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

FECHA:	07 de NOVIEMBRE del 2024
ACTIVIDAD:	Informe de Plan Estratégico y Riesgos de Seguridad
PROCESO VINCULADO:	Seguimiento Planes Institucionales 2024
RESPONSABLE:	Edwin Fabian Castro Quintero
OBJETIVO:	Realizar seguimiento a los planes institucionales 2024 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

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


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.

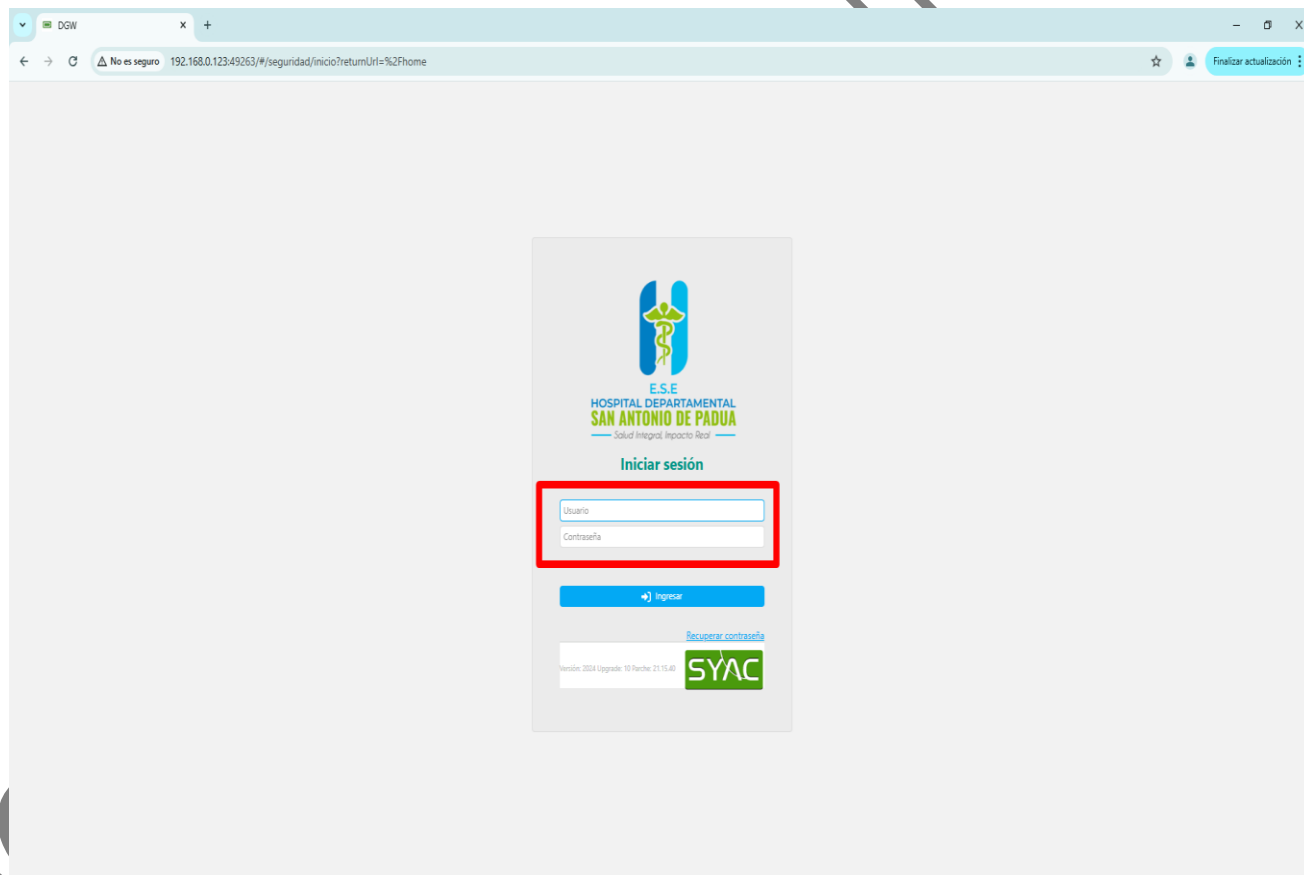
	FORMATO DE INFORME	Fecha: 05/11/2024
	EMPRESA SOCIAL DEL ESTADO	Código: MDE-GPDI-GD-F-004
	HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA LA PLATA HUILA	Versión: 03
PROCESO: GESTIÓN DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO INSTITUCIONAL		Página: 3 de 7

Estrategias de Tratamiento de Riesgos

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

Control de Accesos

Política de acceso basado en roles (RBAC): Establecer control de accesos basada en el rol del usuario, limitando el acceso a la información estrictamente necesaria para cada empleado.

