Guía para el examen

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.
puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.
El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

ISO 17799

es un estándar para la seguridad de la información adoptado por la Organización Internacional de Normalización (ISO) en 2000 este describe como realizar las mejores prácticas con respecto a la confidencialidad, integridad y disponibilidad de información dentro de una organización. El estándar ofrece la de guiar al personal de gestión de información a cargo de establecer sistemas de seguridad. Los temas tratados incluyeron la definición de términos de seguridad de la información, la clasificación de los tipos de información, la descripción de los requisitos mínimos y la sugerencia de respuestas apropiadas a las infracciones de seguridad.

COBIT

presenta un enfoque al negocio que radica en vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI.
Asimismo, presenta un enfoque respecto a procesos de acuerdo a las fases del ciclo de Deming, ofreciendo una visión de extremo a extremo de la TI, ayudando a identificar los recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

NIST

El marco para la mejora de la seguridad cibernética en infraestructuras críticas, mejor conocida en inglés como NIST Cibersecurity Framework. La orientación del marco es ayudar a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

su activo más importante es saber cómo actuar de la mejor manera frente a un ataque cibernético porque, como sucede con los riesgos financieros o de reputación, el riesgo cibernético genera impacto negativo en los objetivos de negocio.

ITIL

Es una guía de buenas prácticas para la gestión de servicios de tecnologías de la información de tecnologías de la información. La guía ITIL ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio.

Los pilares de ITIL son los siguientes principios:

Procesos, necesarios para la gestión de TI de acuerdo a la alineación de los mismos dentro de la organización.

Calidad, entendida como la entrega a cliente del producto o servicio óptimos, es decir, incluyendo las características acordadas.

Cliente, su satisfacción es el objetivo de la mejora de los servicios, siendo, por lo tanto, el beneficiario directo de la implantación de las buenas prácticas de ITIL.

Independencia, siempre deben mantenerse buenas prácticas a pesar de los métodos establecidos para cada proceso y de los proveedores existentes.