PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2023

MAURICIO ANTONIO TORO ZAPATA

GERENTE

INTRODUCCIÓN

Para la ESE Hospital la Merced la información es un activo que cobra importancia en la optimización de sus procesos que se refleja en la satisfacción de los pacientes, por ende, se hace necesario definir el proceso necesario para colocar en marcha la implementación del Modelo de Seguridad de La Información expedido por el Ministerio de Tecnología y Comunicaciones del Estado Colombiano.

La estrategia de Gobierno en Línea - GEL, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente

El Plan de Seguridad y Privacidad de la Información y Continuidad de TI para estar acorde con las buenas prácticas de seguridad y continuidad deberá ser actualizado periódicamente; así mismo recoger los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La seguridad de la información garantiza que los responsables de la información sean capaces de gestionar la información de forma segura, independientemente del formato o soporte en el que se encuentra. Mediante el proceso de Gestión de TI y el modelo de seguridad y privacidad de la información y de continuidad de TI, se trabajará en el fortalecimiento de la seguridad de la información en el HUFT, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

2. OBJETIVOS

2.1 General

Establecer los lineamientos que respondan asertiva y oportunamente a eventos que afecten la seguridad de la información en el marco del Plan de Seguridad y Privacidad de la Información.

2.2 Específicos

- Optimizar la gestión de la seguridad de la información al interior de le entidad
- Definir las fases para diseñar, implementar y evaluar la Estrategia de Seguridad y privacidad de la Información.
- Contribuir a la disminución de incidentes y requerimientos relacionados con la seguridad de la información.
- Promover el uso de mejores prácticas de seguridad de la información en la institución.

3. ALCANCE

Este documento contempla la estructura de gobierno y los lineamientos principales para la seguridad y privacidad de la información en el Hospital la Merced. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus pacientes.

La estructura del Plan se basa en la metodología propuesta por MINTIC para el componente de Seguridad y Privacidad de la Información. El presente plan, aplican a todos los procesos soportados por el proceso de Apoyo Tecnológico del Hospital la Merced

4. MARCO CONCEPTUAL (DEFINICIONES RELEVANTES)

• **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a

La información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

• **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).

• **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

• **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

• **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

• **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

• **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

• **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

• **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

• **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

• **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

• **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

• **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

• **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

• **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

• **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

• **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

• **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la

orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

• **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

• **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

• **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

• **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

• **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 de 2014. (Ley 1712 de 2014, art 6)

• **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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

• **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

• **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

• **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

• **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

• **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

• **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

• **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

• **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

• **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

• **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. (ISO/IEC 27000).

• **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

• **Sistema de Gestión de Seguridad de la Información SGSI**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

• **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

• **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

• **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

• **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

• **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. MARCO LEGAL

La normatividad que sustenta el Plan de Seguridad y Privacidad de la Información es el siguiente:

- Constitución Política de Colombia.
- Ley 489 de 1998.
- Ley Estatutaria 1266 de 2008 ““Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales”
- Ley 1273 de 2009, "Protección de la Información y de los datos”
- Ley 1581 de 2012, "Protección de Datos personales".
- 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”
- Decreto 943 de 2014.
- Decreto Único Reglamentario 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones”

6. COMPROMISO DE LA DIRECCIÓN

La gerencia y administración de la ESE Hospital la Merced muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información a través de la asignación de recursos, la definición de la política de información, los lineamientos de seguridad y el establecimiento del comité de sistemas de información y comunicaciones cuya conformación y responsabilidades se describen a continuación.

7. COMITÉ DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

Creado bajo la Resolución N° 147 de agosto 15 de 2018, cuyas funciones son:

7.1 Funciones del Comité: El comité técnico de sistemas de información y comunicación tendrá las siguientes funciones:

- Definir las políticas de seguridad de información e implementar las estrategias pertinentes.

- Proteger, preservar y administrar objetivamente la información de la ESE 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 confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
- Definir las directrices de la ESE para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información
- Definir la elaboración, mantenimiento y actualización el procedimiento para la correcta definición, uso y complejidad de claves de usuario, definir el control de las contraseñas de red y uso de equipos.
- Garantizar la trazabilidad entre los diferentes procesos que usan los diferentes aplicativos.
- Garantizar que la adquisición, mantenimiento, y funcionamiento de los equipos de cómputo y similares, cuya principal función sea el procesamiento de información, cumpla con los parámetros necesarios para que los objetivos mencionados se cumplan.
- Garantizar el cumplimiento de las normas de propiedad intelectual en cuanto a la adquisición de software propietario o de terceros, regidos por los parámetros internacionales de la BSA y los que hubiere lugar en la legislación colombiana.
- Garantizar el uso eficiente del hardware y software con el que cuenta la institución.
- Definir los procedimientos y seguimiento a la actualización de los contenidos en redes sociales (facebook – twitter y youtube).
- Definir criterios de frecuencia de actualización de la información para todas las áreas.
- Definir cuáles son los contenidos deben mantener la privacidad.
- Definición de la política editorial y de actualización orientada a la implementación de las buenas prácticas para la publicación de contenidos en el Sitios Web y redes sociales de la E.S.E.
- Implementar un modelo de comunicación pública.
- Estandarizar los medios de comunicación de la E.S.E.

