MODELOS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

MADRID, 27 DE MAYO DE 2013

¿Qué es la Seguridad de la Información?

- La información es un activo que, como otros activos importantes del negocio, tiene valor para la Organización y requiere en consecuencia una protección adecuada.
- Asegurar la información significa preservar la confidencialidad, la integridad y la disponibilidad de la información, y en caso necesario, otras propiedades, como la autenticidad, la trazabilidad o la fiabilidad.

Dimensiones de la seguridad de la información

Confidencialidad	• Para asegurar que sólo quienes estén autorizados puedan acceder a la información
Integridad	• Para asegurar que la información y sus métodos de proceso son exactos y completos
Disponibilidad	• Para asegurar que los usuarios autorizados tienen acceso a la información y los servicios
Trazabilidad	• Para asegurar el saber quien, cuando, cómo y qué se ha hecho en un proceso telemático
Autenticidad	• Para que no haya duda de quién es responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores.

Razones para los “fallos” de Seguridad

- Fallo energético
- Virus informático
- Acceso y uso indebido de terceros
- Fraude y uso ilegítimo de la informac
- Error humano: usuarios, operadores, programadores…
- Cambios inadecuados en T.I.
- Fallos en los elementos de T.I.: redes, sistemas, aplicaciones, etc.

Sistemas de Gestión

- Un sistema de gestión es la forma en la que una organización dirige y controla sus actividades.
- Un Sistema de Gestión de Seguridad de la Información es el que asegura que la información está protegida frente a pérdidas de confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad

Beneficios

- Cumplir con las exigencias legales y contractuales
- Mantener y reforzar la ventaja competitiva
- Mantener y mejorar la imagen de la entidad
- Cumplir con las expectativas de los usuarios y la sociedad
- Mejorar los procesos y procedimient

- Evitar multas y/o sanciones

Las Normas de Seguridad de la Información

- La norma ISO27001 especifica los requisitos que debe cumplir el Sistema de Gestión. Esta norma dice qué se debe hacer y es con la que una empresa puede certificarse.
- La norma ISO 27002 es una guía de buenas prácticas en seguridad de la información. Esta es la norma que dice cómo deben hacerse las cosas.

Requisitos Principales I

1. Definición de la Política de Seguridad. Establece el marco y da soporte a la gestión de la seguridad de la información alineándola con los requisitos del negocio y los legales.
2. Inventario de activos. Todos los activos de información se identifican claramente y se valoran.
3. Análisis de riesgos. Se identifican las amenazas relacionadas con los activos identificados, para estimar los riesgos a los que están expuestos.

Requisitos Principales II

4. Selección de controles. Del catálogo de buenas prácticas se seleccionan aquellas que pueden reducir el riesgo de los activos hasta un nivel aceptable.
5. Implantación y formación. Se definen los procedimientos para implantar los controles seleccionados y se forma al personal para aplicarlos.
6. Auditorías. El SGSI se tiene que auditar periódicamente tanto interna como externamente para garantizar que sigue

El Esquema Nacional de Seguridad

- El ENS es un Sistema de Gestión de Seguridad de la Información para las Administración Electrónica.

- El ENS se desarrolla sobre las recomendaciones de la UE y los estándares internacionales en materia de seguridad de la información, especialmente la Norma ISO 27001.

Principios básicos del ENS I

Seguridad Integral: La seguridad de la información en las administraciones se plantea como un proceso integral, que excluye tratamientos coyunturales.

Gestión basada en riesgos: Se analizarán los riesgos donde se deberán identificar y evaluar riesgos inherentes en todos los activos de información incluyendo las personas y la infraestructura que intervienen en su gestión.

Principios básicos del ENS II

Prevención, reacción y recuperación: Los sistemas de seguridad deben tener una orientación preventiva, para evitar las amenazas. Los sistemas dispondrán de medidas de recuperación que permitan asegurar la continuidad de la información y los servicios

Líneas de defensa: Deberá existir una estrategia de protección con diversas capas de seguridad y control.

