Ingeniería
en Desarrollo de Software

Actividad | # | proceso de control de cambios

Seminario de titulación

Ingeniería en Desarrollo de Software

TUTOR: Elizabeth Guevara Roa

ALUMNO: Gabriel German Verdugo Solís

FECHA: 20 de julio del 2025

ÍNDICE

INTRODUCCION 3

DESCRIPCION 3

JUSTIFICACION 4

DESARROLLO 5

- Problemáticas 5
- Objetivos 5
- Soluciones 6
- Resultados 7

CONCLUSIÓN 9

REFERENCIAS 10

INTRODUCCION

En la actualidad, la seguridad de la información es un aspecto esencial en cualquier empresa que busque proteger sus activos y datos frente a amenazas internas y externas. En este sentido, la norma internacional ISO/IEC 27001 proporciona un marco para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). La empresa WorldBest Tech, en su proceso de creación y desarrollo, se enfrenta a diversas problemáticas que deben ser atendidas si desean asegurar sus procesos, la calidad de sus servicios y la protección de la información. Este trabajo tiene como objetivo analizar estas dificultades y proponer soluciones prácticas alineadas con dicha norma. A través de la evaluación de problemas específicos —como la falta de infraestructura adecuada, desconocimiento en gestión de activos, y la necesidad de control de accesos— se plantearán acciones concretas para corregir y optimizar la seguridad en la organización. Esta propuesta, además de estar basada en estándares internacionales, permitirá sentar bases sólidas para el crecimiento seguro de la empresa.

DESCRIPCION

El caso presentado gira en torno a la creación de una empresa llamada WorldBest Tech, dirigida por Gerardo y Wanda, quienes desean emprender en el sector tecnológico. Sin embargo, se enfrentan a una serie de problemáticas fundamentales que comprometen la operatividad, seguridad y crecimiento sostenible de su futura empresa. Entre las principales dificultades destacan la falta de conocimientos sobre el tipo de personal que deben contratar y la capacitación adecuada para garantizar procesos seguros. Asimismo, el edificio donde planean operar no cuenta con condiciones apropiadas para alojar servidores y equipos de cómputo, lo que representa un riesgo físico importante.

Otro punto crítico es la ausencia de un sistema para gestionar los activos tecnológicos,

como hardware y software, lo que puede derivar en pérdida de información o mal uso de recursos. Además, no existe un control de acceso a información sensible ni una estrategia clara para proteger la confidencialidad e integridad en el desarrollo de software. A través de este trabajo se analizarán y propondrán soluciones alineadas a la norma ISO/IEC 27001, permitiendo establecer un Sistema de Gestión de Seguridad de la Información (SGSI) que atienda estas necesidades de manera estructurada y eficiente.

JUSTIFICACION

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 es fundamental para garantizar que la empresa WorldBest Tech funcione de forma segura, profesional y conforme a los estándares internacionales. Esta norma no solo se centra en la tecnología, sino también en la gestión organizacional, abarcando desde la capacitación del personal hasta el control de accesos y la seguridad en los procesos de desarrollo. En el contexto actual, donde la información es uno de los activos más valiosos de cualquier empresa, es indispensable contar con políticas, controles y procedimientos documentados que aseguren su confidencialidad, integridad y disponibilidad.

La adopción de estas prácticas permitirá a WorldBest Tech minimizar riesgos operativos, evitar pérdidas de información y prevenir posibles ataques informáticos o errores humanos. Además, cumplir con la norma mejora la reputación de la empresa, facilita la obtención de certificaciones futuras, y abre puertas a oportunidades comerciales con empresas que exigen estándares de seguridad. Por lo tanto, esta solución no solo es necesaria, sino estratégica para el éxito a corto y largo plazo del emprendimiento

DESARROLLO

- **Problemáticas**

Problemática 1: personal y capacitación.

Los fundadores no tienen claridad sobre el tipo de personal necesario ni qué capacitación brindar para asegurar que se cumplan los estándares de seguridad.

Problemática 2: infraestructura inadecuada.

El edificio carece de condiciones físicas para alojar equipos tecnológicos sensibles como servidores o estaciones de trabajo.

Problemática 3: gestión de activos e información.

No existe una metodología para gestionar y clasificar los activos físicos y digitales.

Problemática 4: control de acceso.

No está definido quién puede acceder a la información sensible ni cómo se gestiona ese acceso.

Problemática 5: seguridad en el desarrollo del software.

No existen procesos para asegurar la seguridad e integridad de los productos de software desarrollados.

- **Objetivos**

Problemática 1: personal y capacitación.

1. Identificar perfiles profesionales clave para la operación tecnológica segura.
2. Establecer un plan de capacitación continua para empleados.
3. Asegurar la concienciación de todos los colaboradores respecto a la seguridad de la información.

