Universidad Estatal a Distancia

Vicerrectoría Académica

Escuela de Ciencias Exactas y Naturales

Cátedra Tecnología de Sistemas

Seguridad y auditoria en las TIC

Código: 03070

Tarea #2

Tema: Informe de Auditoría

Estudiante:

Francisco Campos Sandi

Cédula:

114750560

Sede: San Vito

Grupo: 04

Tutor:

Edgar Valladares Leal

III CUATRIMESTRE 2024

Tabla de contenido

Introducción

En el presente informe se aborda un caso real de fuga de información en un grupo de hospitales privados, destacando la complejidad y la relevancia de la ciberseguridad en el ámbito de la salud. A medida que las instituciones médicas adoptan tecnologías digitales para mejorar la atención al paciente, también se enfrentan a desafíos significativos en la protección de datos sensibles. Este trabajo es crucial, ya que la exposición de información confidencial no solo compromete la privacidad de los pacientes, sino que también puede acarrear consecuencias legales para la organización, como el incumplimiento de la Ley Orgánica de Protección de Datos (LOPD).

El informe se estructura en varias secciones. Primero, se presenta un análisis detallado de la actividad auditada, que incluye antecedentes sobre el uso no autorizado de servicios de almacenamiento en la nube por parte del personal médico, lo que condujo a riesgos serios en el manejo de datos. A continuación, se identifican y describen las situaciones relevantes que afectan significativamente el contexto analizado, así como las situaciones encontradas durante la auditoría, que ofrecen una visión clara de las vulnerabilidades existentes.

Asimismo, se incluyen instrumentos de recopilación de información, como un cuestionario y una lista de chequeo, que permiten una evaluación sistemática del estado actual de la seguridad de la información en los hospitales. Finalmente, se presentan conclusiones y recomendaciones para mitigar los riesgos identificados, resaltando la necesidad de un equilibrio entre funcionalidad y seguridad en la gestión de información sensible. Este trabajo no solo busca informar sobre la situación actual, sino también proporcionar un marco de acción para mejorar las prácticas de ciberseguridad en el sector salud.

Desarrollo

Auditoría de Seguridad de la Información en el Uso de Servicios de Almacenamiento en la Nube en Hospitales Privados

Objetivo

Evaluar el proceso de manejo y almacenamiento de información confidencial de pacientes en servicios de almacenamiento en la nube

Antecedentes

La actividad objeto de auditoría se centra en el uso no autorizado de servicios de almacenamiento en la nube por parte del personal médico en un grupo de hospitales privados. A través de un análisis del tráfico de red, se identificó un patrón inusual de transferencia de datos hacia un servicio de almacenamiento en la nube. Esta práctica, impulsada por la necesidad de mejorar la atención al paciente, comprometió la confidencialidad de la información médica, ya que los datos subidos carecían de la seguridad adecuada y no cumplían con la Ley Orgánica de Protección de Datos (LOPD).

Lista de distribución

Personal Involucrado:

- Director de Seguridad del Hospital
- Gerentes de Tecnología de la Información
- Personal Médico (Médicos de Consultas Externas)
- Personal Administrativo
- Auditores Externos
- Entes Reguladores (Autoridad Nacional de Protección de Datos)

Situaciones relevantes

- Uso No Autorizado de Servicios de Almacenamiento en la Nube: Personal médico subiendo información confidencial a plataformas externas sin control ni autorización.
- Exposición de Datos Sensibles: Almacenamiento y transferencia de historias clínicas y resultados de pruebas sin medidas de seguridad adecuadas.
- Incumplimiento de Normativas: Posible violación de la LOPD debido a la falta de protección en el manejo de datos sensibles.