Evaluación periódica: A través de auditorías y sistemas de verificación de cumplimientos.

Función diferenciada: Las diversas responsabilidades inherentes a la gestión de la seguridad deberán diferenciarse de las relativas a las de gestión de los sistemas de la información.

Requisitos mínimos

- Organización e implantación del proceso de seguridad
- Análisis y Gestión de Riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos
- Seguridad por defecto
- Integridad y actualización del sistema
- Protección de la Información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

Diferencias a reseñar

ISO	ENS
Es opcional	Es una obligación legal para los servicios de administración electrónica
Aplica a toda la información que queramos proteger	Aplica legalmente a la información necesaria para prestar servicios de administración electrónica
Hay que analizar los riesgos de los activos identificados	Establece tres niveles de criticidad de los servicios que se ofrecen: bajo, medio, alto y además hay que hacer un análisis de riesgos
Las medidas de seguridad se aplican según las necesidades de la organización	Establece unas medidas de seguridad obligatorias según el nivel de criticidad, que además se pueden completar con otras según las necesidades.
El catálogo de medidas tiene 133 controles y se pueden añadir otros	El catálogo tiene 75 medidas de seguridad

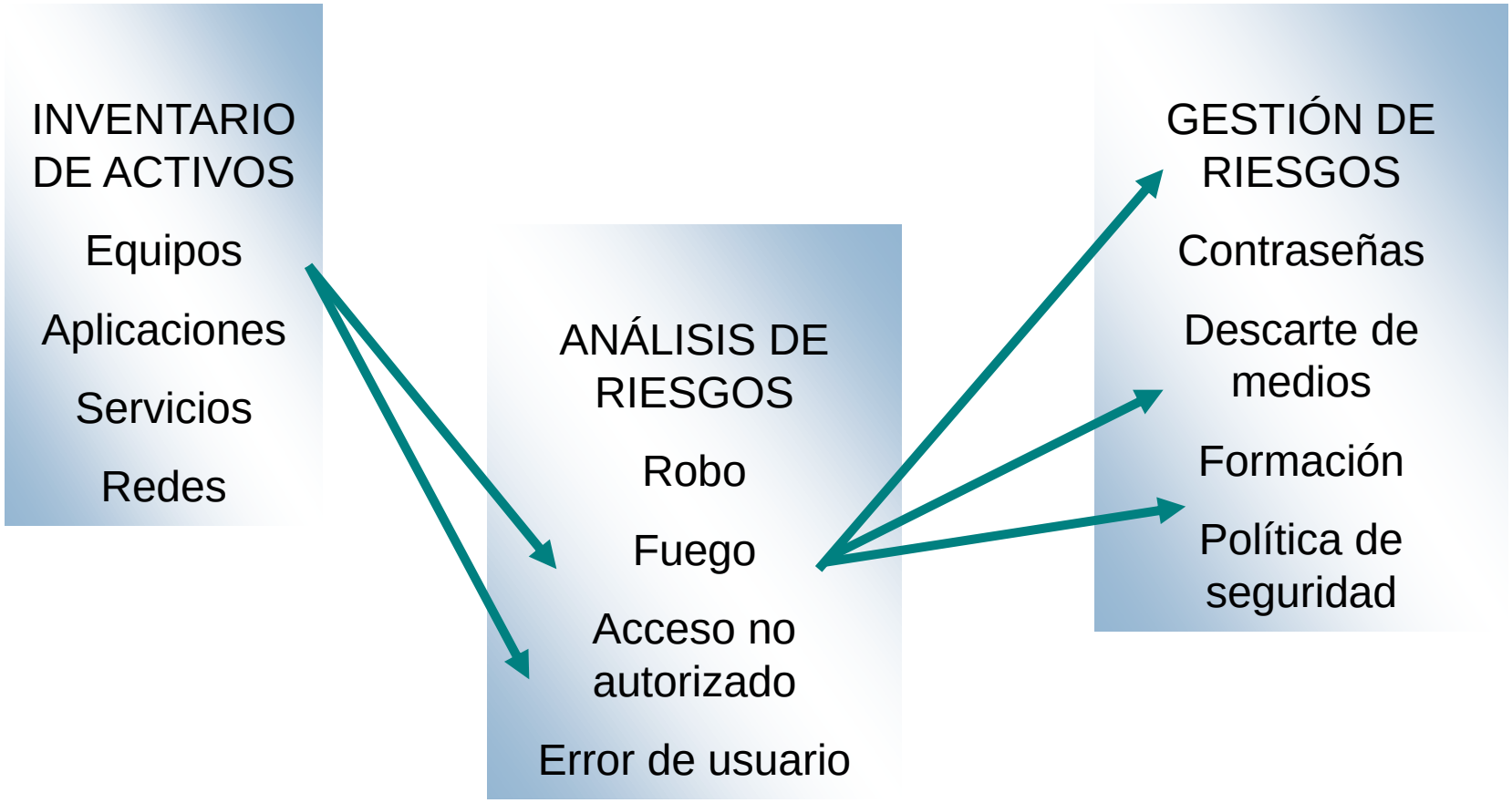
Correspondencia ENS- ISO 27001 I

ENS	REQUISITO	ISO 27001
11	Política de Seguridad	4.2.1.b)
12	Compromiso de la dirección	5.1.c) d)
13.1 13.2	Evaluación de riesgos	4.2.1.c) d) e)
13.3	Gestión de riesgos	4.2.1.f) g)
27.1	Documento de Aplicabilidad	4.2.1.g)
14 - 15	Formación	5.2.2
34.1	Auditorías	4.2.3.e) - 6
26	Mejora continua	8.1

Correspondencia ENS- ISO 27001 II

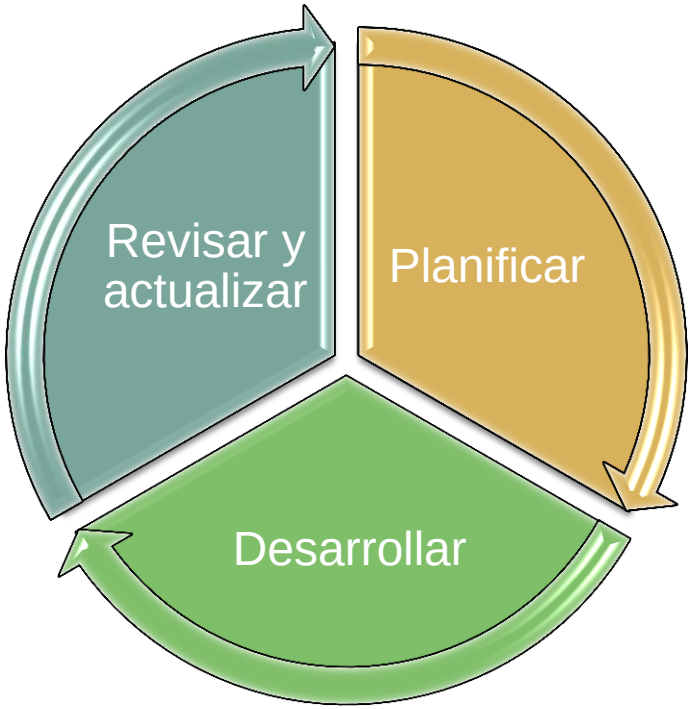
ENS	REQUISITO	ISO 27001
14.3	Uso aceptable de los activos	A7.1.3
14.4	Gestión de privilegios de los usuarios	A10.10.1 A11.2
15.3	Controlar los riesgos de terceros	A6.2
16	Gestión de altas y bajas de usuarios	A11.2.1
17	Control de acceso	A9.1
25	Copias de seguridad	A10.5.1 - 14.1
24.1	Política de prevención de malware	A10.4
24.2	Gestión de incidentes	A13.1 - A13.2
27.2	LOPD	A15.1.4

