UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

Y CIENCIAS DE LA COMPUTACIÓN

Proyecto de implementación de la norma ISO 27001 con un enfoque en la encriptación de datos para la Casa de Cobros de Cartera Morosa

Seguridad y Auditoria de sistemas de información "A" Villa Nueva

Gerardo Daniel Corzo Figueroa

5190-13-10914 Grupo "D"

Guatemala, 15/08/2023

Índice

1. Modelo de Negocio 4

1.1 Planteamiento del Problema 4

1.2 Objetivos (Generales y Específicos) 4

1.3 Planificación de solución 4

2. Modelo de Seguridad 5

2.1 Planteamiento del Proyecto de Seguridad 5

2.2 Viabilidad Técnica y Operativa de la solución 5

2.2.1 Viabilidad Operativa de la Solución: 5

2.2.2 Viabilidad Técnica de la Solución: 6

2.3 Contexto técnico de trabajo o área donde aplicará el modelo de seguridad 7

2.3.1 Hardware 7

2.3.2 Software 7

2.3.3 Metodología, estándar, etc. 7

2.4 Otros recursos y consideraciones 8

2.5 Plan de ejecución 8

3. Auditoría 10

3.1 Puntos de evaluación de Proyecto de Seguridad 10

Conclusiones: 11

Introducción

En el entorno empresarial actual, la protección de la información sensible es esencial para garantizar la confidencialidad y la privacidad de los datos. En este proyecto de curso, se abordará la implementación de un sistema de seguridad basado en la norma ISO 27001 con un enfoque en la encriptación de datos, específicamente diseñado para una Casa de Cobros de Cartera Morosa. La necesidad de esta iniciativa surge de la creciente preocupación por la seguridad de la información financiera y personal de los deudores, con el objetivo de fortalecer la confianza y garantizar la integridad de los datos durante el proceso de recuperación de deudas.

1. Modelo de Negocio

1.1 Planteamiento del Problema

La Casa de Cobros de Cartera Morosa enfrenta el desafío de asegurar la protección adecuada de la información financiera y personal de los deudores. La falta de medidas de seguridad sólidas podría resultar en brechas de seguridad, pérdida de confianza por parte de los deudores y posibles sanciones legales por incumplimiento de regulaciones de privacidad de datos.

1.2 Objetivos (Generales y Específicos)

Objetivo General: Implementar un sistema de gestión de seguridad de la información basado en ISO 27001, centrado en la encriptación de datos, para proteger la información financiera y personal de los deudores en la Casa de Cobros de Cartera Morosa.

Objetivos Específicos:

1. Identificar y clasificar los activos de información críticos que requieren encriptación.
2. Diseñar e implementar políticas de encriptación de datos en diferentes escenarios.
3. Evaluar y seleccionar soluciones de encriptación adecuadas para la organización en su sistema de gestión de documentación.
4. Capacitar al personal en prácticas de encriptación y seguridad de datos.
5. Realizar auditorías internas para garantizar la conformidad con ISO 27001.

1.3 Planificación de solución

La solución propuesta involucra la implementación de un sistema de gestión de seguridad de la información basado en ISO 27001, con un enfoque en la encriptación de datos. El proceso incluirá la identificación de activos críticos, la definición de políticas, la selección de soluciones tecnológicas, la capacitación del personal y la realización de auditorías internas para garantizar la eficacia y el cumplimiento.

2. Modelo de Seguridad

2.1 Planteamiento del Proyecto de Seguridad

El proyecto busca asegurar la protección de la información sensible de los deudores a través de la implementación de un sistema de gestión de seguridad de la información basado en ISO 27001. Se enfocará en la encriptación de datos como medida fundamental para salvaguardar la confidencialidad de la información.

