y el Correo electrónico.

10.4.4. CUENTAS PRIVILEGIADAS (ADMINISTRACIÓN)

Las cuentas privilegiadas son aquellas con acceso de administración sobre los sistemas de información, motores de bases de datos o software base (sistemas operativos).

Estas cuentas son asignadas a los administradores de los sistemas del área de tecnología de la Información y por sus privilegios sobre los sistemas, los rigen los siguientes lineamientos.

- El área de tecnología de la información define un responsable para la administración de cuentas privilegiadas.
- Se cambian las contraseñas que vienen de fábrica y se asignan una teniendo los criterios de complejidad. En lo posible se deshabilitan los usuarios y se crean propios para la administración del sistema.
- Se habilita log de registro cuando se requiera, con el fin de tener trazabilidad de los usuarios privilegiados, en caso de un incidente de seguridad de la información.

10.4.5. REGISTRO DE INICIO DE SESIÓN SEGURO

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda durante el proceso de autenticación.
- Limitar el número de intentos fallidos a un máximo de 5 intentos, auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas en el proceso de acceso.
- No transmitir la contraseña de autenticación en texto claro.

10.5. POLITICA DE CONTROLES CRIPTOGRAFICOS

Con el fin de proteger los activos de información durante su transporte o envió por medios electrónicos, la información clasificada como publica reservada o publica clasificada se deben utilizar software o programas de cifrado de archivos para mitigar riesgos de fuga o pérdida de la información.

En el caso de uso de firmas digitales, la asignación de estas se realiza de acuerdo

con las necesidades del hospital y será solicitará al proveedor de acuerdo con la disponibilidad de asignación. El cifrado de la misma estará directamente ligado a las necesidades de procesamiento, software y necesidad de autenticidad requerida y se asignará un responsable de su manejo.

Para el acceso a medios bancarios o del estado donde se requiera el uso de Tokens y controles criptográficos, serán gestionados de acuerdo con las políticas y directrices emitidas por el HFLLERAS y de acuerdo con los requisitos de cada banco y deben ser coordinados en los líderes de proceso quienes requieran su uso y el área de tecnologías de la información para garantizar la buena operación de estos.

Los sitios del HFLLERAS que recojan información de ciudadanos o que por su naturaleza requieran comunicar la autenticidad del sitio, deberán contar con certificados SSL.

10.6. POLITICA DE ESCRITORIO Y PANTALLA LIMPIOS

EL HFLLERAS debe adoptar la medida de escritorios limpios de papeles, y medios de información, junto con una medida de pantalla limpia, para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Los siguientes controles deben ser considerados:

- Todo el personal del HFLLERAS debe conservar su lugar de trabajo libre de información propia del hospital, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento, esto incluye documentos en papel y dispositivos de almacenamiento como CD, USB, unidades de disco externas, etc.

- Todo el personal del HFLLERAS debe mantener cerrada la sesión de su equipo de cómputo o bloqueada cuando no esté presente o no estén haciendo uso de ellos. Se recomienda para lo anterior usar la combinación de teclas “Logotipo de Windows y L” o CTRL + ALT + DEL y, en el menú de opciones, haga clic en Bloquear este computador.

- Todos los usuarios al finalizar sus actividades diarias deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

- Se deben mantener las oficinas, escritorios y áreas donde se maneje información cerradas y en ausencia de personal con llave para evitar el ingreso de personas ajeno al lugar donde se maneja información.

- Al imprimir documentos con información clasificada como publica reservada o publica clasificada, no deben ser desatendidos en la impresora y retirados inmediatamente. Así mismo, no se deben reutilizar papel que contenga información confidencial.

- Las fotocopiadoras o escáneres deben estar protegidas de uso no autorizado.

- Los tableros o pizarras donde se escriba información como parte de reuniones deben ser borrados al finalizar las mismas para evitar el acceso a información confidencial.

