¿Qué hace un técnico de ciberseguridad en una empresa?

Gonzalo Sánchez Delgado

firexploit

www.incibe.es

https://cybercamp.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

cyber camp

CYBERSECURITY EVENT

2015

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Coordenadas

Gonzalo Sánchez

gonzalo.sanchez@firexploit.com

www.firexploit.com

¿Qué hace un técnico de seguridad de la información en una empresa?

¿ PARA QUÉ ?

¿ QUÉ ?

¿ CÓMO ?

“El comercio no trata sobre mercancías, trata sobre ***información****. Las mercancías se sientan en el almacén hasta que la* ***información*** *las mueve.”*

Caroline J. Cherryh

Integridad

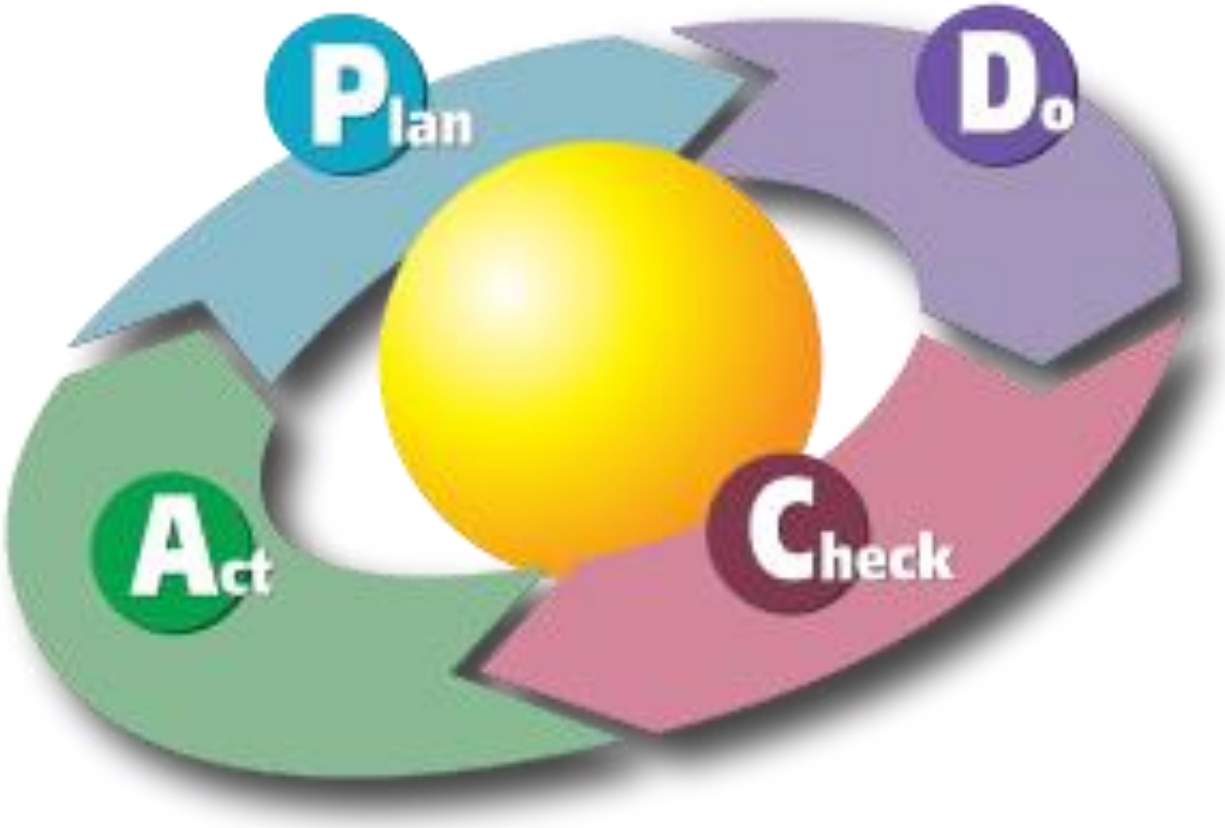
Disponibilidad

Confidencialidad

¿ QUÉ ?

SGSI

Sistema de Gestión de la Seguridad de la Información



Ciclo de mejora continua. Ciclo Deming

La **seguridad** no es un resultado, es un **proceso** en sí mismo.

¿ CÓMO ?

SGSI

Sistema de Gestión de la Seguridad de la Información

ISO/IEC 27001
ISO/IEC 27002

ISO/IEC 27001

Cualquier tipo de organización

Adopción gradual

Especifica requisitos a cumplir no cómo hacerlo.

Versatilidad

ISO/IEC 27002

Guía para la gestión de la SI

ISO/IEC 27001

- **Política de seguridad**: directrices generales
- **Inventario de activos**: propietario/valoración
- **Análisis de riesgos**: amenazas y vulnerabilidades
  Mitigar / Asumir / Transferir / Eliminar
- **Gestión de riesgos**: aprobada por Dirección
- **Documento de aplicabilidad**: controles

ISO/IEC 27002

Lista de puntos de control:

CASO PRÁCTICO

CASO PRÁCTICO

1- Identificación de activos:

Nombre	Descripción	Categoría	Ubicación	Propietario
Srv-mad-rrhh	Servidor RRHH Madrid	Hardware	Madrid	Dep TI

2- Valoración del activo (0-4):

Nombre	Confidencialidad	Integridad	Disponibilidad	Total
Srv-mad-rrhh	4	3	2	9

CASO PRÁCTICO

3- Gestión de riesgos:

Riesgo	Valor activo	Nivel de amenaza (0-3)	Vulnerabilidad (0-3)	Nivel Riesgo
Fuego	7	3	3	**63**
Robo	7	3	1	**21**
(…)	(…)	(…)	(…)	(…)

Amenaza: nivel de daño de la amenaza sobre el activo

Vulnerabilidad: posibilidad de que ocurra la amenaza sobre dicho activo

CASO PRÁCTICO

4- Identificación de activos:

Activo	Riesgo	Tratamiento
Servidor	30	Se asume el riesgo
Servidor	50	Mitigarlo

5- ISO/IEC 27002:

9. Seguridad física del entorno
    9.2 Seguridad de los equipos
        9.2.1 Emplazamiento y protección de los equipos

PARA QUÉ

Puntos de mejora:

- **Instalar sistemas de extinción por detección de humo**
  - **Revisión de proveedor periódica**
- **Instalar sistemas de monitorización de temperatura**
  - **Revisión de datos periódica de registros**

PARA QUÉ

Resultado:

Riesgo	Valor activo	Nivel de amenaza (0-3)	Vulnerabilidad (0-3)	Nivel Riesgo
Fuego	7	3	1	**21**

OTROS CASOS

Activo: Servidor Web

Riesgo: Ataque hacking

ISO 27002: 10.6.2. Seguridad de los servicios de red

Punto de mejora: Instalación de firewall web

Activo: Red de datos cableada

Riesgo: Intrusión no permitida

ISO 27002: 11.4.6 Control de conexión a las redes

Punto de mejora: Instalación de un IDS/IPS

CONCLUSIÓN

¿ Preguntas ?

https://cybercamp.es **#CyberCamp15** **@CyberCampEs**

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD