1. POLÍTICA

Proteger, preservar y administrar objetivamente la información de la E.S.E. Hospital Universitario de la Samaritana junto con las tecnologías utilizada 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.

2. OBJETIVOS

- Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- Disponibilidad: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

3. DESPLIEGUE

Esta política debe desplegarse a todos los usuarios de los servicios tecnológicos de la entidad y unidades funcionales del HUS.

4. ESTRATEGIAS

Seguridad Física y del entorno

Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, subsidiarios y a los cuartos de comunicaciones. La Subdirección de Sistemas elaborará y mantendrán las normas, controles y registros de acceso a dichas áreas.

Seguridad en los equipos

Los servidores que contengan información y servicios institucionales deben ser mantenidos en un ambiente seguro y protegido por los menos con:

• Controles de acceso y seguridad física.

• Detección de incendio y sistemas de extinción de conflagraciones.

• Controles de temperatura.

• Bajo riesgo de inundación.

• Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

4. ESTRATEGIAS

Toda información institucional en formato digital debe ser mantenida en servidores aprobados por la Subdirección de Sistemas. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación de la subdirección de Sistemas.

Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

La Subdirección de Sistemas debe asegurar que la infraestructura de servicios de TI este cubierta por mantenimiento y soporte adecuados de hardware y software

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

Administración de las comunicaciones y operaciones

Reporte e investigación de incidentes de seguridad

El personal de la E.S.E. Hospital Universitario de la Samaritana debe reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su líder de área a la Subdirección de Sistemas.

La Subdirección de Sistemas debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos. La subdirección de sistemas elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos y guías que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

En todo caso y como control mínimo, las estaciones de trabajo del HUS deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de la estaciones no están autorizados a deshabilitar este control.

La Subdirección de Sistemas podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La Subdirección de Sistemas debe mantener actualizada una base de datos con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

La Subdirección de Sistemas debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas. Los registros de copias de

4. ESTRATEGIAS

seguridad deben ser guardados en una base de datos creada para tal fin.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben entregar al respectivo jefe de dependencia las copias de seguridad para su registro y custodia.

Administración de Configuraciones de Red

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Subdirección de Sistemas.

Todo equipo de TI debe ser revisado, registrado y aprobado por la Subdirección de Sistemas antes de conectarse a cualquier nodo de la Red de comunicaciones y datos institucional. Dicha dependencia debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad.

Internet y Correo Electrónico

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por la subdirección de sistemas y en todo caso debe velar por el cumplimiento del código de ética institucional y el manejo responsable de los recursos de tecnologías de la información.

Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas del HUS deben ser aprobadas por la Subdirección de Sistemas, de acuerdo a los procedimientos elaborados para tal fin por dichas dependencias. No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. La subdirección de sistemas deben desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad.

Corresponde a la Subdirección de Sistemas mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos institucionales.

Control de Acceso

Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales debe estar restringido según los perfiles de usuario definidos por la subdirección de sistemas.

Computación Móvil

El HUS reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, notebooks, PDA, celulares, etc). Corresponde a la Oficina de Recursos Humanos en conjunto con la Subdirección de sistemas elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información. Las redes inalámbricas potencialmente introducen nuevos riesgos de seguridad que deben ser identificados, valorados y tratados de acuerdo a los lineamientos de la Política de Seguridad en redes inalámbricas.

Acceso Remoto

El acceso remoto a servicios de red ofrecidos por el HUS debe estar sujeto a medidas de control definidas por la Subdirección de Sistemas, las cuales deben incluir acuerdos escritos de

4. ESTRATEGIAS

seguridad de la información.

Adquisición, Desarrollo y Mantenimiento de Sistemas

Software

Para apoyar los procesos operativos y estratégicos del HUS debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.

La subdirección de Sistemas debe establecer los lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto.

Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo del HUS.

5. INDICADORES

(Mencione como se va a medir la política institucional con base en los objetivos planteados, por favor revisar los indicadores ya existentes en el sistema de información ALMERA, de no existir las variables que midan la política, entonces formular los indicadores correspondientes).

6. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	JUSTIFICACIÓN
01	23/05/2025	NA	Primera Versión
02	01/03/2025	Formato	Actualización Formato

(Una vez formulada la política institucional se debe documentar la resolución de adopción institucional, solicitar a (cargo) una resolución interna).