10.7. POLITICA DE TRANSFERENCIA DE INFORMACIÓN

El HFLLERAS con el fin de proteger la transferencia de información del hospital se establece las directrices para reducir el riesgo de pérdida de información las cuales están descritas en el GA-MN-010 MANUAL PARA LA TRANSMISION DE DATOS.

El Área de Tecnologías de la Información, realiza el control del uso de sistemas de transferencia de archivos a terceros, sin embargo, es responsabilidad de los funcionarios, contratistas, proveedores y demás colaboradores del Hospital seguir los lineamientos e informar al Tecnologia, sobre su uso.

10.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

El HFLLERAS integra la seguridad a los sistemas de información garantizar que la seguridad es parte integral de los sistemas de información.

Los sistemas de información del HFLLERAS a usar pueden ser adquiridos a través de terceras partes bien sea en desarrollos a la medida o mediante herramientas comerciales o no comerciales que satisfagan la necesidad que se pretende

subsanar, sin olvidar que cumplan con medidas o elementos de seguridad. Las herramientas desarrolladas o adquiridas deben estar basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.

La supervisión y seguimiento a proyectos de infraestructura informática deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado al hospital.

Los desarrollos de software deben incluir pruebas de funcionalidad en la cual se evidencia los controles de seguridad establecidos relacionas con la confidencialidad, integridad y disponibilidad, lo anterior debe involucrar la correspondiente documentación interna y externa que permitan identificar sus procedimientos de funcionamiento.

Todos los desarrollos de software, adquisición de sistemas de información y adquisición de equipos de cómputo, deberán tener el aval del área de Tecnologia de la Información.

10.8.1.POLITICA DE DESARROLLO SEGURO

Con el objetivo que los programas desarrollados y actualizaciones de software por el HFLLERAS o sus proveedores y/o contratistas incluyan buenas prácticas de programación segura se establecen los siguientes lineamientos:

- Validar que la información que está en los sistemas de producción no disminuya los niveles de protección, por tanto, para procesos de desarrollo y pruebas, se debe evitar el uso de datos de producción y en caso de ser necesario su utilización, garantizar la eliminación segura al momento de finalización de las pruebas.
- Hay que asegurar que se diseñe e implemente los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
- Los desarrollos adquiridos a través de terceros deben tener un proceso formal de adquisición. Los contratos con los proveedores tendrán incluidos los requisitos de seguridad de la información y el GA-FR-138 ACUERDO DE CONFINDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

- Todos los sistemas de información del HFLLERAS deben pasar por un ciclo de pruebas de aceptación tanto funcionales como de seguridad antes de ser puestos en producción.

Los lineamientos de la política se encuentran en el instructivo GA-IN-050 INSTRUCTIVO PARA DESARROLLO SEGURO DE APLICACIONES

10.9. SEGURIDAD EN LAS OPERACIONES

El HFLLERAS estable los lineamientos para el desarrollo de operaciones correctas y seguras de las instalaciones de procesamiento de Hospital, con el fin de robustecer la continuidad de los sistemas de tecnológicos.

Las actividades realizadas en el hospital están definidas a través de procedimientos, manuales e instructivos debidamente documentados de acuerdo con el PC-PR-007 PROCEDIMIENTO PARA LA ELABORACIÓN Y CONTROL DE LOS DOCUMENTOS DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.

Todos los documentos tendrán un responsable para su definición, mantenimiento e implementación.

La gestión de operaciones tecnológicas está bajo el liderazgo del área de Tecnologia de la Información, que, con el apoyo de las demás áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción. Por ninguna razón se realizarán labores de mantenimientos, ajustes y desarrollos a las aplicaciones directamente en el ambiente de producción, sino serán probados en los ambientes de pruebas para no afecta la continuidad de las operaciones.

10.9.1.CONTROL DE SOFTWARE OPERACIONAL

Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo del HFLLERAS, la interfaz del sistema operativo está configurada solo para que usuarios administradores realicen cambios sobre el equipo y esta labor está a cargo del área de tecnología de la información, para los funcionarios solo debe estar configurada con privilegios de usuario. En caso de detectar que el usuario permite cambios en las aplicaciones del computador, se

debe informar al área de tecnología para su corrección.