Elementos del SGSI



Proyecto de implantación

- Planificar la implantación
  - Organizar el Comité de Gestión
  - Realizar plan de acción
  - Establecer objetivos
  - Recopilar información
- Desarrollar
  - Políticas
  - Inventario de activos
  - Categorización de sistemas
  - Análisis de riesgos
  - Documento de aplicabilidad
  - Normativa de seguridad
  - Procedimientos
  - Formación
- Revisar y actualizar
  - Verificar y validar objetivos
  - Auditorías



Planificación

- Crear y definir el/los Comité/s de Gestión, responsable de velar por el cumplimiento de la política de seguridad de la organización y establecer los objetivos.
- Establecer el plan de acción
- Recopilar la información necesaria:
  - Normativa aplicable
  - Normativa existente
  - Servicios que se prestan
  - Infraestructura para la prestación de los servicios
  - Medidas de seguridad

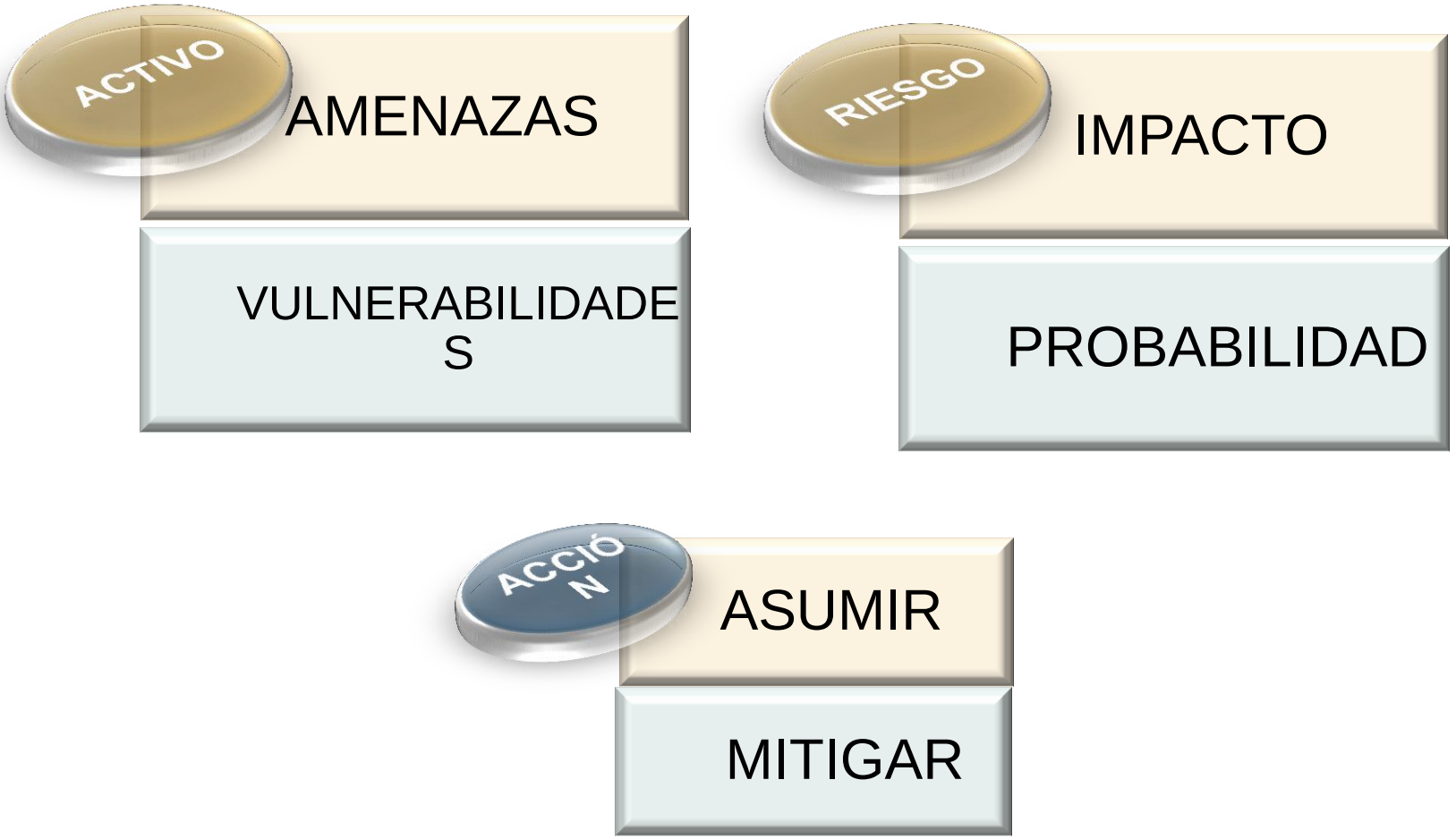
Desarrollo I

- Definir las Políticas de Seguridad y de Gestión de Servicios
- Definir el conjunto de activos dentro del alcance del proyecto
- Identificar los sistemas existentes en la organización y valorarlos de acuerdo a las dimensiones de seguridad especificadas en el ENS
- Determinar la categoría del sistema o sistemas identificados
- Realizar el análisis de riesgos
- Establecer el nivel aceptable de riesgo

Categorización de Sistemas

	SERVICIOS		INFORMACIÓN		SISTEMA
Criterios	Gestión de Nóminas	Gestión de Matrículas	Nóminas	Matrículas	
Confidencialidad	B	M	B	M	M
Integridad	B	M	B	M	M
Autenticidad	B	M	B	M	M
Trazabilidad	B	M	B	M	M
Disponibilidad	B	B	B	M	M

Análisis y gestión de los riesgos



Valoración de Riesgos

Amenazas

ORDENADORES
Fuego
Avería
Acceso no autorizado

