SEGURIDAD INFORMÁTICA

Etapas De Madurez

La seguridad informática consiste en el aseguramiento de los recursos de los sistemas de información (material informático o programas) de una organización, para que sean utilizados de manera objetiva y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Sistema De Gestión De La Seguridad De La Información

Un sistema de gestión de la seguridad de la información (sgsi) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la iso/iec 27001.

El término se denomina en inglés "information security management system" (isms).

El concepto clave de un sgsi es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Sistema de gestión de la seguridad de la información

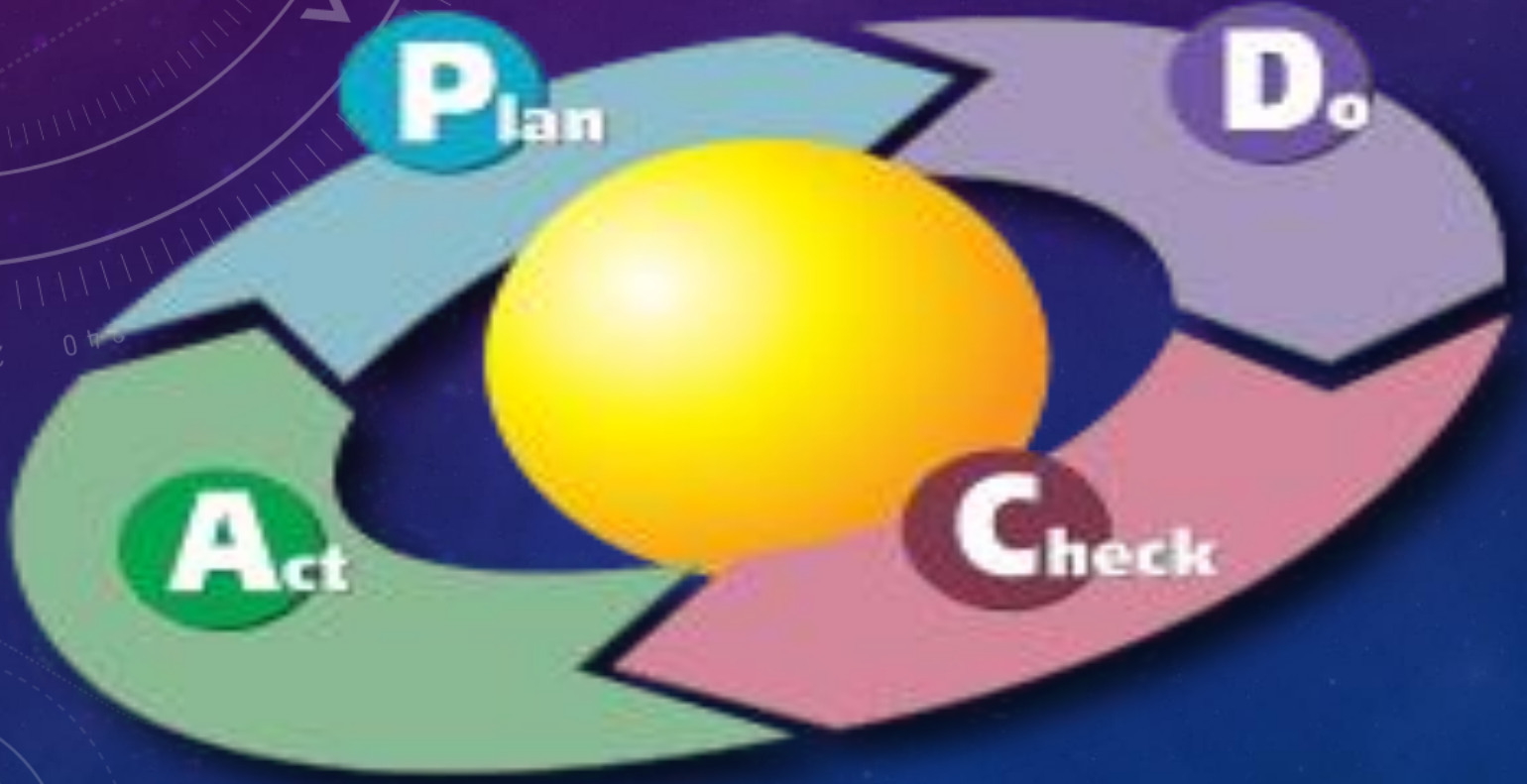
Círculo De Deming

La iso/iec 27001 por lo tanto incorpora el típico "plan-do-check-act" (pdca) que significa "planificar-hacer-controlar-actuar" siendo este un enfoque de mejora continua:

