POLÍTICAS INSTITUCIONALES

2020-2024

DR. PEDRO JAVIER GUTIÉRREZ
GERENTE HPSC

Gestión Estratégica
Código ES-PLI- 01 Vr. 2

HOSPITAL PSIQUIÁTRICO
San Camilo
UN NUEVO COMIENZO

6.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La E.S.E. Hospital Psiquiátrico San camilo en cumplimiento de sus funciones y entendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información institucional, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para asegurar la dirección estratégica La E.S.E. Hospital Psiquiátrico San camilo, se establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información así:

OBJETIVOS ESPECÍFICOS

- Fortalecer la cultura de prevención de riesgos de seguridad de la información por medio de la sensibilización y el entrenamiento constante de los funcionarios del hospital.

- Garantizar la disponibilidad requerida por el hospital, de los sistemas informáticos vitales para el desarrollo de los procesos misionales y asistenciales de la entidad.

- Minimizar los riesgos sobre los sistemas informáticos, identificando y gestionando oportunamente las vulnerabilidades técnicas a nivel de sistemas operativos, aplicaciones de software y bases de datos utilizadas por los procesos internos.

- Gestionar los eventos e incidentes de seguridad y ciberseguridad, fortaleciendo la capacidad para hacer frente a las amenazas y ataques informáticos.

- Sensibilizar a los servidores públicos, contratistas y terceros de la ESE Hospital Psiquiátrico San Camilo acerca de la necesidad de poner en práctica la política de seguridad y privacidad de la información.

- Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.

INDICADORES

1. Controles implementados por cada riesgo de seguridad de la información identificado.
2. Cantidad de colaboradores capacitados en el uso seguro de la información relacionado a la seguridad digital.
3. Cantidad de simulacros de incidentes, simulacros de ingeniería social de evaluación de vulnerabilidades informáticas y respuesta a ataques de seguridad digital implementados al interior del hospital en la vigencia actual
4. Número de copias de respaldo con la debida restauración que garantizan la operación en la vigencia.

ACCIONES ESTRATÉGICAS

- Formular, aprobar e implementar la política de seguridad y privacidad de la información contando con indicadores que permitan medir su cumplimiento adoptado por las diferentes áreas institucionales que conlleve a la protección de los activos de la información, su confidencialidad, integridad y disponibilidad.

- Promover la implementación del sistema de gestión de la seguridad de información (SGSI) que cumpla con las necesidades de información del hospital.

- Establecer roles y responsabilidades específicos respecto a la seguridad de la información.

- Adquirir las competencias necesarias en formación y/o experiencia en el manejo de la seguridad de información

- Establecer, comunicar e implementar controles de tecnología para proteger la información, por ejemplo: Reglamentar y controlar la instalación de todo tipo de software, entre todos los funcionarios y contratistas de la ESE Hospital Psiquiátrico San Camilo

- Realizar jornadas de concientización y/o capacitación del uso seguro de la información.

- Realizar ejercicios de simulación de incidentes, simulacros de ingeniería social, evaluación de vulnerabilidades informáticas y respuesta a ataques de seguridad digital al interior del hospital y generar evidencia de los mismos que permita realizar concientización y formación a partir de los resultados obtenidos.

- Clasificar y etiquetar la información de acuerdo a las leyes aplicables vigentes

- Evaluar los riesgos de seguridad a los que está expuesta cada unidad para evaluar y seleccionar las herramientas de seguridad informática adecuadas para mitigarlos.

- Realizar copias de respaldo con una periodicidad definida con los usuarios de la información y realizar pruebas de restauración de las copias para garantizar su correcto funcionamiento en caso de que sean requeridas.

- Evaluar y actualizar el plan de contingencia para asegurar la continuidad del negocio.