Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

SEMINARIO

Normas, políticas y gestión de la seguridad de la información

Cap. Jesús Cano Carrillo

ACADEMIA DE INGENIEROS

Estado de alarma, 21 mayo de 2020

Lo que siempre quise hacerle a un hacker

Aspectos generales

El negocio y la seguridad

Info: www.welivesecurity.com

La INFORMACIÓN es el activo más importante de una organización.

Ejemplos: documentos, correos electrónicos, bases de datos, nóminas, fax…

La seguridad no es absoluta
-> Idea de riesgo asumible

SGSI: SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Consiste en el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la información en una organización, para asegurar la confidencialidad, integridad y disponibilidad de los activos minimizando a la vez los riesgos de seguridad de la información.

Sobre los activos

Definición: Se denomina activo a aquello que tiene valor para la organización y por tanto debe protegerse

- Activos de información
- Activos físicos
- Activos de servicios
- Activos humanos

Un SGSI es un sistema para asegurar la continuidad del negocio.

Gasto en seguridad	Impacto del riesgo

Gasto en seguridad vs. Impacto del riesgo vs. Valor activo

Visión general

Proceso por fases

Definición e implantación

Política de seguridad = <u>Compromiso</u> de la alta dirección

1. DOCUMENTADO y SISTEMATIZADO
2. IMPLICA A TODA LA ORGANIZACIÓN
3. La APOYA LA ALTA DIRECCIÓN
4. ESTABLECE RESPONSABILIDADES
5. REQUISITOS MÍNIMOS DE SEGURIDAD

Ejemplos de políticas

www.tipsa.net/downloads/sgsi.pdf

Page: 4 of 4 Automatic Zoom

técnicas de informática

POLÍTICA DE SEGURIDAD DEL SGSI

- TIPSA SL es una empresa dedicada a aportar soluciones informáticas a las empresas mediante la implementación de software de gestión. Conscientes de la importancia que la seguridad de la información tiene para el desarrollo de su negocio ha decido implantar un sistema de gestión y suscribe la presente polftica.
- TIPSA SL establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) encaminados a
como la conservación de la confidencialidad, disponibili
como de los sistemas que la soportan, aumentando
otras partes interesadas; junto con el cumplimient
reglamentarios y contractuales que le sean de aplicació
- El diseño, implantación y mantenimiento del SGSI se a
proceso continuo de análisis y gestión de riesgos del

Ejemplo de Implantación de un SGSI

Lecciones Aprendidas

Documentación básica de un SGSI

- Política de seguridad.
  Documento principal del SGSI: política.
- Planes de seguridad.
  Documentos técnicos de dominio, alcance o cometido.
- Procedimientos de seguridad.
- Guías de operación

Ejemplos de políticas

Politica de Seguridad

Capitulos Introductorios

1. Introducción
2. Términos y Definiciones
3. Estructura de la Política modelo
4. Evaluación y tratamiento de riesgos

Capitulos Cláusulas

5. Política de Seguridad
6. Organización
7. Clasificación de Activos
8. Recursos Humanos
9. Seguridad Física Ambiental
10. Gestión de Comunicaciones /Operaciones
11. Gestión de Accesos
12. Adquisición, Desarrollo y mantenimiento de sistemas
13. Gestión de Incidentes de Seguridad
14. Gestión de la Continuidad
15. Cumplimiento

Politicas x cláusula

Objetivo = resultado deseado
Controles = para mitigar riesgos

Cláusulas
Aspecto o dominio particular de la seguridad de la información

Categoría
Grupo de controles de cada claúsula

Control
Punto de evaluación

Info: servicios.infoleg.gob.ar

Serie de normas UNE-ISO/IEC 27000

- ISO 27000: Descripción general de todas las normas de la serie y vocabulario.
- ISO 27001: Norma principal para implantar un SGSI. Los SGSI se pueden certificar por auditores externos.
- ISO 27002: Guía de buenas prácticas: 39 objetivos de control y 133 controles recomendables (en 11 dominios temáticos) para la versión 2007. La última revisión, de 2013, se reordena en 14 dominios, 35 objetivos de control y 114 controles.
- ISO 27003: Guía de implementación y modelo PDCA.
- ISO 27004: Métricas de un SGSI
- ISO 27005: Guía de gestión del riesgo
- ISO 27006: Requisitos de acreditación

