La implementación de la norma ISO 27001 en ByeWorld: guía de procedimiento

**1. Evaluación de riesgos:**

**Identificación de activos:**

* Clasificación de información.
* Dónde se encuentra la información (física, digital, etc.).
* Los responsables de la información.

**Evaluación de amenazas y vulnerabilidades:**

* Análisis del entorno interno y externo
* Identificar amenazas potenciales (ciberataques, errores humanos, etc.).

**Evaluación de vulnerabilidades de sistemas y procesos.**

* Valoración de riesgos:
* Calcular los efectos y las probabilidades de cada riesgo.
* Priorizar los riesgos en función de su criticidad.

**2. Regulaciones de Seguridad:**

**Política general de seguridad de la información:**

* Declaración de compromiso de la dirección con la seguridad de la información.
* Los objetivos y principios de la seguridad se definen.

**Políticas específicas:**

* control del acceso a la información.
* administrar los activos de información.
* Seguridad operativa.
* Seguridad de la comunicación.
* cumplimiento de las regulaciones y leyes.

**3.Los objetivos y metas de seguridad se definen a través de la planificación**.

**crear planes para lograr los objetivos.**

I**mplementación y operación:**

* Aplicar las políticas y controles de seguridad.
* El personal debe recibir capacitación en seguridad de la información.

**Evaluación y monitoreo:**

* vigilar el cumplimiento de las políticas y controles.
* Evaluar la eficacia del SGSI para la seguridad.

**Revisión y mejora:**

* la SGSI se revisa periódicamente para encontrar oportunidades de mejora.
* tomar medidas preventivas y correctivas.

**4. Ejecutar los controles:**

**Los controles de acceso requieren la autorización y la autenticación de los usuarios.**

* Control de acceso a recursos digitales y físicos.
* Los firewalls, los antivirus y los sistemas de detección de intrusiones son controles de seguridad perimetral.

**Controles de seguridad de datos:**

* Encriptación, copia de seguridad y control de versiones.
* Controles de seguridad de aplicaciones: creación de aplicaciones seguras y pruebas de seguridad.
* Los controles de seguridad operacional incluyen la gestión de incidentes, los planes de contingencia y la recuperación de desastres.

**5. Observación y Revisión:**

**Observación de los controles:**

* verificar que los controles funcionen correctamente.
* detectar fallas potenciales.
* La revisión del sistema de gestión (SGSI) es una evaluación periódica del sistema de gestión.
* Identificar oportunidades para mejorar.

**6. Continúa mejorando:**

**Ciclo de desarrollo continuo PHVA:**

* Planear, realizar, verificar y actuar.
* tomar medidas preventivas y correctivas.
* La actualización del SGSI se refiere a la adaptación del sistema a los cambios que puedan surgir en el entorno.
* Incorporar mejores prácticas y nuevas tecnologías.

**Recursos**

**Norma ISO 27001**: https://www.iso.org/standard/27001

**Guía ISO 27002**: https://www.iso.org/standard/75652.html

**Organismos de certificación:** <https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion>

**Recomendaciones**

* Involucrar a la alta dirección y a todo el personal en la implementación del SGSI.
* Asignar los recursos humanos y financieros adecuados para la implementación.
* Si se requiere ayuda, seleccione un consultor con experiencia en ISO 27001.
* Mantenga el SGSI documentado y accesible.
* Enseñar a todo el personal la importancia de la seguridad de la información.

**Los beneficios de seguir la norma ISO 27001 son los siguientes:**

* Mejora la seguridad y protección de los datos.
* Disminuir la probabilidad de ocurrir incidentes de seguridad.
* Aumenta la confianza de los socios y clientes.
* Mejora la reputación y la imagen de la empresa.
* Demuestra que la empresa está comprometida con la seguridad de la información