Conclusiones

La fuga de información no siempre es consecuencia de un ataque malintencionado; a menudo, resulta de prácticas inadvertidas dentro de la organización. La identificación de esta situación en el uso de servicios de almacenamiento en la nube ha puesto de manifiesto la necesidad de equilibrar la funcionalidad con la seguridad. Las medidas propuestas, que incluyen la creación de una nube privada, la prohibición de servicios externos, y la capacitación del personal, son fundamentales para proteger la información crítica y asegurar el cumplimiento normativo, evitando riesgos futuros para la organización.

Situaciones detectadas

- Tráfico de Datos Inusual: Identificación de un aumento significativo en el tráfico hacia un servicio de almacenamiento en la nube.
- Acceso No Controlado a Información Sensible: Personal médico subiendo datos sin los protocolos de seguridad establecidos.
- Falta de Conciencia en Ciberseguridad: Desconocimiento general sobre las implicaciones de subir datos a la nube.
- Ausencia de Normativas Internas: Falta de una política clara sobre el uso de servicios en la nube y manejo de información confidencial.
- Vulnerabilidades en la Infraestructura de TI: Existencia de malware en equipos que puede ser aprovechado para comprometer la seguridad de la información.

Acciones para la Mitigación

- Prohibición del Uso de Servicios Públicos en la Nube: Establecer una normativa interna que prohíba la utilización de estos servicios para datos sensibles y diseñar reglas en el firewall para bloquear dicho tráfico.
- Implementación de una Nube Privada: Crear una infraestructura de nube privada con acceso restringido, asegurando que se cumplan las normativas de protección de datos.
- Programa de Formación en Ciberseguridad: Desarrollar e implementar un programa de capacitación para el personal médico y administrativo sobre las mejores prácticas en el manejo de datos y ciberseguridad.
- Auditorías Periódicas: Realizar revisiones regulares del tráfico de red y auditorías de seguridad para detectar cualquier anomalía de manera proactiva.
- Establecimiento de Protocolos de Seguridad: Definir y documentar procedimientos claros par

Informe de auditoría

Cuestionario de Auditoría de Seguridad de la Información

Auditoría de Seguridad de la Información					
N°	**Preguntas**	**Sí**	**No**	**N/A**	**Comentarios**
1	¿El personal médico está informado sobre las políticas de seguridad de la información?		X		Se identificó falta de comunicación sobre las políticas de seguridad, lo que contribuyó al uso indebido de servicios en la nube.
2	¿Se realizan auditorías periódicas sobre el uso de servicios en la nube?		X		No se habían programado auditorías regulares, lo que permitió que se desarrollaran prácticas inseguras.
3	¿Existen protocolos establecidos para el manejo de datos sensibles?		X		La ausencia de protocolos claros incrementa el riesgo de fuga de información.
4	¿Se ha capacitado al personal sobre los riesgos de usar servicios de almacenamiento en la nube?		X		La capacitación es esencial para concienciar sobre la seguridad de los datos.
5	¿Se han implementado medidas de control para monitorear el tráfico de datos sensibles?	x			Se están llevando a cabo esfuerzos de monitoreo, aunque con áreas de mejora en la implementación de políticas.

Lista de Chequeo de Auditoría de Seguridad de la Información

Preguntas	Sí	No	Anotación
1. Se ha establecido una política de uso de servicios en la nube.		X	No se ha definido formalmente una política clara al respecto.
2. Se controla el acceso a información sensible de forma adecuada.		X	Los accesos no están suficientemente restringidos.
3. El personal ha recibido formación en ciberseguridad.		X	No se ha realizado una capacitación formal.
4. Se realizan revisiones del tráfico de datos en la red corporativa.	X		Aunque se realiza monitoreo, falta un enfoque más sistemático.
5. Existe un protocolo para la gestión de incidentes de seguridad.		X	Carecemos de un protocolo formal para abordar incidentes.
6. Se han implementado medidas de protección en la infraestructura TI.	X		Hay ciertas medidas, pero requieren actualizaciones.
7. Se documentan los accesos y actividades en servicios de almacenamiento.		X	No existe un registro adecuado de estas actividades.
8. Se ha informado al personal sobre las consecuencias de incumplir las políticas de seguridad.		X	La falta de información puede contribuir a riesgos de seguridad.

