PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

E.S.E. HOSPITAL MENTAL UNIVERSITARIO DE RISARALDA

BEATRIZ ELENA VILLEGAS MONTOYA
GERENTE

JHON JAIRO NARANJO RAMÍREZ

2024

INTRODUCCIÓN

La Gerencia del Hospital Mental Universitario de Risaralda - HOMERIS entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Contenido

1 INTRODUCCIÓN 5

2 DEFINICIONES 5

3 OBJETIVO 6

4 ALCANCE DE LA POLÍTICA 6

5 PRINCIPIOS DE LA POLÍTICA 7

6 ELEMENTOS DE LA POLÍTICA 8

6.1 ASPECTOS GENERALES 8

6.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. 10

6.2.1 Recurso Humano 10

6.2.2 En relación a los servicios informáticos. 10

6.2.3 En relación con los recursos informáticos. 12

6.2.4 En relación con usuarios terceros. 13

6.2.5 Lugares Físicos 14

6.2.6 En relación con la seguridad física del edificio. 15

6.2.7 Seguridad De La Red 16

6.2.8 Seguridad de la Información. 18

6.2.9 Política de actualización de hardware. 20

6.2.10 Políticas de seguridad en comunicaciones. 21

6.3 POLÍTICA DE ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN 22

6.3.1 Acceso al servicio de Internet y cuentas de correo electrónico. 24

6.3.2 Gestión de accesos y contraseñas 26

6.3.3 Almacenamiento de Contraseñas 28

6.4 POLÍTICA DE USO DE LAS FACILIDADES DE TI POR PARTES DE LOS USUARIOS 28

6.4.1 Políticas para la estrategia de Uso y Apropiación del portafolio de servicios de TI 28

6.4.2 Políticas de Gestión del Cambio para el Uso y Apropiación del portafolio de servicios de TI 29

6.4.3 Políticas de medición de Resultados del uso y Apropiación del portafolio de servicios de TI 29

7 SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA 30

8 CRONOGRAMA ACTIVIDADES 32

9 CONSIDERACIONES FINALES 36

10 DOCUMENTOS RELACIONADOS 36

1 INTRODUCCIÓN

Actualmente la seguridad de la información ha tomado gran importancia, debido al gran desarrollo y auge de nuevas tecnologías, nuevas plataformas de computación, nuevas aplicaciones, nuevos dispositivos de hardware e interconexión a través de redes, pero al mismo tiempo surgen nuevas amenazas para los sistemas de información.

Se hace necesario desarrollar documentos con reglamentos y recomendaciones que orienten a todo el personal de la entidad en el uso adecuado de los sistemas de información, con el fin de obtener el mayor provecho de la tecnología disponible y prevenir serios problemas como resultado de su uso inadecuado en los bienes y servicios prestados por ella.

En este sentido, las políticas de Seguridad de la Información se convierten en una herramienta para el uso adecuado de los recursos informáticos del Hospital HOMERIS, donde se desarrollan funciones y procedimientos de seguridad para concientizar a cada uno de los colaboradores de la organización en el uso adecuado de los recursos informáticos, permitiendo de esta manera obtener un mejor rendimiento y protección de los diversos sistemas de información y sus recursos.

2 DEFINICIONES

- **Política:** Instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

- Procedimiento: Documento que contiene las fases secuenciales donde se describe detalladamente cómo se lleva a cabo una actividad determinada.

- Recurso Informático: Elementos informáticos (base de datos, sistemas operaciones, redes, sistemas de información y comunicaciones, equipos computacionales) que facilitan servicios informáticos.

- Seguridad de la información: Medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- Sistema de información: Conjunto de elementos orientados al tratamiento y entidad de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. Los elementos pueden ser personas, datos, actividades o técnicas de trabajo y Recursos materiales en general (generalmente recursos informáticos).

- Usuario: Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que utilicen recursos informáticos para desarrollar sus funciones y actividades asignadas.

3 OBJETIVO

Definir parámetros de control para mantener y procurar la seguridad de la información del Hospital HOMERIS en relación con los sistemas de información, utilización de los equipos de cómputo y el uso adecuado de la red, el servicio de internet y correo electrónico.

4 ALCANCE DE LA POLÍTICA

Las políticas definidas en el presente documento aplican a todos los colaboradores del Hospital Mental Universitario de Risaralda – HOMERIS, contratistas, pasantes universitarios, aprendices SENA y otras personas relacionadas a terceras partes, que utilicen recursos informáticos de la administración.

5 PRINCIPIOS DE LA POLÍTICA

Los principios definidos para la política de seguridad de la información del Hospital HOMERIS son los siguientes:

- **Responsabilidad:** Todos los usuarios, sin excepción, son responsables por los accesos, acciones y demás situaciones que se realicen en los diferentes sistemas de información donde se implique el uso de código de usuario y contraseña, así como en el uso de las cuentas de correo electrónico corporativo.

