
	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 1 de 6

TRATAMIENTO DE RIESGOS DE LA PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

UNIDAD DE SALUD DE IBAGUÉ

2025

	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 2 de 6

1. IDENTIFICACIÓN DE RIESGOS


La primera etapa es identificar los riesgos potenciales que pueden comprometer la **privacidad** y la **seguridad** de la información. Los principales riesgos asociados a los sistemas de información de la USI son los siguientes:

- **Acceso no autorizado a datos personales de pacientes:** Debido a una gestión deficiente de usuarios o controles de acceso inapropiados.
- **Violación de la confidencialidad** de la información médica debido a fugas o pérdidas de datos (por ejemplo, por ataques cibernéticos como phishing o ransomware).
- **Desastres o fallos tecnológicos:** Pérdida de información debido a fallos en la infraestructura de TI, como servidores caídos, apagones, problemas de red, etc.
- **Exposición de la infraestructura tecnológica a ciberataques:** Ataques dirigidos contra la red, bases de datos o sistemas médicos, lo cual podría comprometer la disponibilidad o integridad de la información.
- **Involucramiento del personal en prácticas no seguras:** Falta de sensibilización, capacitación o cumplimiento de políticas de seguridad que lleva a prácticas de manejo inadecuado de datos.

2. EVALUACIÓN DEL RIESGO

Una vez identificados los riesgos, estos deben evaluarse en términos de **probabilidad de ocurrencia** e **impacto** sobre la seguridad de la información. Para ello, se aplicará una escala en la que se clasificará cada riesgo según los siguientes factores:

- **Probabilidad:** ¿Qué tan probable es que este riesgo ocurra?
 - Alta: El riesgo tiene alta probabilidad de ocurrir.
 - Media: Es posible que ocurra.
 - Baja: Es poco probable que ocurra.
- **Impacto:** ¿Cuál será el impacto si este riesgo ocurre?
 - Alto: Impacto crítico en la disponibilidad, integridad o confidencialidad de la información.

	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 3 de 6

- Medio: Impacto moderado, afectando operativamente el sistema, pero no comprometiendo gravemente la seguridad de los datos.
- Bajo: No tiene un impacto grave en la operación ni en la seguridad de los datos.

EVALUACION DE RIESGOS

Riesgo	Probabilidad	Impacto	Riesgo Total
Acceso no autorizado a datos médicos sensibles	Alta	Alto	Alto
Pérdida de datos médicos por un ataque cibernético	Media	Alto	Alto
Acceso por empleados sin capacitación adecuada	Alta	Medio	Medio
Destrucción de equipos por desastres naturales	Baja	Medio	Bajo
Fallo en el sistema de respaldo o recuperación	Media	Alto	Alto


3. Tratamiento del Riesgo

Con el fin de mitigar los riesgos identificados, es necesario desarrollar e implementar controles de seguridad y acciones correctivas. Para cada riesgo, se deben considerar las siguientes acciones:

3.1. Tratamiento de Riesgos de Alta Prioridad

1. Acceso no autorizado a datos sensibles

- **Medidas a implementar:**
 - **Control de acceso basado en roles (RBAC):** Asegurar que los accesos a la información se otorguen según la necesidad laboral, empleando una política de **mínimos privilegios**.
 - **Autenticación multifactor (MFA):** Requerir autenticación adicional, especialmente en sistemas críticos, como los servidores donde se almacenan los datos médicos.

	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 4 de 6

- **Monitoreo de registros de acceso:** Implementar herramientas para la auditoría de accesos a datos personales, realizando una revisión periódica para detectar anomalías.

2. Pérdida de datos sensibles (ciberataques)

- **Medidas a implementar:**
 - **Cifrado de datos:** Asegurar que los datos, tanto en reposo como en tránsito, estén cifrados utilizando protocolos de cifrado modernos.
 - **Capacitación continua** en ciberseguridad para todo el personal, con enfoque en prevenir ataques como **phishing**.
 - **Implementación de herramientas de detección de intrusos (IDS/IPS)** y sistemas antivirus actualizados.

