	<b>FORMATO DE INFORME</b>	<b>Fecha:</b> 05/11/2024
	<b>EMPRESA SOCIAL DEL ESTADO</b>	<b>Código:</b> MDE-GPDI-GD-F-004
	<b>HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Versión:</b> 03
	<b>LA PLATA HUILA</b>	<b>Página:</b> 1 de 7
	<b>PROCESO: GESTIÓN DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO INSTITUCIONAL</b>	

<b>FECHA:</b>	10 de JULIO del 2025
<b>ACTIVIDAD:</b>	Informe de Plan Estratégico y Riesgos de Seguridad
<b>PROCESO VINCULADO:</b>	Seguimiento Planes Institucionales 2025
<b>RESPONSABLE:</b>	Edwin Fabian Castro Quintero
<b>OBJETIVO:</b>	Realizar seguimiento a los planes institucionales 2025 según Estándares de Acreditación en Salud Según Res. 5095 de 2018

## CONTENIDO DEL INFORME:

### INTRODUCCIÓN


El manejo adecuado de los riesgos relacionados con la seguridad y la privacidad de la información es crucial en un entorno hospitalario, donde se gestionan datos sensibles de pacientes y empleados. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital Departamental San Antonio de Padua de La Plata, Huila, tiene como objetivo identificar, evaluar y mitigar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información tratada en la institución, especialmente aquella relacionada con la salud de los pacientes.

### OBJETIVO

Revisar incidentes de seguridad y privacidad de la información, seguridad informática o seguridad digital, teniendo en cuenta los lineamientos y estándares definidos, a través de una oportuna identificación, atención y respuesta con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de la E.S.E. Hospital Departamental San Antonio de Padua de La Plata Huila.

### ALCANCE

La gestión de incidentes de seguridad inicia desde la identificación de un evento, detección, contención y solución de este, finalizando con la documentación y lecciones aprendidas. El documento aplica a nivel de la E.S.E. Hospital

	<b>FORMATO DE INFORME</b>	<b>Fecha:</b> 05/11/2024
	<b>EMPRESA SOCIAL DEL ESTADO</b>	<b>Código:</b> MDE-GPDI-GD-F-004
	<b>HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA</b>	<b>Versión:</b> 03
	<b>PROCESO: GESTIÓN DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO INSTITUCIONAL</b>	<b>Página:</b> 2 de 7

Departamental San Antonio de Padua de La Plata Huila.


La gestión de estos datos implica un manejo responsable y conforme a las leyes de protección de datos personales, además de una estricta clasificación de la información para controlar el acceso y minimizar los riesgos.

### Riesgos Identificados

A continuación se presentan los principales riesgos de seguridad y privacidad de la información identificados en el hospital:

- **Acceso no autorizado:** El riesgo de que personal no autorizado tenga acceso a información confidencial, ya sea por fallas en la autenticación, mal manejo de credenciales o negligencia en el control de accesos.
- **Filtración de información:** La posible divulgación no autorizada de datos sensibles debido a la falta de controles en el manejo de la información, ya sea por errores humanos.
- **Pérdida de datos:** El riesgo de pérdida de información crítica debido a fallos técnicos, como la falta de copias de seguridad o ataques de ransomware.
- **Falta de capacitación del personal:** El personal del hospital puede no estar completamente capacitado para identificar y manejar situaciones de riesgo relacionadas con la seguridad de la información.
- **Amenazas cibernéticas:** Riesgos derivados de ataques externos, como phishing, malware, ransomware o ataques de denegación de servicio (DDoS), que pueden comprometer la integridad de los sistemas.
- **Inseguridad en el manejo de dispositivos móviles:** Los dispositivos móviles no siempre están suficientemente protegidos, lo que representa un riesgo importante si se usan para almacenar o acceder a información sensible.