- **Cumplimiento:** Es deber de los usuarios acatar las normas, procedimientos administrativos y técnicos establecidos por la entidad para el uso de los sistemas de información, así como la aplicación de las instrucciones para la protección de la información.

- **Ética:** Se debe mostrar y aplicar una buena conducta en la utilización de los sistemas de información, los cuales han sido destinados únicamente para los servicios prestados por la administración, respetando la propiedad intelectual del software, diseños e información, como también el adecuado uso de la información contenida en ellos.

- **Propiedad:** La entidad es la propietaria de todos los recursos informáticos instalados y entregados a los usuarios para su utilización, entre los que se destacan los siguientes: computadores de escritorio y/o portátiles, dispositivos móviles (celular Smartphone, Tablet, palm, entre otros), correo electrónico y la información resultante en los servicios prestados sobre ellos.

- Vigilancia: La entidad se reserva el derecho de vigilar el uso de los recursos informáticos y acceder a la información contenida en los mismos de ser necesario, procurando la no violación de las normas y principios establecidos por la organización, en especial la información que no tenga relación con las funciones inherentes al cargo del usuario o aquella que no esté debidamente autorizada para su acceso, la cual podrá ser retenida por la entidad en caso de ser hallada durante una revisión.

6 ELEMENTOS DE LA POLÍTICA

La política de seguridad de la información al interior del Hospital Mental Universitario de Risaralda - HOMERIS consta de:

6.1 ASPECTOS GENERALES

La filosofía de la política establece que los usuarios de la entidad deben cumplir con los siguientes aspectos:

a) Usar los recursos informáticos únicamente para los servicios prestados por la administración.

b) Acceder bajo su responsabilidad solo a sus datos, programas y demás recursos asignados necesarios para realizar sus funciones y brindar el servicio designado.

c) Usar solo el software autorizado y asignado por la administración.

d) Respetar las leyes de derecho de autor contempladas en la Ley 23 de 1982, Ley 44 de 1993 y ley 603 de 2000; por lo tanto, no se permite instalar en los computadores de la administración programas no

licenciados ni autorizados por el proceso de gestión de Tecnologías de la Información.

e) No instalar programas de cómputo por cuenta propia.

f) No usar los recursos informáticos para su propio beneficio o de terceros.

g) Proteger su código de usuario y su contraseña. No prestarlos ni divulgarlos.

h) Mantener la confidencialidad y reserva de la información a su cargo, no divulgando ésta a personas extrañas a la administración.

i) No monopolizar la red ni los computadores de la entidad con datos innecesarios, como fotos, videos, música y demás programas de entretenimiento o ajenos a la misma.

j) Respetar y cumplir a cabalidad con las medidas de seguridad de los sistemas de información, recursos informáticos y red corporativa de la administración, obligando a mantener protegida la información y recursos asignados.

k) Hacer buen uso de la red corporativa y de sus recursos, como las impresoras, el papel, los medios de almacenamiento y seguridad, los canales de comunicación, entre otros.

l) No compartir o difundir en la red información sensible que pueda atentar contra la seguridad de la información de la administración, como infecciones por virus informáticos y demás programas que intenten violar la seguridad de la misma.

m) No trasladar los computadores y sus componentes asignados a sitios diferentes a los autorizados.

6.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

6.2.1 Recurso Humano

La entidad considera a las personas como elemento clave de los procesos de gestión de información y como usuarios de tecnología. Se pueden identificar los siguientes tipos de usuario:

1. **Colaboradores directos e indirectos**, que participan en la ejecución de los servicios en la administración.

2. **Clientes y proveedores**, autorizados para el acceso a los recursos de tecnología de la organización.

3. **Demás terceros**, autorizados por la administración, para acceder a la información y demás recursos informáticos.

6.2.2 En relación a los servicios informáticos.

Se considera como falta SIMPLE el incumplimiento de las siguientes consideraciones:

a) Los usuarios deberán velar por el adecuado uso de las impresoras, donde se realicen impresiones sólo de información realmente necesaria para el desempeño de sus servicios asignados, y lograr el eficiente uso de los recursos: tinta, papel, etc., contribuyendo de esta manera con la conservación del ambiente.

b) Los funcionarios solo podrán imprimir los trabajos asociados para el cumplimiento de los servicios asignados.

Se considera como falta MEDIA el incumplimiento de las siguientes consideraciones:

a) El sistema de correo electrónico, herramientas de chat y demás utilidades asociadas, deben ser usadas según los lineamientos adoptados por la organización para el uso de cada una de ellas y únicamente para el ejercicio de las funciones delegadas a cada colaborador y servicios contratados a terceros.

b) Se prohíbe el uso de cualquier programa chat que no sea el institucional. En caso de requerir un programa diferente para estar en contacto directo con clientes y proveedores, se debe enviar por escrito al Proceso de Gestión de Tecnologías de la Información, por intermedio del jefe encargado de área del usuario solicitante, justificando la razón por la cual es necesaria la instalación del mismo para su análisis y aprobación.