de auditores y certificadores

Dominios de control

Dominios ISO 27001:2013

- 14 **dominios**
- 35 objetivos de **control**
- 114 controles

ISO 27001:2013 (14 dominios, 113 Controles)	
A.5	Política de seguridad.
A.6	Organización de la seguridad de la información
A.7	Seguridad de los RRHH.
A.8	Gestión de activos.
A.9	Control de accesos.
A.10	Criptografía.
A.11	Seguridad física y ambiental.
A.12	Seguridad en las operaciones.
A.13	Transferencia de información.
A.14	Adquisición de sistemas, desarrollo y mantenimiento.
A.15	Relación con proveedores.
A.16	Gestión de los incidentes de seguridad.
A.17	Continuidad del negocio.
A.18	Cumplimiento con requerimientos legales y contractuales.

Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2005

(Conjunto de medidas, acciones y documentos que permiten cubrir y auditar cierto riesgo)

N°	Dominio - Control		#Ctrls	Cumplimiento
A5	**Política de seguridad de la información**		**2**	
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.			
A.5.1.1	Política de seguridad de la información	Se dispone de una política de SI aprobada por la dirección, publicada y comunicada a todos los empleados y partes externas pertinentes.		
A.5.1.2		La política de seguridad de información se revisa a intervalos planificados, y si ocurren cambios significativos se asegura su conveniencia, adecuación y eficacia continua.		
A6	**Organización de la seguridad de la información**		**11**	
	Gestionar la organización de la seguridad de información.			
A.6.1.1	Organización interna	La Alta Dirección apoya (dirige, se compromete, demuestra y reconoce responsabilidades) activamente la SI en la Institución.		
A.6.1.2		En las actividades de SI participan representantes de todas las UU.OO. Tienen roles y funciones.		
A.6.1.3		Los roles y responsabilidades en SI están bien definidos.		
A.6.1.4		Está establecido el proceso de autorización para nuevos activos de información (AI).		
A.6.1.5		Están definidos acuerdos de confidencialidad y se revisa con regularidad.		
A.6.1.6		Se mantiene los contactos apropiados con las autoridades pertinentes.		
A.6.1.7		Se mantiene los contactos apropiados con entidades especializadas en SI.		
A.6.1.8		El enfoque de la organización para gestionar la SI se revisa de manera independiente y periódica.		
A.6.2.1	Entidades externas	Se gestiona (identifica e implementa) los riesgos de acceso a la información de entidades externas.		
A.6.2.2		Se trata todos los requerimientos de SI antes de dar acceso a los clientes.		
A.6.2.3		Se establece acuerdos con terceros, que involucran acceder, procesar, comunicar o gestionar la información de la entidad , que abarcan los requerimientos de SI relevantes.		
A7	**Gestión de activos de información (AI)**		**5**	
	Lograr y mantener la protección apropiada de los activos de información			
A.7.1.1	Responsabilidad por los activos	Se mantiene un inventario de AI.		
A.7.1.2		Todo AI tiene asignado un responsable (propietario).		
A.7.1.3		Se dispone de una normativa de uso de los AI		
A.7.2.1	Clasificación de la información	La información está clasificada según su valor, requisitos legales, sensibilidad y criticidad		
A.7.2.2		Se dispone del procedimiento de rotulado y manejo de la información.		
A8	**Seguridad de los recursos humanos**		**9**	
	Asegurar que todo el personal involucrado entienda sus responsabilidades, sean apropiados para sus roles y así reducir el riesgo de robo, fraude o mal uso de los activos de información.			
A.8.1.1	Antes del empleo	Se tiene documentado (de acuerdo a la política) los roles y responsabilidadesde de SI, de todo el personal.		
A.8.1.2		Se verifica antecedentes de todo candidato a empleado o contratista.		
A.8.1.3		Se firman contratos donde se incluye las responsabilidades de SI.		
A.8.2.1	Durante el empleo	Se procura que todos los empleados apliquen la SI según la política.		
A.8.2.2		Se sensibiliza, capacita y educa en SI pertinente a su función de trabajo.		
A.8.2.3		Se tiene establecido un procesos disciplinario ante el incumplimiento de SI.		
A.8.3.1	Terminación o cambio del empleo	Están definidas las responsabilidades para el término o cambio de empleo.		
A.8.3.2		Se procura la entrega de activos al témino de contrato.		
A.8.3.3		Se retira los derechos de acceso al término del contrato.		
A9	**Seguridad física y medioambiental**		**13**	
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.			
A.9.1.1	Áreas seguras	Se utiliza mecanismos de protección perimétrica (muros, vigilantes, etc.) a las áreas que contienen información e instalaciones que procesan información.		
A.9.1.2		Se utiliza mecanismos de control de acceso en entradas críticas.		
A.9.1.3		Se utiliza mecanismos de seguridad en oficinas, habitaciones e instalaciones.		
A.9.1.4		Se utiliza mecanismos de protección ante amenzas externas y ambientales.		
A.9.1.5		Se aplica medidas de seguridad física y directrices para trabajar en áreas seguras.		
A.9.1.6		Se aplica medidas de seguridad en áreas de acceso público (entrega/descarga).		
A.9.2.1	Seguridad del equipo	Los equipos están ubicados en salas con protección física ante un posible acceso no autorizado.		
A.9.2.2		Los equipos están protegidos frente a fallas de servicios públicos.		
A.9.2.3		El cableado eléctrico y de comunicaciones está protegido frente a interceptación o daños.		
A.9.2.4		Los equipos son mantenidos en forma periódica.		
A.9.2.5		Se aplica seguridad a los equipos fuera del local		
A.9.2.6		Antes de dar de baja un equipo se elimina la información		