10.9.2.PROTECCION CONTRA CODIGO MALICIOSO

Toda la infraestructura de procesamiento de información del HFLLERAS, cuenta con un sistema de detección y prevención de virus, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

En todas las estaciones de trabajo y servidores del HFLLERAS se restringe la ejecución de aplicaciones y se mantiene instalado y actualizado el antivirus.

Todos los funcionarios, terceros y/o Contratistas que hacen uso de los servicios tecnológicos y de comunicaciones del HFLLERAS son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

Todos los computadores de terceros que sean autorizados para trabajo en el Hospital deben traer un antivirus licenciado, el cual será verificado por el área de Tecnología de la Información

El antivirus es administrado por el área de Tecnologia y por ninguna razón debe ser manipulado o desinstalado de las maquinas. En caso de presentar fallas o comportamientos o informes de virus, se debe informar inmediatamente a Tecnología.

Todos los equipos conectados a la infraestructura del Hospital pueden monitoreados y supervisados por el área de Tecnología de la Información a través de la herramienta de antivirus, la cual se mantendrá actualizada a las últimas versiones.

En el GA-MN-003 MANUAL DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION se encuentra en mayor detalle las medidas de prevención de código malicioso.

10.9.3.GESTION DE VULNERABILIDADES

Con el fin de establecer el grado de exposición en términos de vulnerabilidades, en el que se encuentran los componentes de la infraestructura tecnológica de HFLLERAS., así como también la generación de recomendaciones y plan de acción para evitar y controlar toda situación adversa que se pueda generar a partir de cada vulnerabilidad.

Anualmente se implementa un programa de gestión de vulnerabilidades en el hospital, cuyo objetivo es identificar los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

El área de Tecnologías de la Información realizará seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas y programa pruebas de verificación para validar que hayan quedado resueltas.

Este programa se aplica para Servidores, aplicaciones y desarrollos propios y de terceros en el hospital.

10.9.4.COPIAS DE RESPALDO

Co el objetivo de mantener la disponibilidad de la información el HFLLERAS cuenta con copias de respaldo de la información almacena en los servidores con el fin de protegerla en caso de pérdida o daño de los servidores de producción, el proceso se realiza diariamente de acuerdo con las políticas de retención de los servidores, y se hacen revisiones periódicas de su funcionalidad y eficacia. Se realiza pruebas de restauración para validar su funcionalidad de forma periodicidad.

La retención de las copias de respaldo y tiempos de restauración a usuarios se gestiona de acuerdo con la capacidad gestionada por el área de sistemas, cuando esta se realizar en los servidores del Hospital, adicionalmente , en el caso de los usuarios que cuenten con correo electrónico del Hospital pueden almacenar hasta 15G de información en un servicio externo llamado Google Drive licenciado por el Hospital, para el uso de este almacenamiento de Backup existe GA-IN-045 INSTRUCTIVO PARA EL USO DEL GOOGLE DRIVE, que detalla el proceso de configuración y uso.

Para copias de respaldo de equipos de funcionarios se realizar de acuerdo con una solicitud a tecnología.

La copia del respaldo de los servidores de producciones se hace de acuerdo con el instructivo GA-IN-008 RESPALDO DE DATOS A APLICACIONES DE PRODUCCIÓN.

El almacenamiento del Backup se realiza en la nube y también se hacen copias en cintas externas que se alojan fuera de las instalaciones principales. El registro de las copias de seguridad se controla a través de la consola de Backup.

10.9.5.REGISTRO DE ACCESO (LOGS)

El registro de acceso a los diferentes sistemas de información del HFLLERAS, deben estar activos y deben guardar como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado. Los datos que contiene el registro de acceso deben conservarse de acuerdo con el periodo de retención definido por el HFLLERAS y el cumplimiento de la legislación aplicable.

10.9.6.SINCRONIZACIÓN DE RELOJES

Todos los relojes de la infraestructura de procesamiento de información del HFLLERAS deben estar sincronizados con la hora legal colombiana.

10.9.7.USO DE DISPOSITIVOS MÓVILES

En el HFLLERAS el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, está permitido para el acceso a los aplicativos Web del hospital y el acceso al correo electrónico institucional, de acuerdo con las necesidades del cargo, sin embargo, bajo el compromiso de uso de software legal y antivirus actualizado.

Los dispositivos móviles de propiedad del hospital, asignados para el desarrollo de sus funciones son para uso de las actividades propias del cargo o desempeño laboral y deben estar protegidos con una contraseña de inicio de sesión. El uso del dispositivo está limitado para actividades laborales y no puede ser usado para

almacenar información personal o instalación de aplicaciones ajenas a las actividades del hospital.

Si el dispositivo requiere acceso a aplicaciones o información no publicados en la web, deberá hacer solicitud formal de una conexión VPN al área de Tecnologia de la Información previa autorización de su jefe directo. La conexión estará limitada a las aplicaciones requeridas siempre y cuando sean compatibles por el dispositivo móvil.

El área de tecnologías de la información adoptará medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móviles.

10.9.8.USO DE INTERNET

Este servicio debe utilizarse exclusivamente para el desempeño de las actividades desarrolladas del Hospital, mediante su buen uso y asegurar una adecuada protección de la información.

- Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro del Hospital.

- Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones del Hospital deben realizarlo por medio de la red WIFI y cumplir con los requerimientos que el área de sistemas, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

- No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo definidas desde la herramienta de administración de contenidos del Hospital

- No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

10.9.9.USO DE REDES SOCIALES

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del Hospital.

- El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con el Hospital.

- No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

- La Oficina de Tecnología de la Información del Hospital, será el encardo de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales de acuerdo con las actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar.

- No se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

10.9.10. GESTIÓN DE CAMBIOS

Con el fin de asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en HFLLERAS se realicen de forma controlada, se tienen documentados en el instructivo GA-IN-007 MANTENIMIENTO A APLICACIONES EN PRODUCCIÓN para el control de cambios ejecutados en el hospital.

Para los pasos a producción o actualización de infraestructura de producción se realiza una solicitud de cambio en los servicios previamente acordado con los dueños de los sistemas de información y en horarios que minimice el impacto

Los cambios a sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información

10.9.11. GESTION DE CAPACIDAD

El HFLLERAS realiza un seguimiento periódico de la capacidad de los servidores y servicios con el fin de realizar proyecciones de los requisitos sobre la capacidad futura y lleva un control de seguimiento en el instructivo GA-IN-052 INSTRUCTIVO PARA LA GESTIÓN DE CAPACIDAD DE T.I y el formato GA-FR-191 BITÁCORA PARA LA GESTIÓN DE CAPACIDAD DE LA INFRAESTRUCTURA DE T.I.

10.9.12. AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN

El HFLLERAS establece y mantiene ambientes separados para el desarrollo y pruebas de los servicios y aplicaciones que están siendo ajustadas antes de su paso a producción, con el fin de reducir los riesgos asociados a modificaciones, alteraciones, cambios o accesos no autorizados en sistemas en producción del hospital.

En el hospital se debe seguir lo definido en el instructivo GA-IN-007 MANTENIMIENTO A APLICACIONES EN PRODUCCIÓN para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente.

En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción, sin antes haber pasado por un proceso de ofuscamiento.

Se debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.

Se deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.