c) Los usuarios no deben utilizar el servicio de chat para fines tales como realización de encuestas, concursos, o cualquier otro tipo de mensajes no solicitados (Comerciales o de otro tipo); solamente se debe utilizar para fines pertinentes a la labor en la administración.

d) Para hacer uso de la herramienta chat institucional, se debe gestionar el acceso directamente con el proceso de gestión de Tecnologías de la Información, por intermedio del Jefe del área del usuario solicitante.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Los usuarios autorizados para acceder a Internet, deberán aceptar, respetar y aplicar las políticas y prácticas del uso adecuado de este servicio en sus labores desarrolladas al interior de la administración.

b) Si los usuarios sospechan de alguna infección causada por un virus informático, deben comunicarlo inmediatamente al proceso de gestión de Tecnologías de la Información para tomar las acciones pertinentes.

c) Los usuarios deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En caso de personas ajenas a la entidad, encargados de área son los responsables de autorizar el acceso a los recursos informáticos de la organización, de acuerdo al trabajo que estas personas realizarán y con previa justificación al proceso de gestión de Tecnologías de la Información.

6.2.3 En relación con los recursos informáticos.

El uso de los recursos informáticos deberá estar regulado por:

- Administración de usuarios: Establece como deben ser utilizadas las claves de acceso a los recursos informáticos, los parámetros de longitud mínima de la contraseña, la frecuencia de cambio de contraseña por parte de los usuarios, entre otras.

- Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con los roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y contraseñas únicos para cada usuario.

b) Todo sistema de información debe tener definidos los perfiles de usuario de acuerdo con los servicios a su cargo y de los usuarios que acceden a ellos.

c) Las contraseñas de acceso a los recursos informáticos que se asignen a los usuarios son su responsabilidad exclusiva y éstas no deben ser divulgadas a ninguna persona.

d) El usuario debe cambiar la contraseña regularmente, mediante los mecanismos dispuestos para tal fin.

e) Los usuarios son responsables de todas las actividades realizadas en los sistemas de información al cual tengan acceso y donde se lleve registro de uso de código de identificación de usuario y clave personal.

6.2.4 En relación con usuarios terceros.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Los dueños de los recursos informáticos que no sean propiedad del Hospital HOMERIS y deban ser ubicados y administrados por ésta, deben garantizar la legalidad en hardware y software del recurso para su funcionamiento dentro de la organización.

b) Cuando se requiera utilizar recursos informáticos que no sean propios del Hospital HOMERIS y deban ubicarse en sus instalaciones, estos serán administrados por el proceso de gestión de Tecnologías de la Información.

c) Los usuarios terceros tendrán acceso limitado y supervisado a los recursos informáticos necesarios para el cumplimiento de su función dentro de la administración. La autorización para acceder a esos servicios debe ser aprobadas por el jefe encargado de área y por el jefe del área del proceso de gestión de Tecnologías de la Información.

d) Los equipos de usuarios terceros que deban tener acceso a la red interna deben cumplir con todas las normas de seguridad de la información vigentes establecidas por la entidad. Adicional a ello debe diligenciarse el acta respectiva donde queda plasmada la información del equipo de cómputo con sus respectivas autorizaciones.

e) La conexión entre los sistemas de información internos de la entidad y terceros debe ser aprobada y certificada por el proceso de gestión de Tecnologías de la Información, con el fin de no comprometer la seguridad de la información de la administración.

f) Como requisito para interconectar las redes de la entidad con terceros, sus sistemas de comunicación deben cumplir con los requisitos establecidos por la entidad. La institución se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. Así como se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la organización.

6.2.5 Lugares Físicos

Los lugares físicos incluyen:

Instalaciones: edificios, salones, oficinas y las salas de centro de cómputo.

- Sistemas de control de acceso físico a los diferentes lugares de la administración.

- Sistemas de detección de fuego, agua, humedad y temperatura, instalados como mecanismos preventivos.
- Centros de almacenamiento de información, magnética e impresa, que la entidad ha dispuesto para tal fin.
- Toda la estructura física de equipos de procesamiento, como computadores, UPS, impresoras, equipos de comunicación, entre otros.

6.2.6 En relación con la seguridad física del edificio.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) La organización deberá contar con mecanismos de control de acceso, tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistemas de alarmas, entre otros. Además, se debe contar con un circuito cerrado de televisión en las dependencias que la entidad considere críticas (por ejemplo, el Data Center).

b) Las áreas consideradas críticas por la administración, deben ser lugares de acceso restringido. Si una persona no autorizada requiere ingresar a ellos, deberá registrar el motivo del ingreso y estar acompañada permanentemente por un usuario con acceso autorizado para estar en esa área específica.

c) Las áreas consideradas críticas por la administración, deberán contar con elementos de control de incendio, inundación, humedad y temperatura.

d) Las áreas consideradas críticas por la administración, deberán estar demarcadas con zonas de circulación definidas para visitantes y delimitar las zonas con acceso restringido.

e) Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con acceso restringido a personal no autorizado.

f) Cuando un usuario detecte un visitante sin compañía de un funcionario y sea sorprendido en alguna área restringida de la administración, debe ser cuestionado inmediatamente, solicitando las razones por las cuales se encontraba en un área restringida e informar de inmediato al jefe o encargado del área donde ocurra el incidente.