3. Pérdida de respaldo o fallo en la recuperación


- **Medidas a implementar:**
 - **Pruebas periódicas de restauración de datos:** Asegurar que las copias de seguridad se restauren correctamente realizando pruebas cada trimestre.
 - **Asegurar almacenamiento redundante:** Almacenar copias de seguridad tanto en servidores locales como en un datacenter alternativo en una ubicación geográfica diferente.

3.2. Tratamiento de Riesgos de Prioridad Media

1. Acceso de empleados sin la capacitación necesaria

- **Medidas a implementar:**
 - **Programas de capacitación y concientización** sobre seguridad de la información al menos dos veces al año.
 - **Evaluación periódica de las políticas de seguridad** para comprobar que todo el personal conoce las mejores prácticas de manejo y protección de datos.

2. Desastres naturales o fallos operacionales

	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 5 de 6

- **Medidas a implementar:**

- **Plan de continuidad de negocio (BCP):** Desarrollar procedimientos operativos estándar para recuperación rápida en caso de desastres naturales, garantizando que la infraestructura tecnológica sea resistente.
- **Implementación de sistemas de redundancia** en redes y servidores (por ejemplo, energía eléctrica, fallos de conexión a internet).

3.3. Tratamiento de Riesgos de Baja Prioridad

1. Destrucción de equipos por desastres naturales

- **Medidas a implementar:**

- **Revisión y refuerzo de la infraestructura física:** Fortalecer las infraestructuras donde se alojan los servidores, como la protección de equipos ante terremotos o inundaciones.
- **Seguro de equipos tecnológicos:** Contratar seguros que protejan los activos tecnológicos en caso de daño o pérdida por desastres naturales.


4. Plan de Monitoreo y Revisión

Para garantizar la eficacia del tratamiento de riesgos, es importante realizar un **monitoreo continuo** y llevar a cabo **auditorías periódicas**. Las actividades para este propósito incluyen:

- **Monitoreo en tiempo real de sistemas críticos**, como bases de datos y servidores médicos.
- **Auditorías externas** cada seis meses para revisar los controles de seguridad y garantizar el cumplimiento de normativas de privacidad.
- **Revisiones anuales del plan** para identificar nuevos riesgos o áreas de mejora.

5. Gestión de Incidentes de Seguridad

Cada vez que ocurra un incidente relacionado con la seguridad de la información o la privacidad, se activará un protocolo de respuesta adecuado:

	UNIDAD DE SALUD DE IBAGUE E.S.E. IBAGUE TOLIMA	CODIGO: GSI-SI-PL-003
	GESTION DE SISTEMAS DE INFORMACIÓN, COMUNICACIÓN Y TICS	VERSION: 001
	SUBPROCESO SISTEMAS	FECHA:
	FORMATO REPORTE TECNICO EQUIPOS DE CÓMPUTO	Página 6 de 6

- **Detección y reporte inmediato del incidente:** El personal debe reportar cualquier sospecha de incidente inmediatamente.
- **Contención del incidente:** Se tomarán medidas rápidas para mitigar los efectos, como bloquear accesos no autorizados o apagar sistemas comprometidos.
- **Investigación y análisis post-incidente:** Se llevará a cabo un análisis de causa raíz para prevenir futuros incidentes similares.
- **Recuperación y restauración** de datos y sistemas afectados, con el soporte de las copias de seguridad.

CONCLUSIÓN

El tratamiento de los riesgos de privacidad y seguridad de la información se logra mediante la implementación de controles adecuados, el monitoreo constante de las amenazas, y la educación continua del personal. Este proceso ayudará a la **Unidad de Salud de Ibagué** a garantizar que la seguridad y la privacidad de la información de los pacientes estén siempre protegidas, y que se cumplan con las normativas vigentes, contribuyendo al bienestar de la organización y sus pacientes.

SAUL BETANCOURTH CARO
Profesional Universitario Sistemas