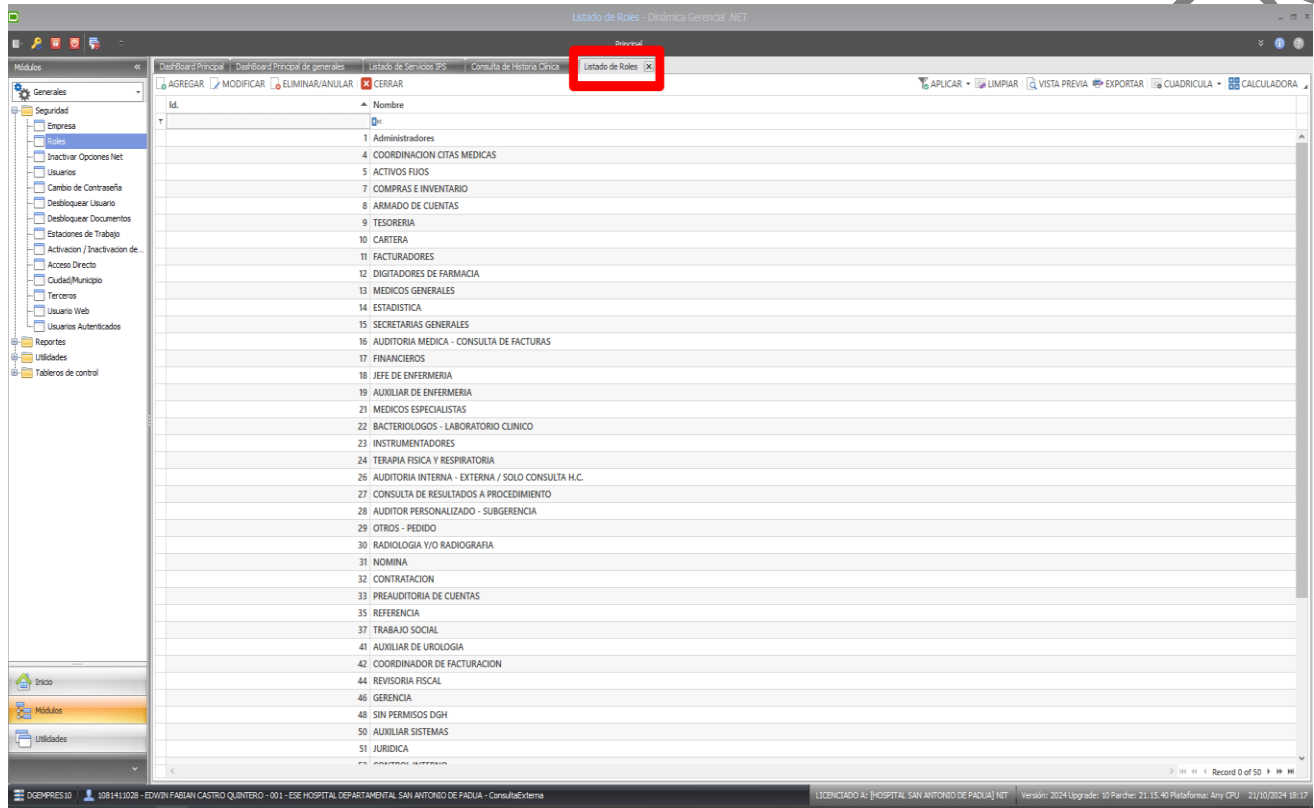




FORMATO DE INFORME
EMPRESA SOCIAL DEL ESTADO
HOSPITAL DEPARTAMENTAL SAN ANTONIO DE PADUA
LA PLATA HUILA
PROCESO: GESTIÓN DE PLANEACIÓN Y
DIRECCIONAMIENTO ESTRATÉGICO O DESARROLLO
INSTITUCIONAL

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

Implementar cifrado de datos tanto en reposo como en tránsito, especialmente para datos sensibles como los registros médicos y la información personal de los pacientes.