6.2.7 Seguridad De La Red

6.2.7.1 Usos de la red

El usuario se compromete a aceptar las condiciones estipuladas por la entidad en las que se señala el uso de los servicios con fines netamente laborales, excluyendo cualquier uso comercial de la red, así como prácticas desleales (hacking) o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información.

En particular quedan expresamente prohibidas las siguientes acciones, de manera tal que su incumplimiento es considerado como falta GRAVE:

a) Tratar de causar daño a sistemas de información o equipos conectados a la red corporativa de la entidad y a otras redes a las que se proporcione acceso.

b) Esparcir "virus", "gusanos", “troyanos” u otros tipos de programas dañinos para sistemas de proceso de la información.

c) Utilizar los medios de la red corporativa con fines propagandísticos o comerciales no concernientes a los procesos de la entidad.

d) Congestionar intencionalmente o no, enlaces de comunicaciones o sistemas de información mediante el envío o recepción de información o programas concebidos para tal fin.

e) Congestionar enlaces de comunicaciones o sistemas de información mediante la transferencia o ejecución de archivos o programas no propios del ambiente laboral.

f) El usuario no puede realizar acciones donde se disminuya el desempeño de los sistemas de información o interfieran con los procesos del sistema propio o de cualquier otro sistema de información.

g) El usuario no puede realizar acciones tendientes a burlar la seguridad del sistema de información, ni usar su cuenta para intentar burlar la seguridad de otros sistemas de información.

h) El usuario no puede intentar cambiar la configuración de los programas ni alterar archivos o información del sistema de información.

i) Los archivos, dispositivos y programas tienen privilegios de acceso asignados por el administrador del sistema. Por tanto, el usuario no puede intentar leer, escribir, copiar o alterar de cualquier manera información que no ha sido autorizada dentro de sus funciones.

j) Intentar o realizar accesos a cuentas de usuario diferentes a la asignada (utilizando cualquier protocolo: telnet, ftp etc.), aunque no se consiga ingresar al sistema de información.

k) Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de otros usuarios.

l) Afectar o paralizar algún servicio ofrecido por el proceso de gestión de Tecnologías de la Información.

m) Modificar archivos que no sean propiedad del usuario, aunque cuente con los permisos de escritura.

n) Acceder, analizar o exportar archivos que sean accesibles a todo el mundo, pero sin ser propiedad del usuario, salvo que se encuentren en una localización destinada para uso público.

o) Se prohíbe el uso de dispositivos USB (memorias, discos duros externos, discos ópticos externos y similares) que no estén asociados a las labores realizadas por el usuario al interior de la empresa. De ser necesario su uso, del jefe o el encargado del área correspondiente deberá hacer la solicitud por escrito ante el proceso de gestión de Tecnologías de la Información, donde se justifiquen las razones para su utilización. Una vez se considere viable la solicitud, la dirección del área solicitante es la responsable de las acciones resultantes del mal uso dado a estos dispositivos.

6.2.8 Seguridad de la Información.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Los usuarios son responsables de la información a su cargo y deberán cumplir los lineamientos generales y especiales regulados por la entidad

para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida da la misma.

b) Todo usuario que utilice los recursos informáticos tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información a su cargo, en especial si dicha información está protegida por reserva legal o ha sido clasificada como crítica.

c) Los usuarios deberán firmar un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad y buen manejo de la información.

d) Cuando un trabajador deja de prestar sus servicios a la entidad, se compromete a entregar toda la información correspondiente a los servicios designados. Una vez retirado, el usuario debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la administración, directamente o a través de terceros; así mismo, los usuarios que detecten el mal uso de la información, están en la obligación de reportar el hecho ante el jefe de área correspondiente.

e) Cuando un funcionario vaya iniciar sus vacaciones, el área de talento humano debe informar al proceso de gestión de Tecnologías de la Información el inicio y terminación de éstas, periodo en el cual se restringirá el acceso a los recursos informáticos asignados a su código y clave de usuario.

f) En caso de suplencia en algún cargo por motivo de vacaciones de un funcionario, se notificará al proceso de gestión de Tecnologías de la Información del reemplazo para proceder a activar el respectivo encargo en los sistemas de información y accesos a los recursos informáticos que le serán asignados. Bajo ninguna circunstancia un código puede ser

usado por otro funcionario distinto; los privilegios de acceso serán limitados para las personas que realizan un reemplazo.

g) Como regla general, la información de políticas, normas y procedimientos de seguridad de la información se deben revelar únicamente a usuarios y entes externos que lo requieran, de acuerdo con su competencia y servicios a prestar, según se requiera.