Dominio de la política de seguridad

Su objetivo es garantizar a la **empresa el soporte y gestión necesarios para la seguridad de la información** según todos los requisitos institucionales y normativos. Se debe establecer la política según los objetivos establecidos por la empresa. Es necesario contar con el compromiso en cuanto a la **seguridad de la información**.

Dominio de la organización en cuanto a la seguridad de la información

Su finalidad es instaurar un **marco de referencia para definir el camino para la implantación** y control de la seguridad de la información dentro de la empresa.

La dirección de la empresa es la responsable de establecer la política de seguridad, además debe **establecer los roles de los comités y nombrar al encargado** mediante una resolución. El encargado debe coordinar y revisar el proceso.

Dominio de gestión de activos

Este dominio tiene el **objetivo de llevar a cabo una protección adecuada** en cuanto a los activos de la empresa.

En todo momento los activos se encuentran **inventariados y controlados** por un responsable que también se encarga de manipularlos de forma correcta.

Dominio de seguridad de los recursos humanos

Su objetivo es fijar las medidas necesarias para **controlar la seguridad de la información**, que ha sido manejada por los recursos humanos de la empresa.

Dominio en cuanto la seguridad física y del medio ambiente

Con este dominio se **consigue proteger todas las instalaciones de la empresa** y toda la información que maneja. Por esto, se establecen **diferentes barreras de seguridad y controles de acceso**.

Dominio gestión de las comunicaciones y operaciones

El objetivo se encuentra en **determinar los procesos y responsabilidades de las operaciones** que lleva a cabo la organización. Se debe asegurar que todos los procesos se encuentren relacionados con la **información ejecutada de forma adecuada**.

Dominio control de acceso

Se asegura el acceso autorizado a todos los **sistemas de información de la empresa**. Es necesario realizar diversas acciones como controles para **evitar el acceso de usuarios** no autorizados, controles de entrada, etc.

Dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

Este dominio se encuentra dirigido a aquellas empresas que **desarrollen software internamente** o que tenga un contrato con otra empresa que se encarga de desarrollarlo. Se tiene que establecer los requisitos en la **etapa de implantación y desarrollo de software** para que sea seguro.

Dominio de gestión de incidentes en la seguridad de la información

Con este dominio se aplica un **proceso de mejora continua en la gestión de percances** de seguridad de la información.

Dominio de gestión de continuidad de negocio

El objetivo es asegurar la **continuidad operativa de la empresa**. Se requiere aplicar controles que eviten o reduzcan todos los incidentes de las actividades desarrolladas por la empresa que puedan generar un impacto.

Dominio de cumplimiento

Su finalidad es asegurar que los **requisitos legales de seguridad** que han sido referidos al diseño y gestión de los sistemas de información.