10.10. SEGURIDAD FISICA Y DEL ENTORNO

El HFLLERAS se preocupa por el entorno físico donde se almacena y proceso la información, por esa razón implementa medidas de seguridad para evitar accesos físicos no autorizados a las instalaciones, que atenten contra la confidencialidad, integridad o disponibilidad de la información del Hospital. Las medidas de

seguridad física del hospital se pueden ver de forma detalla en el manual GA-MN-006 MANUAL PARA LA PRESTACION DEL SERVICIO DE SEGURIDAD Y VIGILANCIA

10.10.1. AREAS SEGURAS

Las áreas seguras dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

Las actividades de limpieza en las áreas seguras son controladas y supervisadas por los funcionarios del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas u otros objetos que no sean propios de las tareas de aseo.

Se cuenta con dispositivos de control de acceso físico al Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, el cual garantice el acceso a solo el personal autorizado.

En el caso de acceso al centro de datos y cableado se debe diligenciar el formato GA-FR-154 CONTROL DE ACCESO AL DATACENTER, previa autorización del área de tecnología.

10.10.2. EQUIPOS DE TECNOLOGIA.

La plataforma tecnológica (Hardware, software y comunicaciones) cuenta con las medidas de protección física y eléctrica, con el fin de evitar daños, interceptación de la información o accesos no autorizados.

Se tiene instalado sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia y generadores de energía en caso de ausencia de energía. Así mismo, se cuenta con contratos de mantenimiento y soporte para la protección de la infraestructura tecnológica, el cual se puede ver en detalle en el instructivo. GA-IN-011 MANTENIMIENTO DE HARDWARE.

10.10.3. SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

Los equipos portátiles que contengan información clasificada como confidencial o reservada, deben contar con controles de seguridad que garanticen la confidencialidad de la información.

Los equipos portátiles no deben estar a la vista en el interior de los vehículos, en lo posible debajo de la silla o en el baúl. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al área de logística y Tecnología de la Información y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.

Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones del Hospital. Para el caso de los equipos que cuentan con puertos de transmisión y recepción de infrarrojo y Bluetooth estos deben estar deshabilitados.

10.10.4. SEGURIDAD EN LA REUTILIZACIÓN O ELIMINACIÓN DE LOS EQUIPOS DE COMPUTO

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada, posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

En los casos que el equipo debe ser dado de baja, se debe diligenciar el formato GA-FR-144 FICHA DE ACTIVOS CON CONCEPTO TECNICO DE BAJA

10.10.5. POLITICA DE TELETRABAJO Y TRABAJO EN CASA

En los casos que el acceso a los sistemas de información del HFLLERAS no pueda realizarse en sitio y se apruebe sea mediante la modalidad de teletrabajo o trabajo en casa, los responsables de estas actividades deberán dar cumplimiento a las condiciones y restricciones definidas entorno a la seguridad de la

información, tales como:

- Seguridad física y de comunicaciones.
- Amenazas de accesos no autorizados a información o recursos.
- Acuerdos de licenciamiento para establecer responsabilidades.
- Establecer políticas acerca de derechos de propiedad intelectual desarrollada en equipos de propiedad privada.

Además, se deberán definir en los lineamientos de acuerdo con la modalidad escogida, los cuales incluirán:

- El suministro de equipo adecuado y de dispositivos de almacenamiento para las actividades de teletrabajo, cuando no se permite el uso del equipo de propiedad privada que no está bajo el control del hospital.
- Una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el teletrabajador está autorizado a acceder.
- El suministro de soporte y mantenimiento del hardware y el software
- Los procedimientos para copias de respaldo y continuidad del negocio
- Auditoría y seguimiento de la seguridad
- La revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades finalicen.

El área de tecnología de la información previa solicitud y autorización asignará los permisos de acceso por medio de una Red privada Virtual (VPN).

Los procesos de autorización están regidos de la siguiente forma:

- El Teletrabajo deberá estar autorizado y reglamentado por él área de Talento Humano, de acuerdo con la Ley 1221 de 2008: “Por la cual se establecen normas para promover y regular el Teletrabajo…” y el Decreto 884 de 2012: “Por medio del cual se reglamenta la Ley 1221 de 2008, y definirá los compromisos de buen uso de la información”.
- El trabajo en casa se autorizará solo para casos de emergencia u ocasiones especiales de acuerdo con la ley 2088 de 12 de mayo de 2021 "Por la cual se regula el trabajo en casa y se dictan otras disposiciones…" y deberá estar aprobado por el jefe del área y la Oficina de Talento Humano.