Problemática 2: infraestructura inadecuada.

1. Evaluar los riesgos físicos que pueden afectar la infraestructura.
2. Adecuar el espacio conforme a los requisitos físicos de la norma ISO.
3. Proteger físicamente los equipos críticos.

Problemática 3: gestión de activos e información.

1. Crear un inventario completo de activos.
2. Asignar responsables de cada activo.
3. Clasificar la información según su criticidad.

Problemática 4: control de acceso.

1. Definir niveles de acceso por rol.
2. Implementar mecanismos de autenticación segura.
3. Registrar y auditar accesos a sistemas.

Problemática 5: seguridad en el desarrollo del software.

1. Establecer un ciclo seguro de desarrollo de software (SDLC).
2. Implementar herramientas de análisis de código.
3. Asegurar que la información usada en desarrollo esté protegida.

- **Soluciones**

Problemática 1: personal y capacitación.

- Contratar personal certificado en ciberseguridad y gestión de TI.
- Definir funciones y responsabilidades conforme a ISO 27001.
- Brindar formación continua mediante plataformas.
- Crear una política de capacitación anual documentada.

Problemática 2: infraestructura inadecuada.

- Realizar una auditoría de seguridad física.
- Instalar sistemas de climatización, control de incendios y energía estable.
- Implementar acceso físico restringido con tarjetas o biometría.

Problemática 3: gestión de activos e información.

- Implementar una base de datos de activos.
- Clasificar los activos como confidenciales, internos o públicos.
- Revisar y actualizar el inventario periódicamente.

Problemática 4: control de acceso.

- Crear una política de control de acceso basada en roles.
- Instalar un sistema de control de acceso.
- Auditar accesos cada mes mediante registros de logs.

Problemática 5: seguridad en el desarrollo del software.

1. Adoptar el modelo DevSecOps.
2. Usar herramientas como GitHub + SonarQube + OWASP ZAP.
3. Aplicar cifrado en los datos sensibles.
4. Definir una política de control de cambios.

- **Resultados**

Problemática 1: personal y capacitación.

- Personal competente y consciente de los riesgos.
- Reducción de errores humanos.
- Cumplimiento de las cláusulas de la norma ISO/IEC 27001.

Problemática 2: infraestructura inadecuada.

- Infraestructura segura y funcional.
- Disminución de riesgos físicos como sobrecalentamiento o intrusiones.
- Protección de los equipos tecnológicos.

Problemática 3: gestión de activos e información.

- Mayor control sobre el uso de activos.
- Disminución de pérdidas o uso indebido.
- Cumplimiento de los controles de ISO 27001.

Problemática 4: control de acceso.

- Protección contra accesos no autorizados.
- Trazabilidad en los accesos.
- Mejor gestión de identidades.

Problemática 5: seguridad en el desarrollo del software.

- Software más seguro y confiable.
- Reducción de vulnerabilidades.
- Mejora en la calidad del producto final.

CONCLUSIÓN

La realización de esta actividad permitió comprender la importancia de aplicar normas internacionales como la ISO/IEC 27001 en el diseño, desarrollo y operación de una empresa tecnológica como WorldBest Tech. A través del análisis de cinco problemáticas clave, se identificaron soluciones prácticas y estructuradas que no solo corrigen fallas operativas, sino que también previenen riesgos a futuro. Esta norma ofrece un marco sólido para proteger los activos de información, garantizar la confidencialidad, integridad y disponibilidad de los datos, y establecer controles tanto físicos como digitales.

Desde una perspectiva laboral, implementar un Sistema de Gestión de Seguridad de la Información (SGSI) incrementa la eficiencia de los procesos, mejora la reputación de la empresa y permite cumplir con regulaciones vigentes. En lo personal, conocer y aplicar estos estándares aporta habilidades esenciales para cualquier profesional del área de tecnología, administración o seguridad informática. Fortalecer una empresa desde sus cimientos con políticas claras y buenas prácticas asegura un crecimiento ordenado, confiable y competitivo en el mercado actual.

REFERENCIAS

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001

OWASP Foundation. (2024). *Secure Software Development Lifecycle Project*. https://owasp.org/www-project-secure-software-development-lifecycle/

Teclib'. (2024). *GLPI ITSM & Asset Management Software*. https://glpi-project.org/

Lansweeper. (2024). *IT Asset Management Software*. https://www.lansweeper.com/

Microsoft. (2025). *Introduction to identity and access management*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/fundamentals/identity-access-management-overview

Udemy. (2025). *ISO/IEC 27001 courses*. https://www.udemy.com/topic/iso-27001/

AENOR. (2022). *UNE-EN ISO/IEC 27001:2023. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (ISO/IEC 27001:2022, IDT)*. Asociación Española de Normalización. https://www.aenor.com/normas-y-libros/buscador-de-normas/une?c=N0061322