6.2.9 Política de actualización de hardware.

Se considera como falta MEDIA el incumplimiento de las siguientes consideraciones:

a) En caso de necesitarse un nuevo dispositivo, éste debe gestionarse, sin excepción alguna, ante el proceso de gestión de Tecnologías de la Información.

b) Cualquier cambio para mejorar el rendimiento en alguno de los equipos de cómputo del Hospital HOMERIS (procesador, adición de memoria RAM o tarjeta), debe tener previamente una evaluación técnica y autorización del proceso de gestión de Tecnologías de la Información.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) La reparación técnica de algún equipo de cómputo donde se implique su apertura, únicamente puede ser realizada por personal autorizado.

b) Los recursos tecnológicos no deben ser movidos o reubicados sin la aprobación previa del jefe del área involucrada, en acuerdo con el proceso de Tecnologías de la Información.

6.2.10 Políticas de seguridad en comunicaciones.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Las direcciones internas (IP), topologías, configuraciones e información relacionadas con el diseño, la arquitectura y seguridad de la organización, deberán ser consideradas y tratadas como información confidencial.

b) Todas las conexiones a redes externas de tiempo real con acceso a la red interna de la administración, debe pasar a través de los sistemas firewall, administración de permisos de circulación y autenticación de usuarios.

c) Todo intercambio electrónico de información o interacción entre sistemas de información con el Hospital HOMERIS externas, deberá estar soportado con un acuerdo o documentos de formalización, y preferentemente este intercambio generarlo con información cifrada.

d) Los equipos de la organización que requieran conexión de manera directa con computadores del Hospital HOMERIS externas, lo realizaran con previa autorización y supervisión o ejecución del proceso de gestión de Tecnologías de la Información.

e) El acceso remoto a los recursos informáticos de la entidad estará restringido SÓLO para personal autorizado. Cualquier intento de acceder o violar la seguridad de los recursos informáticos, como el uso e instalación de herramientas para este fin, será catalogado como una falta GRAVE.

Nota aclaratoria: Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la entidad e Internet deberá estar cifrada.

6.3 POLÍTICA DE ACCESO A LAS TECNOLOGÍAS DE LA INFORMACIÓN

Para el Hospital Mental Universitario de Risaralda - HOMERIS, construir una política de acceso a las TI, propicia un ambiente donde la inversión está directamente ligada a la puesta en funcionamiento de su infraestructura tecnológica permitiendo conectar eficientemente las necesidades priorizadas con las capacidades organizacionales y los retos consignados en los planes de desarrollo a los cuales se encuentra alineada la entidad.

En el presente capítulo se detalla la política de acceso a las tecnológicas de la información, mediante la cual los grupos de interés caracterizados por la administración tienen acceso a los servicios que se han implementado utilizando mecanismos de transformación basados en el uso adecuado de las TIC, como soporte a todos y cada uno de los proyectos que conforman el Portafolio de Servicios del proceso de gestión de Tecnologías de la Información.

Igualmente, es necesario establecer el uso y acceso de las Tecnologías de la Información y Comunicaciones dispuestas en el Hospital HOMERIS para los grupos de interés caracterizados en el Plan Estratégico, de desarrollo para Determinar las directrices y capacidades de la Empresa para el uso adecuado del acceso a las tecnologías de la información representadas en los servicios tecnológicos prestados por el proceso de gestión de TI.

La presente política de acceso a las TI, velará por el adecuado cumplimiento de los fundamentos a saber:

a) Acceso a las TI del usuario interno: Desarrollo y mantenimiento de infraestructura interna, bajo adecuados estándares de calidad para ofrecer los servicios detallados en el portafolio de servicios de lal Proceso de Gestión de TI; para la sostenibilidad de dicha infraestructura, el proceso de gestión de TI deberá adoptar mecanismos de calidad para contextualizar las iniciativas de regulación para mejorar la prestación de los servicios de TI en la administración.

b) Educación Y Entrenamiento en accesos: Periódicamente habrán espacios de formación continúa para romper la brecha de resistencia al cambio frente a la utilización de todos los servicios de TI de la administración, conforme a lo establecido en la política de Gobierno Digital del Estado colombiano.

I. Usuario externo

4. Acceso a las TI del usuario externo caracterizado por la Empresa: la infraestructura de la Empresa, deberá ser lo suficientemente sólida para garantizar a los usuarios externos lo siguiente: Acceso Y Servicio Universal1, Acceso Universal 2, Servicio Universal3

De este modo, los fundamentos enmarcados deberán estar caracterizados por:

a) Disponibilidad: Disponibilidad del servicio en el área de influencia de la administración. Accesibilidad: Todos los usuarios caracterizados en los grupos de interés del Plan estratégico del Hospital HOMERIS, pueden utilizar los servicios ciudadanos digitales, al margen del lugar donde residan, su género, discapacidades u otras características.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Todos los usuarios deben tener acceso sólo a la información necesaria para el desarrollo los procesos asignados

b) En el caso de personas ajenas a la administración, los secretarios o encargados de área son los responsables de autorizar sólo el acceso

indispensable de acuerdo con el trabajo realizado por estas personas, con previa justificación.