10.11. GESTION DE SEGURIDAD EN LA REDES

El HFLLERAS proporciona a los funcionarios, contratistas y/o terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el área de Tecnologia de la Información.

10.11.1. SEGREGACIÓN DE REDES

El HFLLERAS establece un esquema de segregación de redes (VLAN), entre las diferentes áreas y servidores con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se establecen medidas técnicas para la conexión segura de la red con los servicios de red, entre ellos mecanismos de autenticación segura para el acceso a la red y registro de equipos para evitarla la conexión no autorizada.

Se encuentran separadas las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información, adicionalmente se tienen establecido grupos de conexión con diferentes niveles de seguridad.

10.12. RELACIONES CON PROVEEDORES Y TERCEROS

En los contratos o acuerdos con los proveedores y/o contratistas se debe establecer mecanismos de control, con el objetivo de asegurar que la información que tenga acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del HFLLERAS, incluyendo la firma del GA-FR-138 ACUERDO DE CONFINDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN.

Se establecen criterios de selección que contemplan experiencia 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 el hospital, lo anterior se apoya en el documento GA-

MN-005 MANUAL PARA LA GESTIÓN DE COMPRAS.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del HFLLERAS, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

10.13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

El HFLLERAS establece un procedimiento GA-IN-048 INSTRUCTIVO PARA LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION, y un formato GA-FR-183 BITACORA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION, para gestionar los eventos que puedan afectar la seguridad y privacidad de la información con el fin de gestionarlo de forma eficiente y estandarizar las actividades a seguir para su atención y manejo.

El objetivo principal de la gestión de incidentes es tener una estructura adecuada de administración de los incidentes de seguridad, de tal manera que permitan generar oportunidades de mejora, cuantificar y clasificar los incidentes de seguridad de la información, a través de una base registros de incidentes que permitan generar indicadores.

10.14. GESTION DE LA CONTINUIDAD DEL NEGOCIO

El HFLLERAS es importante establecer estrategias que permitan garantizar el funcionamiento del hospital ante incidentes que afecten la continuidad de las operaciones, por lo anterior tiene definido un conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades del hospital, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

El HFLLERAS trabaja en prevenir interrupciones en la funcionalidad de la plataforma tecnológica del hospital, que generan indisponibilidad de la funcionalidad de los procesos del hospital, afectados por situaciones no previstas o desastres.

El HFLLERAS debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.

El HFLLERAS establecerá un plan de pruebas periódico para entrenar y validar la funcionalidad del plan de contingencia de la plataforma tecnológica.

En el instructivo, GA-IN-054 INSTRUCTIVO PARA LA GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO, se encuentra en mayor detalle las directrices para la continuidad en la seguridad de la información, de los servicios del HFLLERAS.

10.15. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

El HFLLERAS con el fin de proteger la información personal establece el GA-MN-008 MANUAL DE POLITICA DE TRATAMIENTO DE DATOS PERSONALES, donde se describen los lineamientos para el tratamiento de datos personales.

El objetivo del manual es cumplir con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios para el tratamiento y seguridad de la información personal.

El manual contempla el tipo de información que está sujeta a tratamiento, los derechos y deberes de los titulares de los datos, modos de utilización de la información y sus finalidades.

Los lineamientos y políticas de seguridad de la información del HFLLERAS cubren la información que hace parte del tratamiento.

10.16. POLITICA DE GESTIÓN DOCUMENTAL

El HFLLERAS es importante establecer un control de la información que genera, almacena y custodia por ese motivo establece un programa anual GA-PG-008 PROGRAMA DE GESTION DOCUMENTAL, para la protección de la información en la cual se tuvieron en cuenta las directrices definidas por el gobierno nacional.