DISPOSITIVOS USB
Robo
Degradación del soporte
Contaminación electromagnética

DATOS DE PROYECTOS
Error de usuario
Virus
Fuga de información

- Impacto: alto, medio, bajo
- Probabilidad de ocurrencia: alta media, baja
- Riesgo: Función del valor del activo, el impacto que ocasionaría la amenaza y la probabilidad de que realmente ocurra dicha amenaza

Gestión de Riesgos

Para reducir los riesgos detectados en el análisis de riesgos, se seleccionarán controles apropiados

DATOS DE PROYECTOS

Error de usuario → Formación, Asignación de responsabilidades

Virus → Programas antivirus, Copias de seguridad

Fuga de información → Gestión de contraseñas, Control de accesos a redes

Desarrollo II

- Determinar las medidas de seguridad del Anexo 1 que aplican a los sistemas según su nivel
- Determinar las medidas de seguridad a aplicar también teniendo en cuenta los resultados del Análisis de Riesgos
- Documentar la Declaración de Aplicabilidad
- Definir la Normativa de Seguridad, detallando cómo y quien hace las distintas tareas
- Definir la Normativa de Gestión de Servicios de TI
- Formar a todo el personal sobre la política, normativa y procedimientos.

Revisar y actualizar

- Evaluar los objetivos midiendo la eficacia de las medidas adoptadas
- Revisar el sistema de gestión para mantenerlo actualizado
- Realización de auditorías de cumplimiento de las normas aplicables, tanto externas como internas (procedimientos)
- Planificar y ejecutar las acciones correctoras y preventivas necesarias para corregir y evitar no conformidades

Gracias por su atención

Dudas y preguntas

START-UP S.L.
www.esquemanacionaldeseguridad.es
www.seguridadinformacion.com
info@seguridadinformacion.com