- Realizar los diagnósticos de percepción de los usuarios internos y externos frente a las comunicaciones.

7.2 Conformado por:

Subgerente administrativo.
Jefe de enfermería asistencial.
Funcionaria área de sistemas.
Auxiliar de gestión documental.
Funcionario de Comunicaciones.
Asesor de Calidad.
Gerente de Sistemas de Información en salud.

8. ADMINISTRADORES DE SEGURIDAD DE LA INFORMACIÓN

- Auxiliar de archivo clínico
- Auxiliar de gestión Documental
- Técnico de sistemas
- Gerente de sistemas de información

Objetivo	La responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores Específicas de seguridad.
Principios de operación	□ Reportar las actividades realizadas a la gerencia □ Desarrollar los planes de seguridad definido para cada área
Responsabilidades	□ Gestionar la seguridad de la información de aplicaciones, infraestructura, accesos. □ Identificar y ejecutar controles para los riesgos. □ Llevar registro de métricas, y evaluaciones de seguridad.

9. LINEAMIENTOS DE SEGURIDAD

9.1 Gestión de activos

Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada proceso, el cual debe estar alineado con el inventario general de activos de información.

En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

9.2 Uso aceptable de los activos

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad del HOSPITAL LA MERCED, son activos de la Institución y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos del negocio.

El HOSPITAL LA MERCED podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este plan y en cualquier proceso legal que se requiera.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y terceros determinadas por los Líderes de área y Subgerentes.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas del HOSPITAL LA MERCED se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable de aquellos.

El funcionario y/o contratista se compromete a cumplir con los procedimientos establecidos para el servicio y consulta de documentos según lo definido en el proceso de *Planificación y Consolidación del Sistema de Gestión Integral de Calidad y el área propietaria de la información*.

Para la consulta de información en XENCO se establecerán privilegios de acceso a los funcionarios, terceros y/contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el jefe de área, quien comunicará al encargado de la administración del software el listado con los funcionarios y sus privilegios.

El jefe de área, serán quien determinen el carácter de reserva o restricción de los documentos físicos. Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “Acuerdo de Confidencialidad de la Información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en la Política de Información del HOSPITAL LA MERCED y los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo a lo definido al tratamiento de este tipo de incidentes.

9.3 Acceso a Internet:
No está permitido:

El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y /o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

El acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Hospital.

El Intercambio no autorizado de información de propiedad del Hospital, de sus clientes, usuarios y/o de sus funcionarios, con terceros.

La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Líder respectivo o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

El HOSPITAL LA MERCED debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente.

Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

Los funcionarios, contratistas y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del Hospital, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del HOSPITAL LA MERCED.

9.4 Correo electrónico:

El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del Hospital.

Los mensajes y la información contenida en los buzones de correo son propiedad del HOSPITAL LA MERCED y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo es determinado por el área de Sistemas de la entidad de acuerdo con las necesidades de cada usuario y previa autorización del Jefe y/o Líder del área correspondiente.

El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de estos deberán ser definidos e implementados por el área de Sistemas del HOSPITAL LA MERCED.

El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el HOSPITAL LA MERCED proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.

El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del área de Comunicaciones y la autorización del área de Sistemas del Hospital. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre del área respectiva y/o servicio habilitado para tal fin y no a través de cuenta de correo electrónico asignadas a un usuario particular.

Toda información del HOSPITAL LA MERCED generada con los diferentes programas computacionales (Office, Project, Access, Wordpad, ect.), que requiera

Ser enviada fuera de la entidad, y que por sus características de confidencialidad eintegridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de Sistemas. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el HOSPITAL LA MERCED y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad.

Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.

El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto el Hospital no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.

El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.

No está permitido:

Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

Utilizar la dirección de correo electrónico del HOSPITAL LA MERCED como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y las áreas de Sistemas y Comunicaciones del HOSPITAL LA MERCED.