10.17. MEJORA CONTINUA DEL SGSI

Una vez realizado el seguimiento, evaluación, análisis y monitoreo al Sistema de Seguridad y Privacidad de la Información, es necesario, desarrollar un proceso de mejoramiento continuo, el cual le permitirá al HFLLERAS, establecer oportunidades de mejora para corregir y mejorar el sistema.

Para lograr la mejora continua se deben tener en cuenta las siguientes consideraciones:

- Cuando existan no conformidades, el proceso correspondiente debe llevar a cabo las acciones para mitigar el impacto de su existencia.
- Se revisan las no conformidades para disminuir o eliminar las causas y consecuencias que estas puedan generar, y evitar que se presente nuevamente.
- Se determinan si existen otras no conformidades similares para establecer acciones preventivas evitando su materialización.
- Emprender acciones preventivas que permitan gestionar el riesgo a tiempo, disminuyendo el impacto y la probabilidad de ocurrencia.
- Llevar un registro en el sistema de información que determine el HFLLERAS a los tratamientos realizados y a las no conformidades, así como las acciones realizadas para mitigar el impacto.

11. CONTROL DE REGISTROS

Identificación		Almacenamiento		Clasificación	Tiempo de retención en archivo de gestión	Disposición Final
Código Formato	**Nombre**	**Lugar de Archivo**	**Medio de archivo**			
PC-FR-070	Acta de entrega de la gestión	Gestión del talento Humano	Físico	Fecha	80 años	Forma parte de la Hoja de vida
GA-FR-184	Formato de identificación de activos de seguridad de la información	T.I	Electrónico	Fecha	2 Años	Histórico
GA-FR-138	Acuerdo de confidencialidad y no divulgación de la información	T.I	Físico	Fecha	2 Años	Archivo Central
GA-FR-015	Creación de cuentas de usuarios	T.I	Físico	Fecha	2 Años	Archivo Central
GA-FR-037	Bitácora de seguimiento al soporte de infraestructura**.**	T.I	Electrónico	Fecha	2 Años	Histórico
GA-FR-154	Control de acceso al Datacenter	T.I	Físico	Fecha	2 Años	Archivo Central
GA-FR-144	Ficha de activos con concepto técnico de baja	T.I	Físico	Fecha	2 Años	Archivo Central
GA-FR-183	Bitácora gestión de incidentes de seguridad de la información	T.I	Electrónico	Fecha	2 Años	Histórico
GA-IN-050	Instructivo para desarrollo seguro de aplicaciones	T.I	Electrónico	Fecha	2 Años	Archivo Central
GA-IN-051	Instructivo de clasificación y etiquetado de información	T.I	Electrónico	Fecha	2 Años	Archivo Central
GA-IN-052	Instructivo para la gestión de capacidad de T.I.	T.I	Electrónico	Fecha	2 Años	Archivo Central
GA-IN-053	Instructivo para la capacitación en seguridad de la información	T.I	Electrónico	Fecha	2 Años	Archivo Central
GA-IN-054	Instructivo para	T.I	Electrónico	Fecha	2 Años	Archivo

	la gestión de la seguridad y privacidad de la información en la continuidad del negocio					Central
GA-FR-189	Paz y salvo de servicios de tecnología	T.I	Físico	Fecha	2 Años	Archivo Central
GA-FR-190	Declaración de aplicabilidad del sistema de gestión de seguridad de la información	T.I	Electrónico	Fecha	2 Años	Archivo Central
GA-FR-191	Bitácora para la gestión de capacidad de la infraestructura de T.I.	T.I	Electrónico	Fecha	2 Años	Archivo Central

12. CONTROL DE CAMBIOS

FECHA DEL CAMBIO	VERSIÓN	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
31/08/2022	1	Creación documento	P.U. de Tecnología de la información
31/10/2022	2	Integración de nuevos instructivos y formatos	P.U. de Tecnología de la información