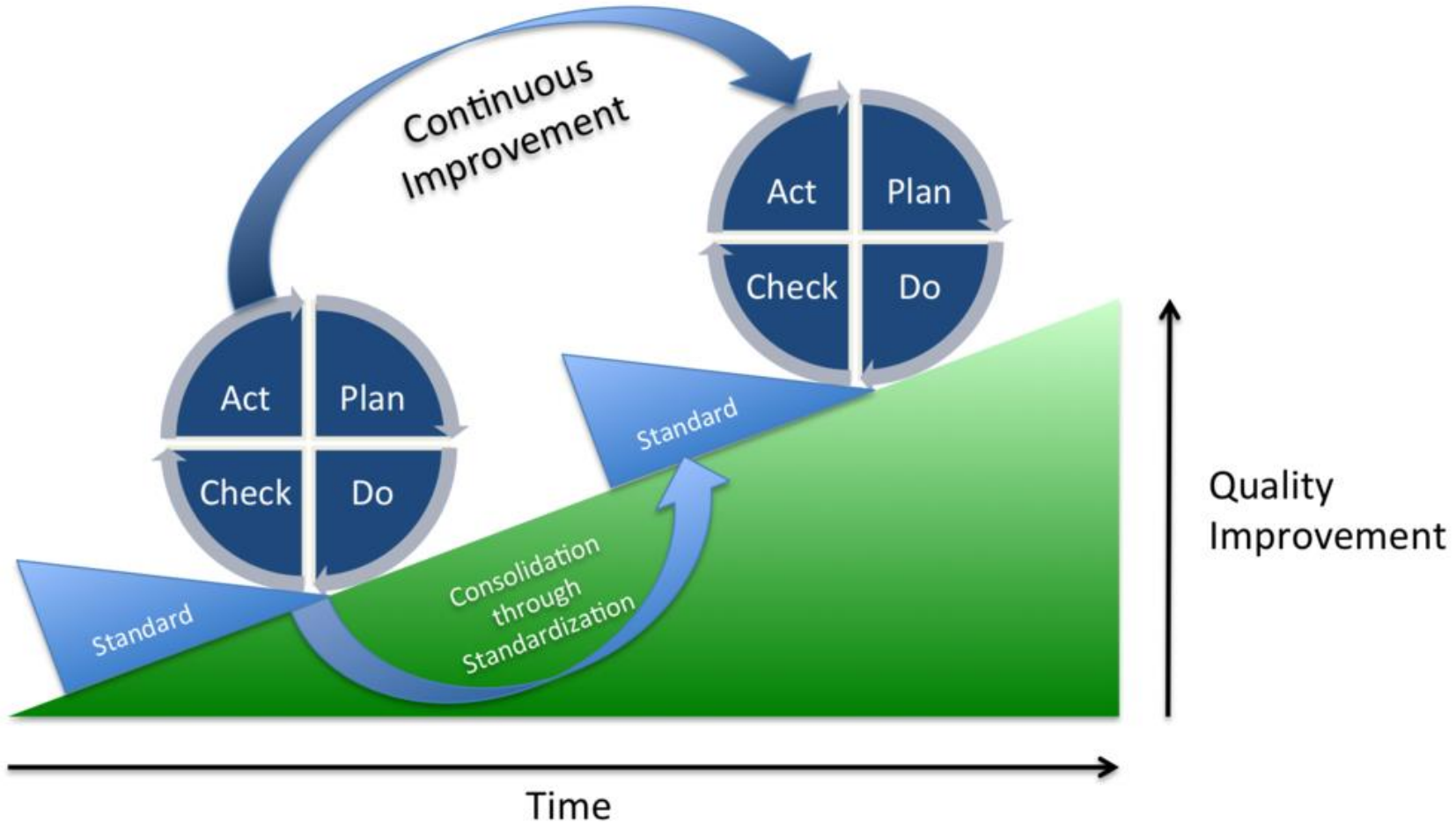
Proceso de mejora continua

PDCA: Círculo de Deming

- Planificar (qué y cómo)
- Hacer lo planificado (Do)
- Verificar resultado (Check)
- Actuar (analizar y corregir)

También se denomina

Espiral de mejora continua



Otros sonidos de Seguridad de la Información

- Information Security Management Maturity Model (ISM3) basado en metodología de procesos.