Desarrollar y poner en marcha políticas claras sobre cómo debe manejarse la información sensible, incluyendo el uso adecuado de contraseñas, el cifrado de dispositivos y el acceso remoto.

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".



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: 5 de 7

<input type="checkbox"/>	Nombre para mostrar ↑	Nombre de usuario	Licencias	Seleccionar columnas
<input type="checkbox"/>	Activos fijos	activosfijos@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	adminesep	adminesep@esesanantoniodepadua.gov.co	Sin licencia	
<input type="checkbox"/>	adminpad	adminpad@esesanantoniodepadua.gov.co.onmicrosoft.com	Sin licencia	
<input type="checkbox"/>	adminpad2	adminpad2@esesanantoniodepadua.gov.co	Sin licencia	
<input type="checkbox"/>	Almacen central	almacencentral@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Almacen Insumos	almaceninsumos@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Archivo	archivo@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Armado de cuentas	armado.cuentas@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Asesor Administrativo	asesoradministrativo@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Auditoria Cuentas Medicas	auditoria.cuentasmedicas@esesanantoniodepadua.gov.co	Office 365 E3	
<input type="checkbox"/>	Auditoria Medica Calidad	auditoriacalidad@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	autorizacion.salud	autorizacion.salud_huila.gov.co=EXTF@esesanantoniodepadua.gov.co.onmicrosoft.com	Sin licencia	
<input type="checkbox"/>	Calidad	calidad@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	
<input type="checkbox"/>	Calidad Institucional	calidad.institucional@esesanantoniodepadua.gov.co	Microsoft 365 Empresa Estándar	

Protección Contra Amenazas Cibernéticas

Antivirus y firewall actualizado: Instalar y mantener actualizado un sistema de protección antivirus y firewall en todos los dispositivos y servidores que manejen información crítica.

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: 6 de 7

System Information

Model:	T2 350
Product Code:	19331
Serial Number:	[REDACTED]
Authentication Code:	F4DU-6XAV
Firmware Version:	SonicOS Enhanced 6.5.4.13-105n
SafeMode Version:	SafeMode 6.2.3.12
ROM Version:	SonicROM 5.6.2.2
CPU:	17.65% - 2.40 GHz (2 x 1200 MHz Hiips64 Octeon Processor)
Total Memory:	1 GB RAM, 64 MB Flash
System Time:	2024/11/07 17:59:15
Up Time:	17 Days 07:49:06
Connections:	Peak:11045 Current:2766 Max:67500
Connection Usage:	4.098%
Last Modified By:	[REDACTED]
Registration Code:	[REDACTED]

Security Services

Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
SSL VPN Nodes/Users	Licensed 3 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Licensed 4 Licenses (0 in use)
CFS (Content Filter)	Licensed
Expanded Feature Set	Not Licensed
Capture Client Enforcement	Not Licensed
McAfee AV Enforcement	Not Licensed
Client Content Filtering	Not Licensed
DPS-SSL Enforcement	Not Licensed
Gateway Anti-Virus	Licensed
Capture ATP	Not Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
App Control	Licensed
App Visualization	Licensed
Anti-Spam	Not Licensed
Analyzer	Licensed
DPS-SSL	Licensed Client/Server
DPS-SSH	Not Licensed
WAN Acceleration	Not Licensed
WOLAC Acceleration	Licensed
Botnet	Licensed

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.



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: 7 de 7

Plan de Respuesta a Incidentes y Recuperación ante Desastres

Desarrollo de un Plan de Respuesta a Incidentes (IRP): Establecer un protocolo claro de actuación ante incidentes de seguridad, identificando roles y procedimientos para la respuesta rápida.

Copia de seguridad y recuperación ante desastres (DRP): Implementar un sistema robusto de copias de seguridad periódicas y garantizar que existan planes de recuperación ante desastres para restaurar rápidamente los datos y sistemas en caso de un incidente.