— Salud Integral, Impacto Real —

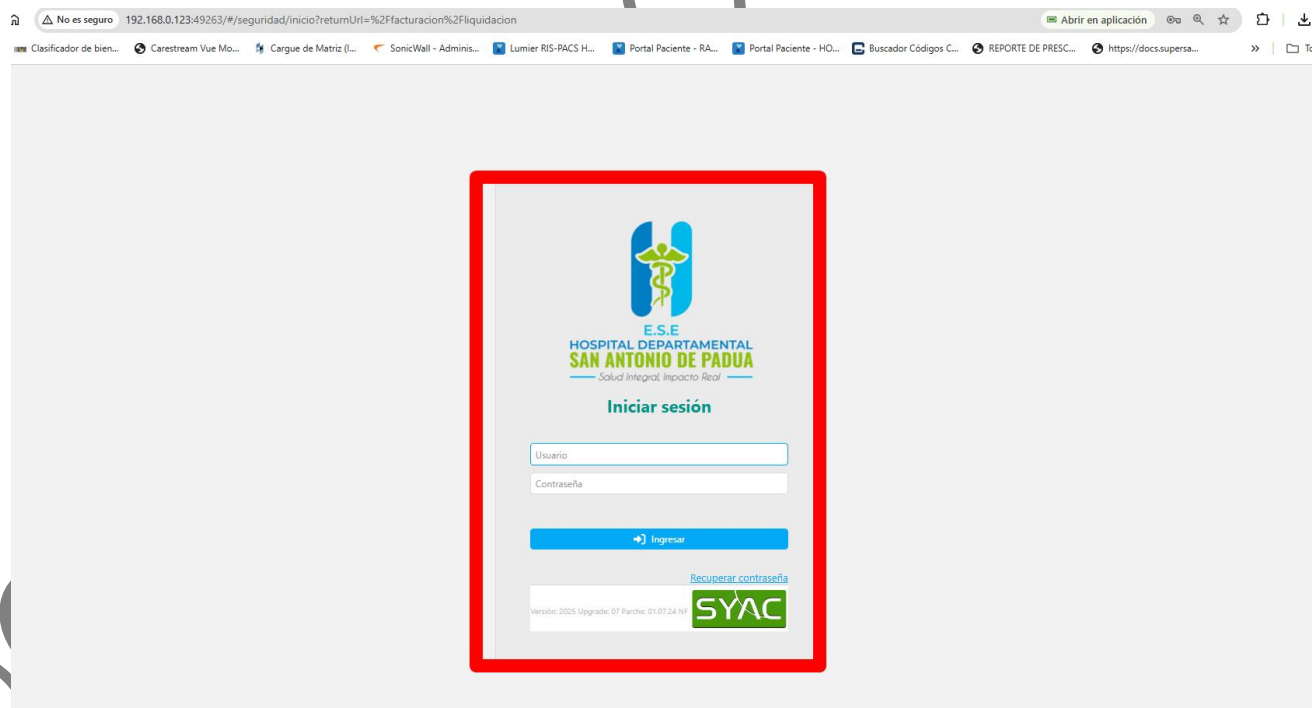
	<b>FORMATO DE INFORME</b>	<b>Fecha:</b> 05/11/2024
	<b>EMPRESA SOCIAL DEL ESTADO</b> <b>HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b> <b>LA PLATA HUILA</b> <b>PROCESO: GESTIÓN DE PLANEACIÓN Y</b> <b>DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO</b> <b>INSTITUCIONAL</b>	<b>Código:</b> MDE-GPDI-GD-F-004 <b>Versión:</b> 03 <b>Página:</b> 3 de 7

## Estrategias de Tratamiento de Riesgos

Para mitigar los riesgos identificados, se proponen las siguientes estrategias y medidas de tratamiento:

## Control de Accesos

La implementación de controles de acceso efectivos es esencial para preservar la confidencialidad, integridad y disponibilidad de los datos institucionales. El uso de un modelo de acceso basado en roles (RBAC) asegura que cada funcionario acceda únicamente a la información necesaria para cumplir sus funciones, reduciendo la superficie de exposición y facilitando la trazabilidad. El monitoreo constante y las auditorías permiten detectar intentos de acceso no autorizados y establecer acciones correctivas de manera proactiva. Esto permite mitigar riesgos derivados de credenciales mal gestionadas o de usuarios con privilegios excesivos.