c) Para dar acceso a la información se tendrán en cuenta la clasificación de ésta al interior de la administración, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la organización.

d) El otorgamiento de acceso a la información está regulado mediante las normas/reglas y procedimientos definidos para tal fin.

e) Todos los privilegios para el uso de los sistemas de información de la entidad deben terminar inmediatamente después del cese de actividades del trabajador en la organización. Proveedores o terceras personas solamente deben tenerlos durante el periodo del tiempo requerido para llevar a cabo las labores asignadas.

f) Mediante el registro de eventos de los diversos recursos informáticos integrados en la plataforma tecnológica, se hará disponible la ejecución de un seguimiento de los accesos realizados por los usuarios a los sistemas de información de la organización, con el objeto de minimizar el riesgo de pérdida de integridad de la información.

g) Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

6.3.1 Acceso al servicio de Internet y cuentas de correo electrónico.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a) Para hacer uso de este tipo de herramientas se debe gestionar el acceso directamente con el Proceso de Gestión de Tecnologías de la Información por escrito y por intermedio de la dirección del área del usuario solicitante.

b) El servicio de Internet y correo electrónico estará disponible únicamente para propósitos institucionales y corporativos concernientes a la administración.

c) Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro diferente al laboral que dio origen a la habilitación del servicio.

d) Está prohibido transmitir cualquier material que viole cualquier regulación de la entidad y en general de la República de Colombia; esto incluye: derechos de autor, amenazas, mensajes ofensivos, mensajes en cadena, mensajes intencionales que no contengan información o que contengan basura informática, material obsceno o información protegida por secreto comercial.

e) El usuario de Internet o cuenta de correo no tiene permitido acceder o intentar acceder a la cuenta o a los datos de otros usuarios.

f) El usuario de Internet o cuenta de correo no tiene permitido autorizar a otras personas a utilizar su cuenta.

g) Cualquier evidencia de acceso no autorizado a la cuenta o a los datos tiene que ser informada inmediatamente al Proceso de Gestión de Tecnologías de la Información.

6.3.2 Gestión de accesos y contraseñas

6.3.2.1 5.3.2.1 Gestión de Accesos

Remítase a la Directiva de Gestión de Accesos

6.3.2.2 5.3.2.2 Gestión de Contraseñas

Para las directivas de contraseñas configuradas mediante la administración de directivas de grupo a través del controlador de dominio, se definen los siguientes parámetros:

Exigir historial de contraseñas. El hospital Homeris actualmente cuenta con las siguientes contraseñas:

- Equipos de cómputo 97
- Software Dinámica Gerencial.net
- SIFAS
- DGH Versión anterior
- Plataforma SISAP (Saludito)
- Plataforma Ministerio de salud
- Plataforma Supersalud
- Plataforma Ministerio de hacienda
- Plataforma Mi seguridad social
- Plataforma EPS (Rips)
- MIPRES
- Acceso a servidores
- NAS (5)
- Ventanilla única
- Gestión documental
- Correo electrónico
- SPARK
- Call center

Esta configuración de seguridad determina el número de nuevas contraseñas únicas que deben asociarse a una cuenta de usuario antes de poder reutilizar una contraseña antigua.

La contraseña debe cumplir con los requisitos de complejidad (habilitada)

Con la habilitación de esta directiva, las contraseñas deben cumplir los siguientes requisitos mínimos:

- ✓ No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- ✓ Tener una longitud mínima de 8 caracteres
- ✓ Incluir caracteres de tres de las siguientes categorías:
- ✓ Mayúsculas (de la A a la Z)
- ✓ Minúsculas (de la A a la z)
- ✓ Dígitos de base 10 (del 0 al 9)
- ✓ Caracteres no alfanuméricos (por ejemplo, !, $, #, %)
- ✓ Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.

- Longitud mínima de la contraseña 8 caracteres

Esta configuración de seguridad determina el número mínimo de caracteres que debe contener la contraseña de un usuario.

- Vigencia máxima de la contraseña 60 días

Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el sistema solicite al usuario que la cambie.

- Vigencia mínima de la contraseña 1 día

Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el usuario pueda cambiarla.

6.3.3 Almacenamiento de Contraseñas

Todas las contraseñas de los sistemas operativos de servidores, servicios de TI, bases de datos y dispositivos de red deberán ser cambiadas en periodos de tres meses a excepción de la contraseña de administrador de dominio la cual cambia con las políticas anteriormente descritas.

El compilado de todas las contraseñas debe ser impreso en dos copias originales. Una copia deberá ser enviada al jefe para su respectiva custodia y la otra copia deberá ser guardada en la caja de seguridad destinada para tal fin.

6.4 POLÍTICA DE USO DE LAS FACILIDADES DE TI POR PARTES DE LOS USUARIOS

En el Hospital HOMERIS, el uso institucional de los activos de información se está multiplicando en la medida que los usuarios ven la necesidad de hacer uso de los servicios tecnológicos como medio de avance progresivo de comunicar efectivamente. En este sentido, Involucrar los grupos de interés del Hospital, en las iniciativas de TI y el desarrollo de competencias TI, impulsa las estrategias de la entidad con el propósito de establecer normas que aseguren el buen funcionamiento de los servicios de TI.