Situaciones relevantes

Situación 1	Uso No Autorizado de Servicios en la Nube: Se identificó que el personal médico está utilizando un servicio de almacenamiento en la nube para gestionar historias clínicas y resultados de pruebas, lo que expone la información confidencial de los pacientes a riesgos de seguridad y posibles incumplimientos de la LOPD.
Situación 2	Falta de Políticas de Seguridad: No existen políticas claras y formalmente establecidas sobre el uso de servicios en la nube y la gestión de datos sensibles, lo que incrementa el riesgo de violaciones de seguridad y la exposición de información confidencial.
Situación 3	Desconocimiento de Riesgos: El personal médico no está adecuadamente capacitado sobre los riesgos asociados al uso de servicios de almacenamiento en la nube, lo que contribuye a prácticas inseguras en el manejo de datos sensibles.

Situaciones encontradas

Situación 1	Tráfico de Datos Inusual: Se detectó un aumento significativo en el tráfico de datos hacia un servicio de almacenamiento en la nube, lo que indica un posible uso indebido de estos servicios por parte del personal.
Si8tuación 2	Acceso No Controlado a Datos Sensibles: Se observó que los médicos suben información confidencial sin las medidas de seguridad adecuadas, lo que pone en riesgo la privacidad de los pacientes.
Situación 3	Ausencia de Auditorías Regulares: No se están realizando auditorías periódicas para monitorear el uso de servicios en la nube, lo que impide la identificación temprana de prácticas inseguras.
Situación 4	Falta de Conciencia en Ciberseguridad: Se evidenció una falta de formación y concienciación en ciberseguridad entre el personal, lo que resulta en un uso

	inadecuado de tecnologías y un mayor riesgo de incidentes.
Situación 5	Vulnerabilidades en la Infraestructura de TI: Se encontraron equipos con malware en la red, lo que podría ser aprovechado para comprometer la seguridad de la información sensible.

Conclusión

La auditoría realizada en el grupo de hospitales privados ha permitido identificar varios aspectos críticos en el manejo de la información confidencial de los pacientes, especialmente en lo que respecta al uso de servicios de almacenamiento en la nube. Uno de los hallazgos más significativos fue el uso no autorizado de estas plataformas por parte del personal médico, motivado por la necesidad de optimizar la atención al paciente.

Asimismo, se destacó la falta de políticas claras y formalmente establecidas que regulen el uso de tecnologías de la información y la gestión de datos sensibles. La ausencia de estas normativas incrementa la posibilidad de que se realicen acciones que comprometan la seguridad de la información.

Además, el personal médico no había recibido la capacitación adecuada en ciberseguridad, lo que resultó en una escasa concienciación sobre los riesgos asociados al uso inadecuado de servicios de almacenamiento en la nube. Sin dejar de lado que la carencia de revisiones sistemáticas del tráfico de datos y el acceso a información sensible contribuyeron a un ambiente donde las vulnerabilidades pasaron desapercibidas, poniendo en riesgo la integridad de la información corporativa y la privacidad de los pacientes.

En conclusión, la auditoría ha subrayado la importancia de establecer un equilibrio entre la funcionalidad y la seguridad en el ámbito de la salud. Se recomienda que la organización implemente política claras sobre el uso de servicios en la nube, realice auditorías regulares, y brinde capacitación continua al personal en ciberseguridad. Estos pasos no solo ayudarán a mitigar los riesgos detectados, sino que también fomentarán una cultura de seguridad en el manejo de información confidencial, garantizando así una atención al paciente más segura y eficiente.

Referencia

INCIBE. (2015, 27 de octubre). *¿Cómo identificar una fuga de información? Monitoriza y analiza el trafico* [Video]. YouTube. https://www.youtube.com/watch?v=W4bpnk8-W_4