— Salud Integral, Impacto Real —

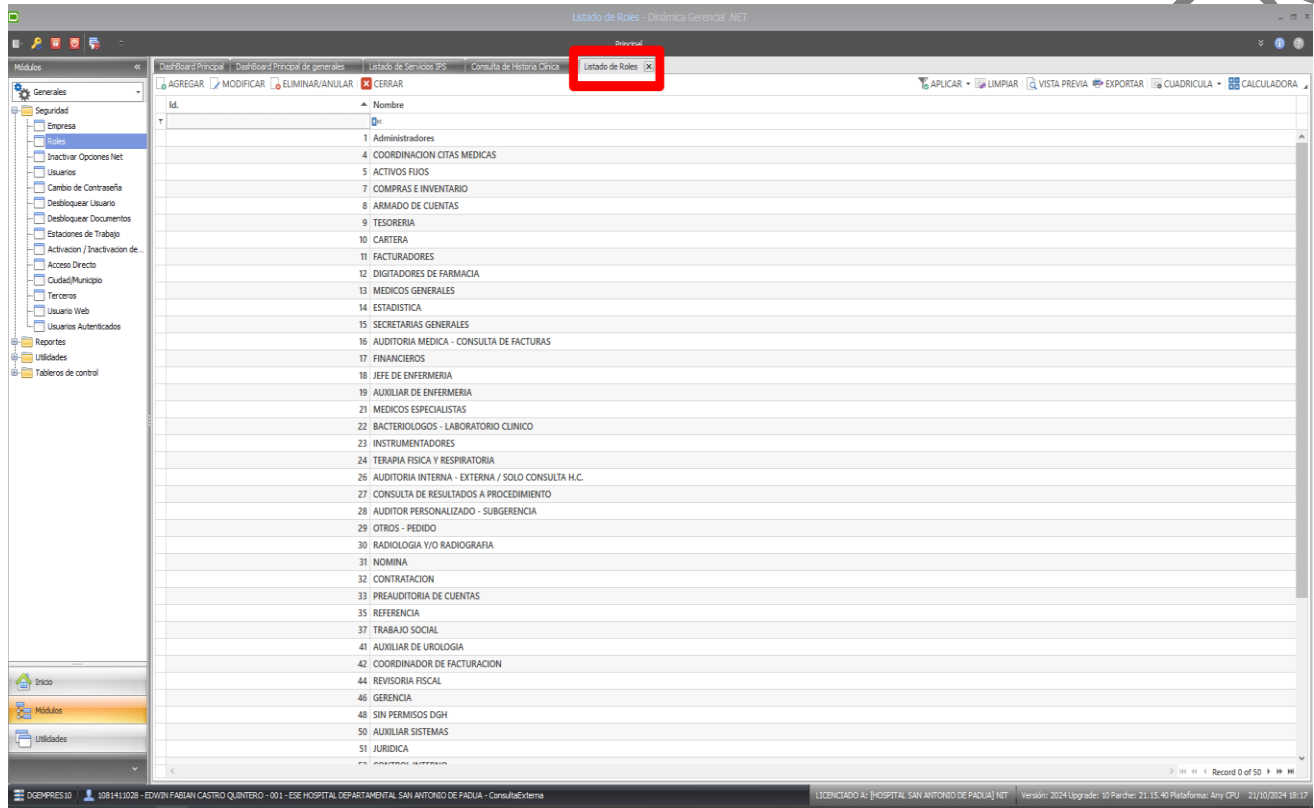
"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".



**FORMATO DE INFORME**  
**EMPRESA SOCIAL DEL ESTADO**  
**HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA**  
**LA PLATA HUILA**  
**PROCESO: GESTIÓN DE PLANEACIÓN Y**  
**DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO**  
**INSTITUCIONAL**

**Fecha:** 05/11/2024  
**Código:** MDE-GPDI-GD-F-004  
**Versión:** 03  
**Página:** 4 de 7

Monitoreo y auditoría de accesos: Establecer procedimientos de monitoreo continuo de accesos a sistemas y bases de datos, realizando auditorías periódicas para identificar accesos no autorizados.




