SESION 2 1er parcial

Introducción a la administración de la seguridad informática

Objetivo: al finalizar la sesión el alumno identificara los conceptos base en la administración de la seguridad informática bajo estándares de certificación ISO 27000

Consideraciones teóricas: la forma internacional ISO (organización internacional de normalización) específicamente para ISO 2700 formaliza procesos, estándares, metodologías en función a sistemas de gestión de la seguridad de la información, sus directrices, gobernabilidad y administración. Define lo siguiente:

1. Administración. Procesos por etapas (planeación, organización, dirección y control) para obtener mayor productividad, un costo beneficio optimo en cualquier área de la función (nube, ciberseguridad, sistemas operativos, bases de datos, soporte técnico ti, infraestructura, redes, telecomunicaciones, etc)
2. Información. Datos, comunicación, adquisición de conocimiento digital, conocimiento humano que permite ampliar o presentar un campo, materia o área almacenado
3. Seguridad informática. Protección, salvaguarda de los activos tecnológicas, digitales en contra de amenazas, vulnerabilidades, ataques, riesgos aplicados (confidencialidad, integridad, disponibilidad)

Administración de la seguridad informática.

Apoya, organiza, planifica, automatiza, controla todas las tareas, actividades, procesos, funciones a nivel tecnológico, infraestructura de las empresas para identificar, renidminetos, productividad, identificar riesgos, amenazas , resoluciones y toma de decisiones bajo diseño, implementación y mantenimiento de sistemas de gestión de la seguridad de la información (SGSI) norma iso 27000-27040

Imagen que contiene Diagrama

Descripción generada automáticamente

Desarrollo:

Descargue y ejecute la herramienta MSAT (Microsoft segurity admin tool) regulado bajo la norma iso 27000 para evaluar la administración de la seguridad informática de la universidad

TEST profesional de evaluación de la administración de la seguridad informática MSAT

Incluye un cuestionario regulado por ISO 27000 y NIST permite ver los posibles agujeros, vulnerabilidades, riesgos y situaciones críticas de la empresa.

Proporciona un perfil de la situación de la seguridad en todos los ámbitos tecnológicos

Da estadísticas y gráficos de impacto importantes

Ofrece recomendaciones de las buenas prácticas de la administración de la seguridad informática

Cuestionario interactivo que da por resultado DiDI (índice de defensa) y BRP (perfil de riesgos de negocios)

Es una implementación de el marco de trabajo iso 27000-NIST es empleada con agentes de ciberseguridad CEO

uin\_Alejandro\_2024

escriba al menos 5 términos palabras o tecnologías desconocidas en investiguen

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Conclusión

la seguridad de la información es fundamental para el rendimiento empresarial, ya que protege los activos digitales y garantiza la continuidad operativa frente a posibles amenazas cibernéticas.