9.5 Recursos tecnológicos:

La instalación de cualquier tipo de software o hardware en los equipos de cómputo del HOSPITAL LA MERCED es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el HOSPITAL LA MERCED a través de esta área.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el área de Sistemas.

El área de Sistemas del HOSPITAL LA MERCED definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Hospital.

Los funcionarios serán conectados a la red del HOSPITAL LA MERCED con previa solicitud escrita y autorizada por el Líder del área. Los terceros y/o contratistas se conectarán a la red del HOSPITAL LA MERCED, bajo los lineamientos del área de Sistemas, asegurando la legalidad del equipo a través de certificados emitidos por la empresa contratista, de acuerdo a lo definido por el área de sistemas.

Los usuarios que requieren acceder a la infraestructura tecnológica del HOSPITAL LA MERCED desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas. Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo a lo definido por el área de sistemas.

La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe ser

Autorizado de forma explícita por el líder de la dependencia respectiva, en conjunto con el apoyo del área de Sistemas del HOSPITAL LA MERCED.

Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar o grabar música.

Ningún funcionario contratista o tercero podrá copiar para uso personal archivos o programas de propios del Hospital.

9.6 Acuerdos sobre confidencialidad

Todos los funcionarios, colaboradores y/o terceros que presten sus servicios al HOSPITAL LA MERCED deberán aceptar los acuerdos de confidencialidad definidos por la institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del HOSPITAL LA MERCED a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

9.7 Partes externas

El HOSPITAL LA MERCED identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

9.8 Clasificación de la información

El HOSPITAL LA MERCED con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o clientes, ha establecido niveles para la

Clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

Los propietarios de los activos de información son los responsables de identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación, y su protección se establece de acuerdo con lo definido en el inventario de activos de información del HOSPITAL LA MERCED.

9.9 Seguridad de los recursos humanos

Todos los funcionarios del HOSPITAL LA MERCED, contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información del HOSPITAL LA MERCED. De igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

Todos los funcionarios del HOSPITAL LA MERCED deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

Todos los funcionarios del HOSPITAL LA MERCED deben hacer buen uso de la escarapela que los acredita como sus servidores, este documento debe ser devuelto al HOSPITAL LA MERCED en el momento de desvinculación.

9.10 Devolución de Activos.

Todo funcionario al momento de su retiro o cambio de funciones en la institución debe hacer entrega a su jefe inmediato del equipo que se le había asignado, con toda la información contenida en él y una relación de la misma.

9.11 Protección y ubicación de los equipos

Los equipos que hacen parte de la Infraestructura tecnológica del HOSPITAL LA MERCED tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de

Los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica del HOSPITAL LA MERCED no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

Cualquier traslado de equipos de cómputo se realizará con la coordinación del área de Sistemas y del almacén previa verificación de las condiciones técnicas y de seguridad.

Toda persona que note algún problema de funcionamiento o ataque de virus en una estación de trabajo debe reportarlo de inmediato al personal de sistemas

El HOSPITAL LA MERCED debe proveer suministros y equipamiento de soporte como electricidad, aire acondicionado, planta eléctrica y un sistema de alimentación no interrumpida (UPS) que asegure el tiempo necesario para apagar adecuadamente los servidores donde se alojan los sistemas de información ante una falla en el suministro de cualquiera de estos elementos, evitando así la pérdida o corrupción de información. Estos suministros deben ser monitoreados, revisados y medidos permanentemente para asegurar su funcionamiento y condiciones normales de operación y evitar futuros daños.

De igual manera, el HOSPITAL LA MERCED debe establecer un programa de planeación y ejecución de mantenimientos preventivos anuales (como mínimo), a la infraestructura tecnológica.

Ningún empelado, contratista o tercero podrá desarmar o destapar equipos sin la autorización previa del Departamento de Sistemas.

9.11 Seguridad de los equipos y medios de información fuera de las instalaciones

Independientemente del propietario, todos los funcionarios son responsables de velar por la seguridad de los equipos del HOSPITAL LA MERCED que se encuentren fuera de las instalaciones de la organización.

En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

Los equipos de infraestructura del HOSPITAL LA MERCED deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

Los equipos del HOSPITAL LA MERCED deberán contar con un seguro que los proteja de robo.

En caso de pérdida o robo de un equipo del HOSPITAL LA MERCED, se deberá informar inmediatamente al jefe de área, almacén y administración para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de HOSPITAL LA MERCED, fuera de las instalaciones de la organización debe seguir los procedimientos establecidos por la Subgerencia Administrativa y el área de Sistemas del HOSPITAL LA MERCED.