## Protección de la Información Sensible

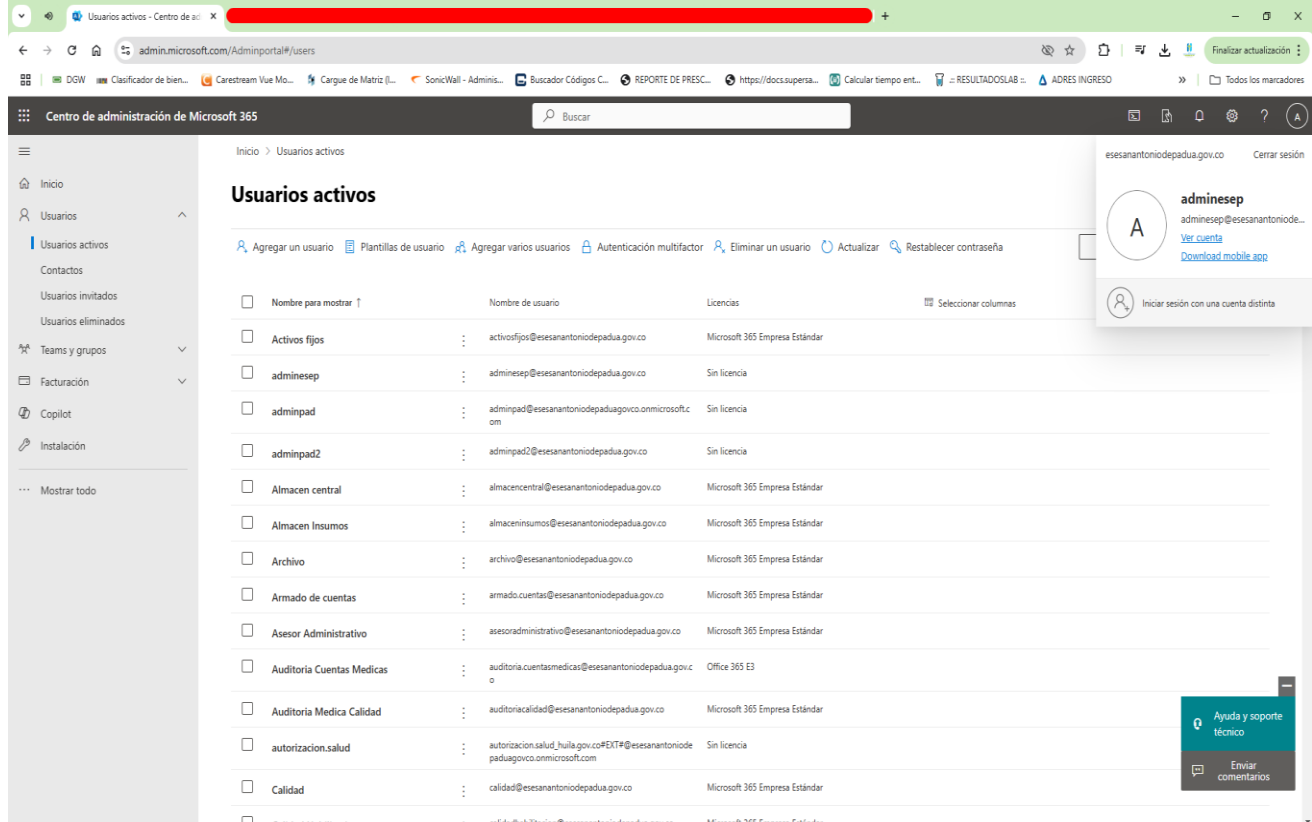
Dado que los datos clínicos y personales manejados por el hospital son considerados sensibles según la legislación colombiana, es indispensable implementar políticas estrictas de manejo, cifrado y acceso. La protección mediante criptografía de la información en tránsito y en reposo impide que actores no autorizados accedan a los datos incluso si comprometen un dispositivo o red. La existencia de lineamientos claros para el uso de contraseñas, cifrado de dispositivos y control del acceso remoto refuerzan la seguridad general de la institución frente a vulnerabilidades comunes.