- COBIT: Control Objectives for Information and related Technology, es una marco de trabajo de buenas prácticas de gestión de tecnología de la información (TI). Mantenido por ISACA (Information Systems Audit and Control Association)

Esquema Nacional de Seguridad

- Es la política de seguridad de la información de la Administración Pública en España. (R.D. 3/2010)
- Expresa los principios básicos de seguridad y los requisitos mínimos para proteger la información.
- Categoriza los sistemas en Alto, Medio o Bajo.
- Tiene 75 medidas de seguridad.

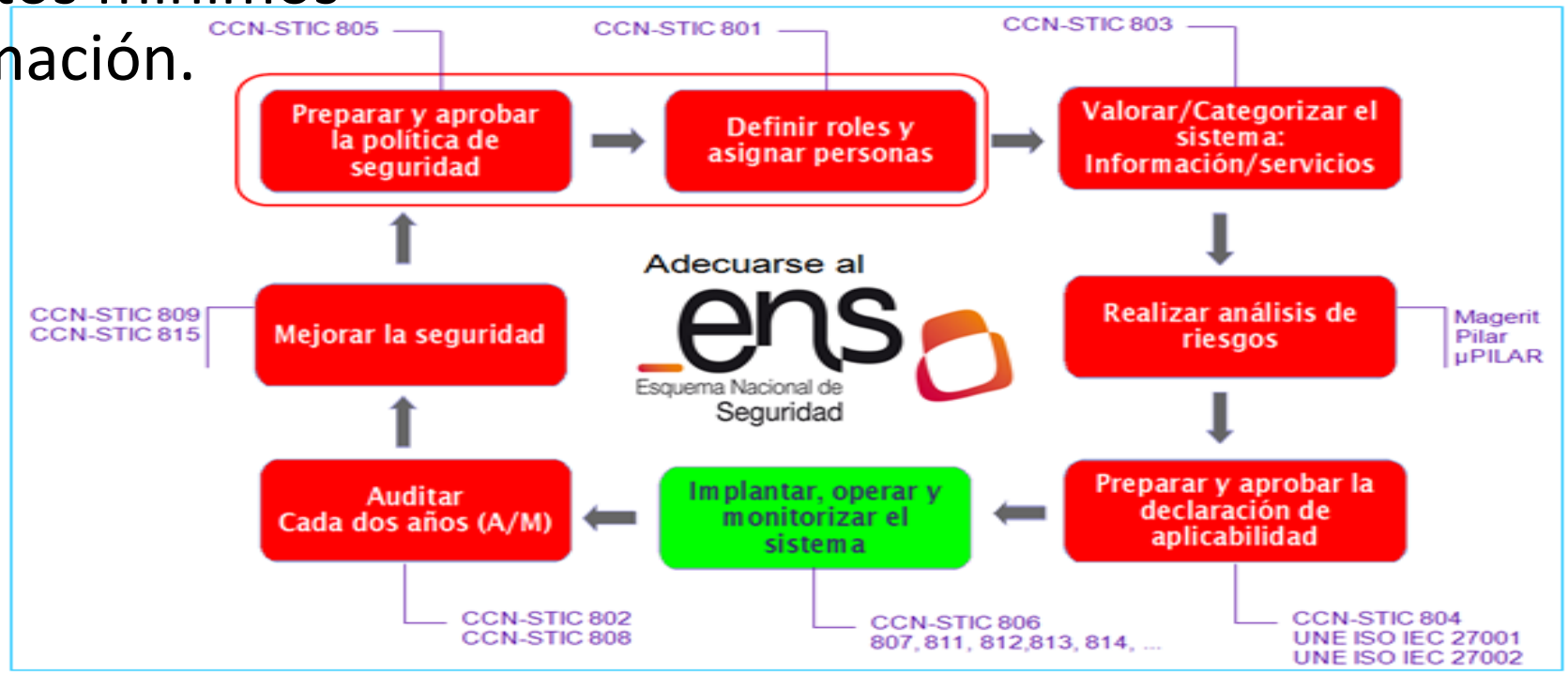
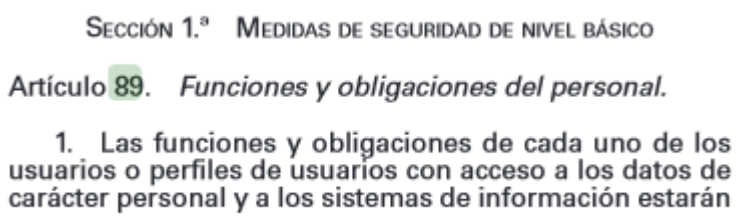


Figura: Adecuación al Esquema Nacional de Seguridad.