6.4.1 Políticas para la estrategia de Uso y Apropiación del portafolio de servicios de TI

a) Divulgación, seguimiento, evaluación y control del plan de involucramiento, el plan de gestión del cambio y el plan de monitoreo.

b) Actualización, Identificación, Clasificación y Priorización de todos los grupos de interés que participan en el actuar de la administración que hacen uso de los servicios de TI.

c) Desarrollar efectivamente acciones que permitan una motivación hacia la adopción u correcta utilización del Portafolio de servicios de TI del Proceso de Gestión TI del Hospital HOMERIS.

d) Fortalecer las competencias generales y específicas de TI en los colaboradores de la administración.

6.4.2 Políticas de Gestión del Cambio para el Uso y Apropiación del portafolio de servicios de TI

a) Implementar el Plan de Gestión del Cambio (Definición de prácticas, Procedimientos, Asignación de recursos, Herramientas); así mismo realizar la debida evaluación, el seguimiento y control del plan.

b) Facilitar a los grupos de interés del Hospital HOMERIS, la adopción del portafolio de servicios de TI, teniendo como base el diseño y monitoreo de indicadores de cambio, planteados en el Plan de Gestión del Cambio.

c) Consolidar, evaluar y hacer seguimiento al plan de gestión de Impactos para identificar los cambios asociados a cada grupo de interés identificados en el Plan Estratégico del Hospital HOMERIS.

6.4.3 Políticas de medición de Resultados del uso y Apropiación del portafolio de servicios de TI

a) Se debe garantizar la sostenibilidad de Impactos, asegurando con ello la continuidad de la transformación hasta formar parte de la cultura organizacional de la administración.

b) Realizar constantes acciones de mejora basadas en análisis de resultados de la aplicación de los siguientes indicadores de Uso y Apropiación:

- Nivel de conocimiento
- Nivel de utilidad percibida

- Nivel de competencias en TI
- Nivel de cumplimento de actividades de Formación y Desarrollo
- Nivel de cumplimiento de las actividades de cambio
- Estabilidad de las iniciativas de TI
- Impacto en los atributos de la cultura organizacional

7 SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA

a) En caso de infracción debidamente comprobada de alguna de las normas anteriores o de cualquier abuso efectuado por el usuario de los recursos informáticos de la administración, el jefe o encargado del Proceso de Gestión de Tecnologías de la Información puede tomar acciones que van, desde una simple advertencia hasta la restricción completa del uso de los servicios computacionales y de red de la entidad hasta no efectuar proceso de descargos con el área del usuario infractor. Todo este proceso será informado directamente a la dirección de área del usuario infractor.

b) Cuando se trate de una falta que afecte directamente el normal funcionamiento del recurso tecnológico o infrinja leyes del ámbito jurídico, se aplicarán también todas las normas vigentes en el contrato de trabajo del Hospital HOMERIS, conforme a las normas del Régimen Laboral, y de la legislación colombiana e internacional. En estos casos, la aplicación de sanciones se delega a la dirección de área del usuario implicado.

c) Cuando por consecuencia de una violación de las normas se suspendan privilegios de los servicios computacionales a un usuario, para reactivar los servicios la dirección de área del usuario infractor debe solicitar por escrito el levantamiento de la restricción ante el Proceso de Gestión de Tecnologías de la Información.

d) La reincidencia de una falta SIMPLE la convierte en GRAVE.

8 CRONOGRAMA ACTIVIDADES

ACTIVIDADES REALIZADAS PERIODO 2023			
FASE MSPI	ACTIVIDADES	META	PRODUCTO
Diagnóstico	Se llevo a cabo el diagnóstico del modelo seguridad privacidad de la Información de la ESE Hospital Mental Universitario de Risaralda	Establecer las fortalezas y debilidades que tiene la entidad en cuanto a la seguridad y privacidad de la información	Diagnóstico del modelo de seguridad y privacidad de la información
	Se Definieron los Roles y responsabilidades de seguridad y privacidad de la información.	Lograr establecer los roles y responsabilidades en seguridad y privacidad de la información que incluyan los temas de seguridad de la información en la entidad.	Roles y responsabilidades de seguridad y privacidad de la información.
	Se elaboró la matriz de activos de información	Documento con la metodología para identificación, clasificación y valoración de activos de información.	Matriz de Inventario de activos de información.

Diagnóstico, planeación e implementación	Transición e implementación protocolo IPv4_IPv6	Se llevo a cabo la fase de transición del protocolo IPv4 a IPv6	Protocolo IPv4 a IPv6 implementado, y contrato del pool de direcciones IPv6 vigente.