## CORREOS ELECTRONICOS CORPORATIVOS

— Salud Integral, Impacto Real —

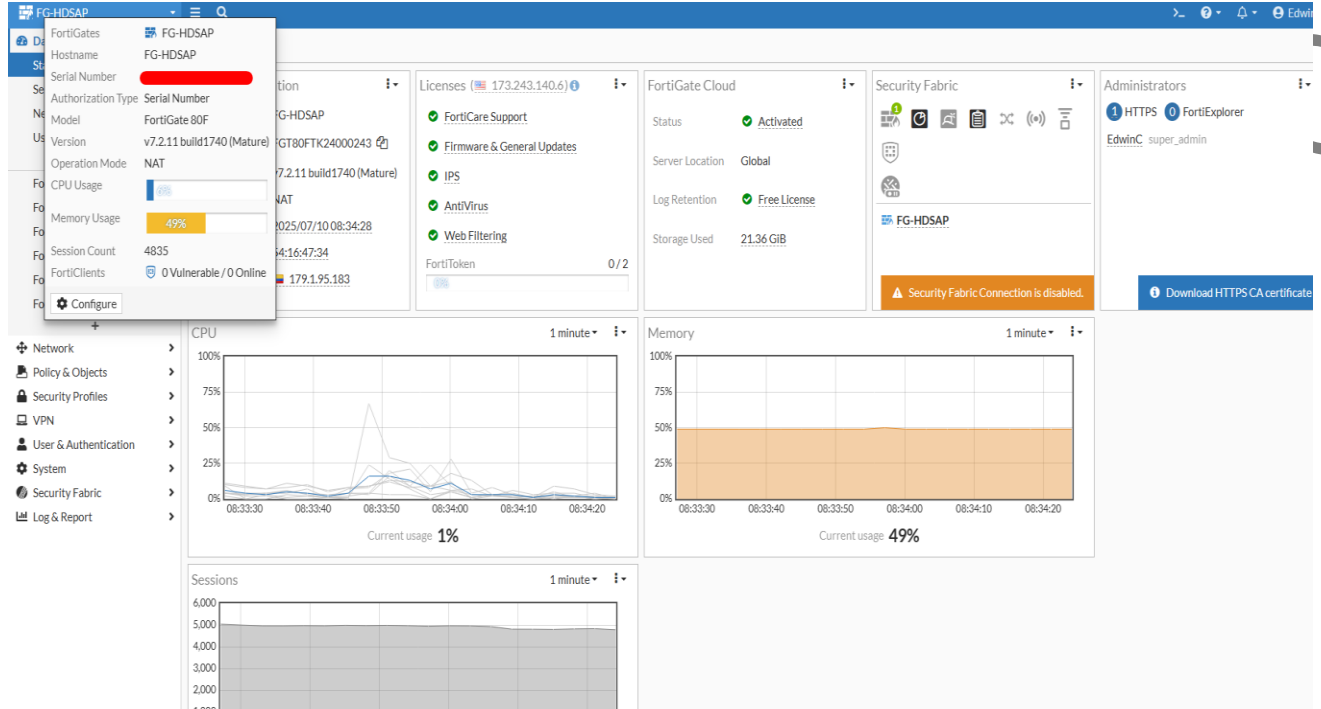
"Documento no valido en medio impreso sin la identificación de sello seco "Documento Controlado" Este documento contiene información de carácter confidencial y es propiedad del Hospital. Ninguna parte de su contenido puede ser usado, copiado, divulgado sin autorización escrita por parte del Hospital".

	<b>FORMATO DE INFORME</b>	<b>Fecha:</b> 05/11/2024
	<b>EMPRESA SOCIAL DEL ESTADO</b>	<b>Código:</b> MDE-GPDI-GD-F-004
	<b>HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Versión:</b> 03
	<b>LA PLATA HUILA</b>	<b>Página:</b> 5 de 7
	<b>PROCESO: GESTIÓN DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO INSTITUCIONAL</b>	



## Protección Contra Amenazas Cibernéticas


En un entorno digital expuesto a ataques constantes, la protección contra amenazas cibernéticas como virus, ransomware o phishing se convierte en una prioridad estratégica. El uso de soluciones actualizadas de antivirus, firewalls y monitoreo de red permite prevenir y detectar incidentes en etapas tempranas. Complementar estas tecnologías con análisis de comportamiento y segmentación de red fortalece la resiliencia ante ataques dirigidos y asegura la continuidad de los servicios clínicos.



## Capacitación y Concienciación del Personal

Programas de capacitación continua: Desarrollar programas de capacitación en seguridad informática, privacidad de la información y manejo adecuado de datos sensibles para todo el personal, incluyendo médicos, administrativos y técnicos.

Concienciación sobre políticas de seguridad: Realizar campañas periódicas de concienciación sobre la importancia de la seguridad de la información y las políticas de privacidad.

	<b>FORMATO DE INFORME</b>	<b>Fecha:</b> 05/11/2024
	<b>EMPRESA SOCIAL DEL ESTADO</b>	<b>Código:</b> MDE-GPDI-GD-F-004
	<b>HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA</b>	<b>Versión:</b> 03
	<b>LA PLATA HUILA</b>	<b>Página:</b> 7 de 7
	<b>PROCESO: GESTIÓN DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO INSTITUCIONAL</b>	

## Plan de Respuesta a Incidentes y Recuperación ante Desastres

Contar con planes formales de respuesta ante incidentes (IRP) y de recuperación ante desastres (DRP) es vital para minimizar los efectos negativos de una brecha de seguridad o falla técnica. Estos planes permiten actuar con rapidez, asignar responsabilidades y garantizar la recuperación de datos e infraestructuras en plazos aceptables. La existencia de copias de seguridad confiables y su validación regular a través de simulacros asegura que la institución esté preparada para restaurar operaciones críticas en tiempo oportuno.