Control de los empleados

Documento de seguridad

Real Decreto 1720/2007



SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán

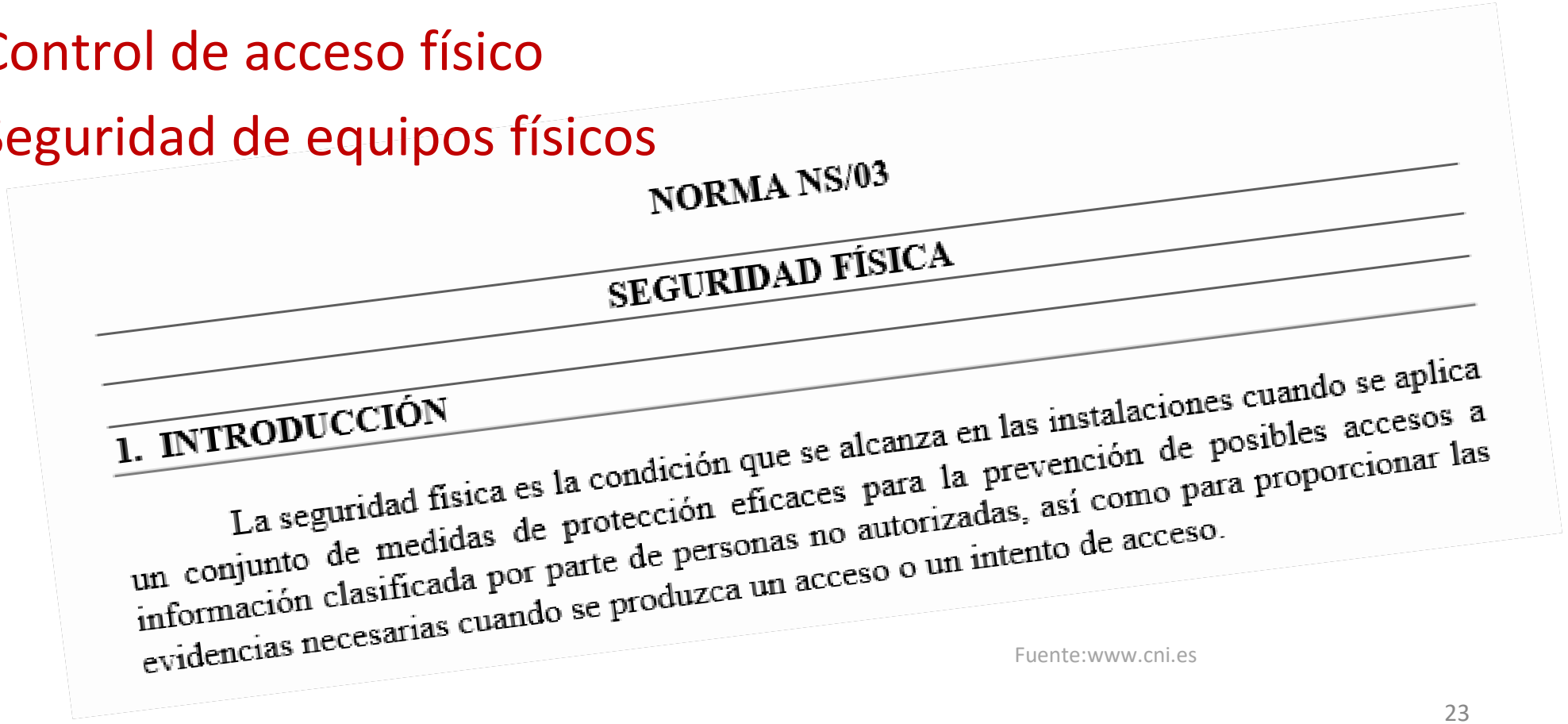
- ALTA DE EMPLEADOS
- BAJA DE EMPLEADOS
- FUNCIONES, OBLIGACIONES Y DERECHOS DE LOS USUARIO
- FORMACIÓN Y SENSIBILIZACIÓN DE LOS USUARIOS

Control en la adquisición de productos y relación con proveedores

Fuente:ticpymes.es

Control de la Seguridad física de las instalaciones

- Perímetros y zonas
- Control de acceso físico
- Seguridad de equipos físicos



NORMA NS/03

SEGURIDAD FÍSICA

1. INTRODUCCIÓN

La seguridad física es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.