1. Plan (planificar): es una fase de diseño del sgsi, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
2. Do (hacer): es una fase que envuelve la implantación y operación de los controles.
3. Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del sgsi.
4. Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el sgsi a máximo rendimiento.

La mejor definición de sgsi es descrito por la iso/iec 27001 y iso/iec 27002 y relaciona los estándares publicados por la international organization for standardization (iso) y la international electrotechnical commission (iec).

¿QUÉ ES EL CÍRCULO DE DEMING?



TAREA

- Definir según la ISO 27001: SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- Ensayo mínimo de 2 páginas: ISO/IEC 27001

Sistema de gestión de la seguridad de la información

OTROS SGSI

Sogp otro sgsi que compite en el mercado es el llamado "information security forum's standard of good practice" (sogp). Este sgsi es más una "best practice" (buenas prácticas), basado en las experiencias del isf.

Ism3 information security management maturity model ("ism3") (conocida como ism-cubed o ism3) está construido en estándares como itil, iso 20000, iso 9001, cmm, iso/iec 27001, e información general de conceptos de seguridad de los gobiernos ism3 puede ser usado como plantilla para un iso 9001 compliant. Mientras que la iso/iec 27001 está basada en controles. Ism3 está basada en proceso e incluye métricas de proceso.

Otros marcos de trabajo:

1. En el caso de cobit, los controles son aún más amplios que en la iso-iec 27001.
2. En el caso de itil (sobre todo la v.3) tiene muchos puntos de contacto respecto a cuestiones de seguridad.
3. Prince2 es otro marco de trabajo de buenas prácticas, en este caso relacionadas con la gestión de proyectos.

Consideraciones para elaborar un sistema de seguridad integral

Desarrollar un sistema de seguridad significa: "planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa."

Consideraciones para elaborar un sistema de seguridad integral

UN SISTEMA INTEGRAL DEBE CONTEMPLAR:

- Definir elementos administrativos
- Definir políticas de seguridad

- A nivel departamental
- A nivel institucional

- Organizar y dividir las responsabilidades
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Definir prácticas de seguridad para el personal:

- Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores.

- Números telefónicos de emergencia
- Definir el tipo de pólizas de seguros
- Definir elementos técnicos de procedimientos

Consideraciones para elaborar un sistema de seguridad integral

UN SISTEMA INTEGRAL DEBE CONTEMPLAR:

- Definir las necesidades de sistemas de seguridad para:
- Hardware y software
- Flujo de energía
- Cableados locales y externos
- Aplicación de los sistemas de seguridad incluyendo datos y archivos
- Planificación de los papeles de los auditores internos y externos
- Planificación de programas de desastre y sus pruebas (simulación)
- Planificación de equipos de contingencia con carácter periódico
- Control de desechos de los nodos importantes del sistema:
- Política de destrucción de basura copias, fotocopias, etc.
- Consideración de las normas iso 14000

Etapas para implementar un sistema de seguridad

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

1. Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
2. Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
3. Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

Etapas para implementar un sistema de seguridad

Plan de seguridad ideal (o normativo)

- El plan de seguridad debe asegurar la integridad y exactitud de los datos
- Debe permitir identificar la información que es confidencial
- Debe contemplar áreas de uso exclusivo
- Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
- Debe asegurar la capacidad de la organización para sobrevivir accidentes
- Debe proteger a los empleados contra tentaciones o sospechas innecesarias
- Debe contemplar la administración contra acusaciones por imprudencia

Consideraciones para con el personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una autoevaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

- Motivar
- Capacitación general
- Ética y cultura
- Capacitación de técnicos

Beneficios de un sistema de seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

ACTIVIDAD

- Mencione 3 beneficios de un sistema de seguridad
- Explique