Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

MÓDULO I

INTERPRETACIÓN DE LA NORMA ISO 27001

CLASE 01

Mg. Ing. Julio Pereyra Rosales


DIPLOMA DE ESPECIALIZACIÓN
IMPLEMENTADOR Y AUDITOR
SEGURIDAD DE LA INFORMACIÓN – ISO 27001
CONTINUIDAD DEL NEGOCIO – ISO 22301
MÓDULO I
INTERPRETACIÓN DE LA NORMA ISO 27001
INGRESAR
MÓDULO II
IMPLEMENTACIÓN DE LA NORMA ISO 27001
INGRESAR
MÓDULO III
INTERPRETACIÓN DE LA NORMA ISO 22301
INGRESAR
MÓDULO IV
IMPLEMENTACIÓN DE LA NORMA ISO 22301
INGRESAR
MÓDULO V
FORMACIÓN DE AUDITORES INTERNOS EN LAS NORMAS ISO 27001 E ISO 22301
INGRESAR

1.Alcance del sistema de gestión de seguridad de la información (SGSI)

1.Objeto y campo de aplicación

- Engaña a usuario para que pueda compartir información confidencial.
- DoS . Permite que un usuario no acceda a un recursos informático.
- MitM. Permite interceptar la comunicación entre dos parte.
- Engaña a los programas de antivirus básicos y se esconde de ellos.
- Limita el acceso a archivos o partes del sistema operativo.

- Software malicioso que puede dañar o robar información de un dispositivo.
- Se inyecta un código SQL malicioso en una aplicación.
- DDoS . Permite iterrumpir un servicio o sitio web.
- Permite al atacante el acceso simple a una máquina, lo que le permite robar datos
- Ingreso de contraseña de manera maliciosa.

1.Objeto y campo de aplicación

La norma ISO 27001:2022 proporciona:

- Una decisión estratégica para la organización.
- Confidecialidad, integridad y disponibilidad de la información mdiante el proceso de gestión de riesgos.
- Brinda confianza a las partes interesadas.
- Integración de los procesos de negocio.

1.Objeto y campo de aplicación

https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

1.Objeto y campo de aplicación

Ventajas de la norma ISO 27001:2022

- Reducción del impacto y de la ocurrencia de riesgos por su identificación previa
- Aumento de la confiabilidad respecto a la empresa, ya que los clientes saben que sus datos están seguros
- Mejor adaptación a cambios, ya que toda la información está documentada y la gestión optimizada
- Mejora de la organización interna
- Atención a estándares exigidos por clientes y por la ley
- Ganancia de ventaja competitiva en general.

1.Objeto y campo de aplicación

2.Normas para consulta

ISO 27002: 2022

Buenas practicas de seguridad de la información.

ISO 27003: 2017

Guía para implementar el sistema de gestión de seguridad de la información

ISO 31000: 2018

Gestión del riesgo.

ISO 27000:2018

Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

ISO 19011: 2018

Directrices para auditorías de sistemas de gestión

3.Términos y definiciones

3.1
Control de acceso
Medios para garantizar que el acceso a los activos está autorizado y restringido en función de la actividad empresarial y la seguridad

3.2
Ataque
Intentar destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado a un activo o hacer un uso no autorizado del mismo.

3.23
Gobernanza d la seguridad de la información
Sistema por ele cual las actividades de seguridad de la información de una organización se dirigen y controlan.

3.28
Seguridad de la información
Preservación de la confidencialidad, integridad y disponibilidad de la información.

3.29
Continuidad de la seguridad de la información
Procesos y procedimientos para garantizar la continuidad de las operacioes de seguridad de la información.

3.30
Evento sobre seguridad de la información
Aparición identificada de un estado del sistema, servicio o red que indique una posible violencia de la política de seguridad de información o un fallo de los controles , o una situación previamente desconocida que pueda ser relevante para la seguridad.

2.Gestión del contexto organizacional

4. Contexto de la organización

4.1 Comprensión de la organización y su contexto

La organización debe determinar :

- Administrativos.
- Marketing. / Comercial.
- Operaciones.
- Finanzas.
- Gestión Humana
- Tecnología.
- Innovación

Cuestiones internas

- Política.
- Económico.
- Social.
- Tecnológico.
- Medio ambiente
- Legal.

Cuestiones externas

Que sean pertinentes para su propósito y que afecten su capacidad para lograr los resultados deseado de su SGSI.

4. Contexto de la organización

4.2 Comprensión de las necesidades y expectativas de partes interesadas

La organización debe determinar :

Partes interesadas que son pertinentes al SGSI.

- Proveedores.
- Clientes.
- Terceros.
- Entidades del estado.
- Accionistas.
- Gerencias.

- Los requisitos relevantes de estas partes interesadas para el SGSI.
- Cuáles de estos requisitos se abordarán a través del SGSI.

4.2.1 Generalidades

4. Contexto de la organización

Nueva consideración para el cambio climático

Esta cláusula incluye ahora explícitamente la afirmación "La organización determinará si el cambio climático es una cuestión relevante".

4. Contexto de la organización

4.3 Determinar el alcance del SGSI.

La organización debe determinar :

- Límite
- Aplicabilidad

ISO 27001

Información documentada

Disponible.

La organización debe determinar :

Cuestiones internas.

Cuestiones externas.

Requisitos de partes interesadas pertinentes.

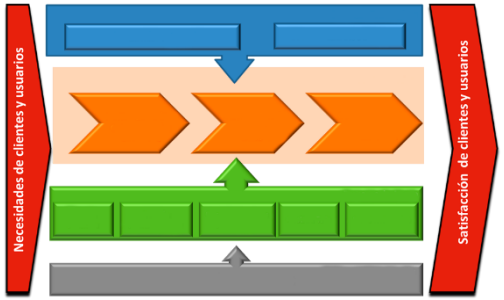
Productos y servicios

Interfases y dependencias entre las actividades realizadas por la empresa y las que se lleva a cabo por otras empresas.

4. Contexto de la organización

4.4 Sistema de gestión de seguridad de la información

La organización de debe establecer, implementar, mantener y mejorar el SGSI



La organización debe determinar los procesos necesarios para el SGSI y su aplicación en la empresa

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón