UNIVERSIDAD BERNARDO O'HIGGINS

FACULTAD DE INGENIERÍA, CIENCIAS Y TECNOLOGÍA

Carrera de Ingeniería en Informática

Curso Diseño y Auditoría en Ciberseguridad

Profesor:

Miguel Castillo

Alumno:

Aldo Fernando Hernández Tamez

Informe ISO 27001

La ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización, esta se encarga de establecer estándares para productos a nivel mundial. La familia de normas ISO 27000 tiene como función proporcionar un marco para la gestión de la seguridad de la información (SGSI).

Principalmente, la norma ISO 27001 especifica los requisitos genéricos aplicables para cualquier organización para el establecimiento, implementación, mantenimiento y mejora continua de un conjunto de políticas de administración de la información llamado sistema de gestión de la seguridad de la información (SGSI) en el contexto de dicha organización. Además, incluye los requisitos para la apreciación y tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización junto con la definición de procedimientos para gestionarlos.

Antes de implementar un SGSI, la organización debe:

- Contexto y alcance
    - Entender su contexto externo e interno que pueda afectar su capacidad para lograr sus resultados previstos.
    - Determinar las partes interesadas y sus requisitos relevantes.
    - Definir los límites y la aplicabilidad del sistema para establecer su alcance.
- Liderazgo y compromiso
    - Asegurar la integración de los requisitos del sistema en los procesos de la organización.
    - Establecer una política de seguridad de la información adecuada al propósito de la organización que cumpla con los requisitos aplicables e incluya objetivos de seguridad de la información (o proporcione un marco de referencia para establecerlos).
    - Asignar responsabilidad y autoridad para asegurar que el sistema de la información es conforme con la Norma 27001.

- Planificación y gestión de riesgos
    - Identificar y evaluar los riesgos relacionados con la seguridad de la información.
    - Definir y efectuar un proceso de tratamiento de los riesgos.
    - Establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

  La norma sugiere u obliga a la organización implementar:

- Contexto y Liderazgo
    - Límites y aplicabilidad del sistema para establecer su alcance.
    - Asegurar el establecimiento de la política y objetivos de seguridad de la información junto con los recursos necesarios para el sistema.
    - Que la política de seguridad de la información contenga el compromiso de cumplir con los requisitos aplicables a la seguridad de la información y un compromiso de mejora continua del sistema.
- Planificación
    - Conservar información documentada sobre los procesos llevados a cabo.
    - Establecer y mantener criterios sobre riesgos de seguridad.
    - Elaborar una "Declaración de Aplicabilidad" que contenga los controles necesarios con su justificación, si dichos controles están implementados o no y la justificación de cualquiera de los controles del Anexo A de la Norma.
    - Tener una métrica para los objetivos de seguridad de la información en las funciones y niveles pertinentes si es posible.
    - Planear cualquier cambio al sistema antes de implementarlo.
- Controles
    - Se sugieren 93 controles en diversas categorías: organizacionales, personas, infraestructura y tecnología.
    - No es necesaria la implementación de todos los controles debido a que dependen de la organización y sus objetivos, por lo que se consideran

sugerencias generales que deben adaptarse según las necesidades de cada organización.

En conclusión, la Norma ISO 27001 busca definir un marco de referencia para un sistema de gestión de la seguridad de la información a fin de garantizar el manejo seguro de la información dentro de una organización. Esta Norma deja en claro todas las responsabilidades que tiene la organización junto con la definición de sus alcances. Si bien esta Norma no es obligatoria, es de gran utilidad frente a otras alternativas debido a que establece una sólida referencia para un manejo confiable de la información.