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
FASE MSPI	**ACTIVIDADES**	**META**	**PRODUCTO**	**RESPONSABLE(S)**	**FECHA**
Planificación	Realizar Cronograma de actividades de las fases del modelo de seguridad y privacidad de la información MSPI	Establecer el cronograma de actividades correspondiente a la implementación del modelo de seguridad y privacidad de la información	Plan de seguridad y privacidad de la información	Profesional Universitario del área de sistemas	20/03/2024
	Actualizar Políticas de seguridad de la información	Actualizar las políticas de seguridad y privacidad de la información de la entidad	Políticas de seguridad y privacidad de la información actualizadas	Profesional Universitario del área de sistemas	10/05/2024
	Actualizar los Procedimientos de seguridad de la información.	Actualizar los procedimientos de seguridad y privacidad de la información, con el fin de que sean normalizados.	Procedimientos de seguridad de la información.	Profesional Universitario del área de sistemas	10/06/2024
	Actualizar la matriz de activos de información	Actualizar el documento con la metodología para identificación, clasificación y valoración de activos de información.	Matriz de Inventario de activos de información actualizado.	Profesional Universitario del área de sistemas	05/08/2024

	Con base a la matriz de inventario de activos de información, se actualizan los riesgos de seguridad y privacidad de la información y seguridad digital	Actualización de la Identificación, valoración y tratamiento del riesgo.	Plan de tratamiento de riesgos de seguridad y privacidad de la información y matriz de riesgos de seguridad y privacidad de la información	Profesional Universitario del área de sistemas	10/09/2024
	Realizar piezas gráficas y/o material de promoción y sensibilización en seguridad de la información.	Documento para la comunicación, sensibilización y capacitación sobre el plan de tratamiento de seguridad y privacidad de la información	Sensibilización de los usuarios con respecto al manejo y seguridad de la información.	Profesional Universitario del área de sistemas	15/11/2024

FASE MSPI	ACTIVIDADES	META	PRODUCTO	RESPONSABLE(S)	FECHA
Implementación	Definir y medir los indicadores de gestión de la implementación del modelo de seguridad y	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Indicadores De Gestión.	Profesional Universitario del área de sistemas	14/02/2025
	Realizar las actividades necesarias con el fin de dar seguimiento al plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos.	Implementación del plan de tratamiento de riesgos.	Profesional Universitario del área de sistemas	10/03/2025

FASE MSPI	ACTIVIDADES	META	PRODUCTO	RESPONSABLE(S)	FECHA
Evaluación Desempeño	Con los datos obtenidos en la implementación, se debe realizar plan donde se evalué el desempeño de la planificación e implementación del modelo MSPI	Crear documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Plan seguimiento MSPI	Profesional Universitario del área de sistemas	10/04/2025

FASE MSPI	ACTIVIDADES	META	PRODUCTO	RESPONSABLE(S)	FECHA
Mejora Continua	Con base en los resultados de la evaluación de desempeño se debe plantear el plan de mejoramiento.	Realizar un Plan de mejoramiento, con el fin de comenzar de nuevo el ciclo del modelo MSPI y corregir lo que haya lugar	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Profesional Universitario del área de sistemas	16/06/2025

9 CONSIDERACIONES FINALES

Por todo lo anterior, se solicita la gestión de todos los colaboradores para conservar un ambiente seguro en los sistemas de información y recursos informáticos de la administración, informando de cualquier irregularidad observada en los procesos que se lleve en los sistemas de información, o al uso dado a los recursos informáticos, procurando el aseguramiento de calidad y mejora continua en la ejecución de los servicios prestados. No olvidemos que la entidad es de todos y todos somos responsables de su seguridad.

10 DOCUMENTOS RELACIONADOS

- Ley 1273 de 2009, sobre la protección de la información y de los datos.
- Ley 1581 del 17 octubre 2012, sobre Protección de datos personales.
- Ley 23 de 1982, sobre derechos de autor
- Ley 44 de 1993, Modifica Ley 23
- Ley 603 2000, Gestión de software, modifica Ley 23
- Guías Modelo de Seguridad y Privacidad

  Guía 1 - Metodología de pruebas de efectividad
  Guía 2 - Política General MSPI v1
  Guía 3 - Procedimiento de Seguridad de la Información
  Guía 4 - Roles y responsabilidades
  Guía 5 - Gestión Clasificación de Activos
  Guía 6 - Gestión Documental
  Guía 7 - Gestión de Riesgos
  Guía 8 - Controles de Seguridad de la Información
  Guía 9 - Indicadores Gestión de Seguridad de la Información
  Guía 10 - Continuidad de Negocio
  Guía 11 - Análisis de Impacto de Negocio
  Guía 12 - Seguridad en la Nube
  Guía 13 - Evidencia Digital (En actualización)
  Guía 14 - Plan de comunicación, sensibilización, capacitación

Guía 15 - Auditoria
Guía 16 - Evaluación de Desempeño
Guía 17 - Mejora continua
Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
Guía 19 - Aseguramiento de protocolo IPv4_IPv6
Guía 20 - Transición IPv4_IPv6
Guía 21 - Gestión de Incidentes