INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 16

9 DE ENERO DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

Enunciado

Son herramientas destinadas a facilitar el cumplimiento normativo aplicable en materia de seguridad y la obtención de certificados en esas normativas.-

Certificación normativa

¿Qué es?

Son herramientas destinadas a facilitar el cumplimiento normativo aplicable en materia de seguridad y la obtención de certificados en esas normativas. Posibilitan la implementación de políticas de seguridad, la realización de análisis de riesgos, la valoración de activos, la implantación de medidas de seguridad, la verificación y el cumplimiento de las políticas y medidas establecidas. En este grupo se incluyen las herramientas de Gestión de Riesgos, así como los Sistemas de Gestión de Seguridad de la Información (SGSI), los planes y las políticas de seguridad.

Tipos

- ISO 9001 - Gestión de Calidad:

Establece los criterios para un sistema de gestión de calidad efectivo en una organización. Se centra en la mejora continua, la satisfacción del cliente y la eficiencia operativa.

- ISO 27001 - Seguridad de la Información:

Establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Se enfoca en la protección de la confidencialidad, integridad y disponibilidad de la información.

- ISO 14001 - Gestión Ambiental:

Define los requisitos para un sistema de gestión ambiental efectivo. Se centra en la minimización del impacto ambiental de las operaciones organizacionales.

- ISO 45001 - Salud y Seguridad Ocupacional:

Establece los requisitos para un sistema de gestión de salud y seguridad ocupacional. Busca proporcionar un entorno de trabajo seguro y saludable.

- ISO 22301 - Gestión de la Continuidad del Negocio:

Define los requisitos para un sistema de gestión de continuidad del negocio (SGCN). Se enfoca en garantizar la capacidad de una organización para continuar sus operaciones en situaciones de crisis.

- SOC 2 (Service Organization Control 2):

Se centra en la seguridad, confidencialidad, privacidad, integridad y disponibilidad de los datos manejados por proveedores de servicios en la nube y otras organizaciones de servicios.

- PCI DSS (Payment Card Industry Data Security Standard):

Establece requisitos para la seguridad de la información de las tarjetas de pago. Se aplica a las organizaciones que manejan datos de tarjetas de crédito y débito.

- HIPAA (Health Insurance Portability and Accountability Act):

Se aplica a las organizaciones que manejan información de salud en los Estados Unidos. Establece estándares para la privacidad y seguridad de la información de salud.

- GDPR (Reglamento General de Protección de Datos):

Se aplica a organizaciones que manejan datos personales de ciudadanos de la Unión Europea. Establece normas para la protección de la privacidad y los derechos de los individuos.

- ISO 50001 - Gestión de la Energía:

Define los requisitos para un sistema de gestión de la energía. Se centra en mejorar el rendimiento energético y la eficiencia.

Recomendaciones

- Desarrollar políticas de seguridad en las que se valoren los riesgos a los que están expuestos los sistemas de información.

- Contar con servicios de consultoría previos a la implantación de cualquier herramienta asociada a esta categoría, debido a la complejidad a la hora de abordar cualquier proceso de adecuación y cumplimiento de normativa.

- Establecer rutinas de gestión de la seguridad y verificar su cumplimento para minimizar riesgos de seguridad.