2.2 Viabilidad Técnica y Operativa de la solución

2.2.1 Viabilidad Operativa de la Solución:

La viabilidad operativa se refiere a la capacidad de implementar y mantener la solución propuesta en el entorno de la Casa de Cobros de Cartera Morosa de manera efectiva y sin interrupciones en sus operaciones diarias. Aquí están los aspectos clave de la viabilidad operativa:

1. **Recursos Humanos:** Evaluar si la organización tiene personal capacitado o si puede adquirir el conocimiento necesario para implementar y gestionar la encriptación de datos. Además, considerar la disponibilidad de personal para la gestión continua y la realización de auditorías internas.
2. **Capacidad de Integración:** Asegurarse de que las soluciones de encriptación se integren adecuadamente con los sistemas y aplicaciones existentes en la organización. Esto garantiza que no haya interrupciones en los procesos operativos y que la información fluya de manera fluida.
3. **Procesos Operativos:** Evaluar cómo las medidas de seguridad propuestas se ajustarán a los flujos de trabajo actuales. Es importante que las políticas de encriptación no ralenticen los procesos ni creen obstáculos innecesarios.
4. **Formación y Concientización:** La viabilidad operativa incluye la capacidad de brindar una formación efectiva a los empleados sobre las nuevas políticas y prácticas de seguridad. La

concienciación es fundamental para asegurar que todos los miembros del equipo comprendan la importancia de la encriptación y cómo aplicarla correctamente.

2.2.2 Viabilidad Técnica de la Solución:

La viabilidad técnica se refiere a la posibilidad de implementar las soluciones tecnológicas necesarias para cumplir con los objetivos de seguridad y encriptación de datos. Aquí están los aspectos clave de la viabilidad técnica:

1. **Infraestructura Tecnológica:** Evaluar si la infraestructura existente es compatible con las soluciones de encriptación propuestas. Esto incluye servidores, almacenamiento, redes y cualquier otra tecnología involucrada en el proceso de gestión de datos.
2. **Selección de Soluciones:** Evaluar la disponibilidad de soluciones tecnológicas que cumplan con los requisitos de encriptación y seguridad de la información. Esto podría incluir herramientas de cifrado de datos, soluciones de protección de correo electrónico, sistemas de autenticación, etc.
3. **Rendimiento:** Asegurarse de que las soluciones tecnológicas seleccionadas sean capaces de manejar la carga de trabajo actual y futura. La solución debe ser escalable para acomodar el crecimiento de la organización y la cantidad de datos.
4. **Compatibilidad:** Verificar la compatibilidad entre las soluciones de encriptación y los sistemas operativos, aplicaciones y plataformas utilizados en la organización. La falta de compatibilidad podría generar problemas de implementación y rendimiento.
5. **Mantenimiento y Actualización:** Evaluar la facilidad de mantenimiento y actualización de las soluciones de encriptación. Esto incluye la capacidad de aplicar parches de seguridad y actualizaciones sin afectar negativamente las operaciones.

2.3 Contexto técnico de trabajo o área donde aplicará el modelo de seguridad

2.3.1 Hardware

En el contexto de implementar medidas de seguridad de la información basadas en la encriptación de datos, el hardware desempeña un papel crucial en asegurar la integridad y confidencialidad de la información. Algunos aspectos relevantes incluyen:

- Servidores seguros: La organización debe contar con servidores robustos y seguros para almacenar y procesar datos encriptados. Estos servidores deben cumplir con estándares de seguridad y contar con medidas de protección física, como sistemas de acceso restringido y protección contra incendios.
- Dispositivos de almacenamiento cifrado: Para proteger los datos almacenados en dispositivos físicos, es recomendable utilizar unidades de almacenamiento cifradas, como discos duros y unidades USB encriptadas. Esto garantiza que, en caso de pérdida o robo, los datos sigan estando protegidos.

2.3.2 Software

El software desempeña un papel fundamental en la implementación de la encriptación de datos y la gestión de la seguridad de la información. Aquí están algunos aspectos clave:

- Soluciones de encriptación: Se pueden implementar soluciones de encriptación de datos para bases de datos, archivos y comunicaciones. Estas soluciones garantizan que los datos estén encriptados en reposo y en tránsito, lo que reduce el riesgo de acceso no autorizado.
- Sistemas de gestión de claves: Los sistemas de gestión de claves son esenciales para administrar y proteger las claves de encriptación. Estos sistemas aseguran que las claves se generen, almacenen y compartan de manera segura.
- Herramientas de monitoreo y detección: Las soluciones de seguridad también pueden incluir herramientas de monitoreo que permitan detectar actividades sospechosas o no autorizadas en tiempo real, lo que ayuda a prevenir incidentes de seguridad.

2.3.3 Metodología, estándar, etc.

La implementación de la seguridad de la información basada en la encriptación de datos se guiará por la norma ISO 27001 y otros estándares y buenas prácticas de la industria, como:

- ISO 27002: Proporciona un conjunto de controles y directrices específicas para la implementación de medidas de seguridad de la información.

- NIST SP 800-53: Define controles de seguridad recomendados para sistemas de información federales en los Estados Unidos.
- Cifrado de extremo a extremo: Esta metodología se utiliza para proteger las comunicaciones entre dos puntos, asegurando que solo los participantes autorizados puedan descifrar el contenido.

2.4 Otros recursos y consideraciones

- Recursos financieros: La implementación exitosa de medidas de seguridad de la información requiere una inversión en hardware, software y capacitación. Asegúrate de tener un presupuesto adecuado para cubrir estos costos.
- Recursos humanos: Necesitarás personal capacitado en seguridad de la información para implementar y administrar las soluciones de encriptación. Esto puede incluir expertos en ciberseguridad, administradores de sistemas y personal de TI.
- Colaboración interdepartamental: La seguridad de la información es responsabilidad de todos en la organización. Asegúrate de involucrar a todas las áreas relevantes, desde TI hasta recursos humanos y legal, para garantizar la adopción exitosa de las medidas de seguridad.
- Actualización continua: La seguridad de la información es un proceso en constante evolución. Debes estar preparado para mantener y actualizar regularmente tus medidas de seguridad para enfrentar nuevas amenazas y desafíos.
- Cumplimiento legal y regulatorio: Asegurarse de conocer y cumplir con las leyes y regulaciones relacionadas con la privacidad de datos y la seguridad de la información en la jurisdicción.

2.5 Plan de ejecución

La implementación exitosa de medidas de seguridad de la información basadas en la encriptación de datos requiere una planificación meticulosa y una ejecución ordenada. A continuación, se desglosan las etapas del plan de ejecución, desde el diseño hasta la implementación:

Etapa 1: Diseño

En esta etapa, se establecen los fundamentos para la implementación de medidas de seguridad de la información centradas en la encriptación de datos.

1. **Identificación de activos críticos:** Realizar un inventario de los activos de información críticos que requieren encriptación, como bases de datos de clientes, datos financieros y registros de deudas.
2. **Definición de políticas de encriptación:** Diseñar políticas claras y específicas para la encriptación de datos en diferentes contextos, como almacenamiento, transmisión y comunicaciones.
3. **Diseño de soluciones de encriptación:** Seleccionar las soluciones de encriptación adecuadas para cumplir con las políticas definidas. Esto puede incluir soluciones de encriptación de disco, encriptación de bases de datos y encriptación de comunicaciones.

Etapa 2: Desarrollo

En esta fase, se lleva a cabo la implementación práctica de las medidas de seguridad basadas en la encriptación de datos.

1. **Configuración de soluciones de encriptación:** Configurar las soluciones de encriptación seleccionadas según los requisitos de seguridad y las políticas definidas.
2. **Desarrollo de procesos de encriptación:** Crear flujos de trabajo y procesos para la encriptación de datos en diferentes escenarios, como el almacenamiento de información y la transmisión de datos.
3. **Integración con sistemas existentes:** Asegurarse de que las soluciones de encriptación se integren de manera efectiva con los sistemas y aplicaciones existentes en la organización.

Etapa 3: Pruebas

En esta etapa, se verifican y validan las soluciones de encriptación implementadas antes de pasar a la fase de implementación completa.

1. **Pruebas de funcionalidad:** Verificar que las soluciones de encriptación funcionen según lo previsto en diferentes escenarios y contextos.
2. **Pruebas de rendimiento:** Evaluar el impacto de la encriptación en el rendimiento de los sistemas y aplicaciones para asegurarse de que no haya degradación significativa.
3. **Pruebas de recuperación de datos:** Realizar pruebas de recuperación de datos en caso de fallos o incidentes para garantizar que la encriptación no afecte la capacidad de recuperación.

Etapa 4: Implementación

En esta fase, se implementan las medidas de seguridad de la información en toda la organización.

1. **Capacitación del personal:** Proporcionar capacitación a los empleados sobre las políticas de encriptación, prácticas seguras y cómo usar las soluciones de encriptación en su trabajo diario.
2. **Comunicación interna:** Comunicar de manera efectiva a todos los empleados sobre la implementación de las medidas de seguridad y la importancia de la encriptación de datos.
3. **Implementación escalonada:** Implementar las soluciones de encriptación de manera escalonada, comenzando por los activos más críticos y expandiéndose gradualmente a otros sistemas y áreas.