Fuente:www.cni.es

Control de los sistemas de protección eléctrica

- Fallas de fluido eléctrico y oscilación de red.
- Desde reguladores de corriente, supresores de picos a UPS.
- Suelo térmico
- Climatización

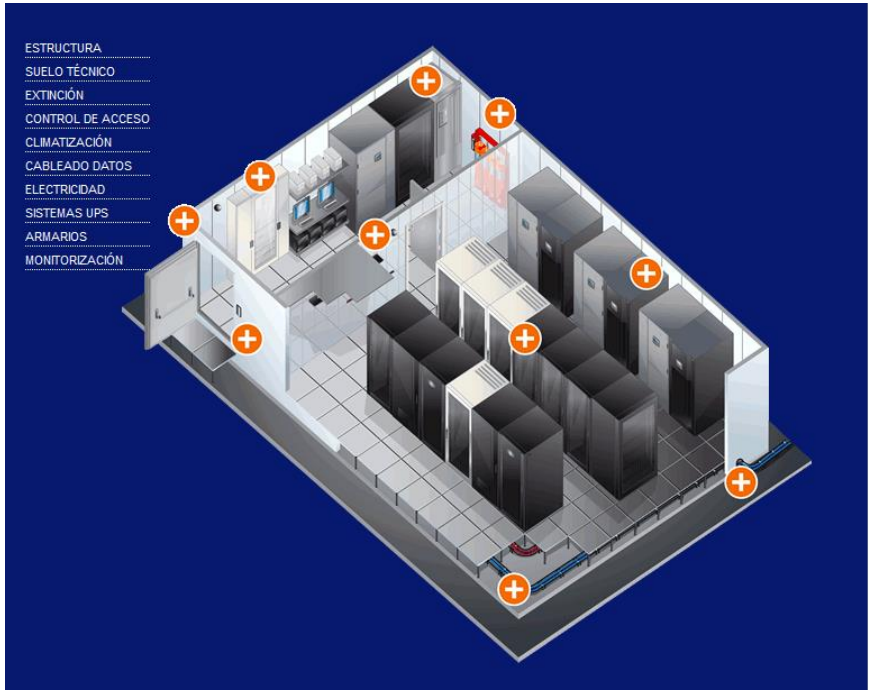


Imagen:cpdcontrol.com

Control del nivel de emisiones electromagnéticas

Vigilancia en la red y de los elementos de conectividad

Control de salida de equipos

Protección en el acceso y configuración de los servidores

Seguridad en los dispositivos de almacenamiento

Protección de equipos y estaciones de trabajo

Copias de seguridad

Control de seguridad de impresoras y periféricos

Gestión de Soportes informáticos

Gestión de cuentas de usuario

Identificación y autenticación

Autorización y control de acceso lógico

Protección de datos y documentos sensibles

Monitorización servidores y dispositivos de red

Seguridad en las conexiones remotas

Detección y respuesta ante incidentes

Realización de pruebas y auditorías periódicas

Bibliografía

Material	pp	tipo
www.normas-iso.com/iso-27001		web
G.Pallas y M. E. Corti, “Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica”, Grupo de Seguridad Informática, Universidad de la República, Uruguay, http://www.fing.edu.uy/inco/grupos/gsi	15	pdf
Hoja resumen de controles de seguridad ISO 27002. http://www.iso27000.es/download/ControlesISO27002-2005.pdf	1	pdf
Gómez Fernández, L. y Andrés Álvarez, A. “Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes”. AENOR Ediciones, 2ª Ed. 2012 (pp. 1-21 www.aenor.es/aenor/descargadocumento.asp?nomfich=/Documentos/Comercial/Archivos/NOV_DOC_Tabla_AEN_22994_1.pdf)	21	pdf libro
NIST Special Publication 800-53. Recommended Security Controls for Federal Information Systems. 2005.	123	pdf
Política de Seguridad de la Información. ENS Guía 805. Centro Criptológico Nacional. http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/805-ENS_politica-sep11.pdf	17	pdf

ACADEMIA DE INGENIEROS

Seminario