3. Auditoría

3.1 Puntos de evaluación de Proyecto de Seguridad

1. Cumplimiento de ISO 27001: Verificar si las prácticas y medidas implementadas cumplen con los requisitos de la norma.
2. Eficacia de la encriptación: Evaluar si la encriptación de datos está funcionando según lo previsto.
3. Capacitación del personal: Revisar si el personal está al tanto de las políticas y prácticas de seguridad.
4. Gestión de riesgos: Evaluar la identificación y mitigación de riesgos de seguridad.
5. Conformidad legal: Verificar el cumplimiento de leyes y regulaciones de privacidad de datos.

Conclusiones:

La implementación de medidas de seguridad de la información basadas en la encriptación de datos, siguiendo el marco de trabajo de ISO 27001, ha demostrado ser esencial para garantizar la protección de la información financiera y personal en una Casa de Cobros de Cartera Morosa. A través de un enfoque cuidadoso en el diseño, desarrollo, pruebas e implementación, se ha logrado fortalecer la seguridad y la confidencialidad de los datos, reduciendo el riesgo de brechas de seguridad y mejorando la confianza tanto de los deudores como de los clientes. El compromiso de la alta dirección, la colaboración interdepartamental y el seguimiento constante han sido fundamentales para el éxito de esta iniciativa.

Glosario:

- **Encriptación:** Proceso de transformar información en un formato incomprensible para proteger la confidencialidad.
- **ISO 27001:** Norma global para la gestión de seguridad de la información.
- **Activos de información:** Datos valiosos para la organización, como información financiera y personal.
- **Seguridad de la información:** Medidas para proteger datos contra amenazas.
- **Normas y regulaciones:** Directrices legales y estándares de seguridad.
- **Sistema de gestión de claves:** Infraestructura para administrar claves de encriptación.
- **Flujo de trabajo:** Pasos secuenciales para ejecutar una tarea.
- **Cumplimiento legal:** Adhesión a leyes y regulaciones.
- **Privacidad de datos:** Protección de información personal.
- **Políticas de encriptación:** Directrices para uso seguro de encriptación.
- **Ciberseguridad:** Protección contra ciberataques y amenazas digitales.
- **Confidencialidad:** Protección de información sensible.
- **Integridad:** Mantenimiento de precisión y confiabilidad de los datos.
- **Disponibilidad:** Acceso oportuno y confiable a los datos.
- **Vulnerabilidad:** Debilidad que puede ser explotada por amenazas.
- **Riesgo de seguridad:** Posibilidad de pérdida debido a amenazas.
- **Auditoría de seguridad:** Evaluación de medidas de seguridad.
- **Autenticación:** Verificación de identidad de usuario.
- **Autorización:** Concesión de permisos a usuarios.
- **Cifrado simétrico:** Uso de una clave única para encriptar y desencriptar.
- **Cifrado asimétrico:** Uso de pares de claves pública y privada para encriptar.
- **Firewall:** Barrera de seguridad para proteger redes.
- **Ataque de phishing:** Engaño para obtener información confidencial.
- **Política de seguridad:** Conjunto de reglas y directrices de seguridad.
- **Incidente de seguridad:** Evento que amenaza la seguridad de la información.
- **Control de acceso:** Restricción de acceso a recursos.
- **Registros de auditoría:** Historial de actividades de seguridad.
- **Gestión de incidentes:** Manejo de problemas de seguridad.

- **Biometría:** Uso de características físicas para autenticación.
- **Detección de intrusiones:** Monitoreo y detección de actividades no autorizadas.
- **Respuesta a incidentes:** Acciones tomadas ante incidentes de seguridad.
- **Hackeo ético:** Pruebas de seguridad para identificar vulnerabilidades.
- **Multifactorial:** Autenticación con varios métodos.
- **Virus informático:** Software malicioso que se propaga.
- **Ransomware:** Software malicioso que bloquea acceso y exige rescate.
- **Token de seguridad:** Dispositivo para autenticación.
- **Vulnerabilidad zero-day:** Vulnerabilidad desconocida y no parcheada.
- **Ciberinteligencia:** Recopilación y análisis de información sobre ciberamenazas.