BASTIONADO DE REDES Y SISTEMAS

TEMA 2: DISEÑO DE PLANES DE SECURIZACIÓN

INTRODUCCIÓN AL TEMA

1

En este tema vamos a repasar todos los conceptos relacionados con el diseño de planes de securización en una empresa, a todos los niveles.

2

Ciertamente la teoría tiene mucho peso en esta unidad, pero sienta las bases necesarias para aclarar conceptos y poder continuar trabajando los siguientes temas.

3

Recuerda que vuestras aportaciones tienen tanto valor (o incluso más) que lo que se de en estas diapositivas.

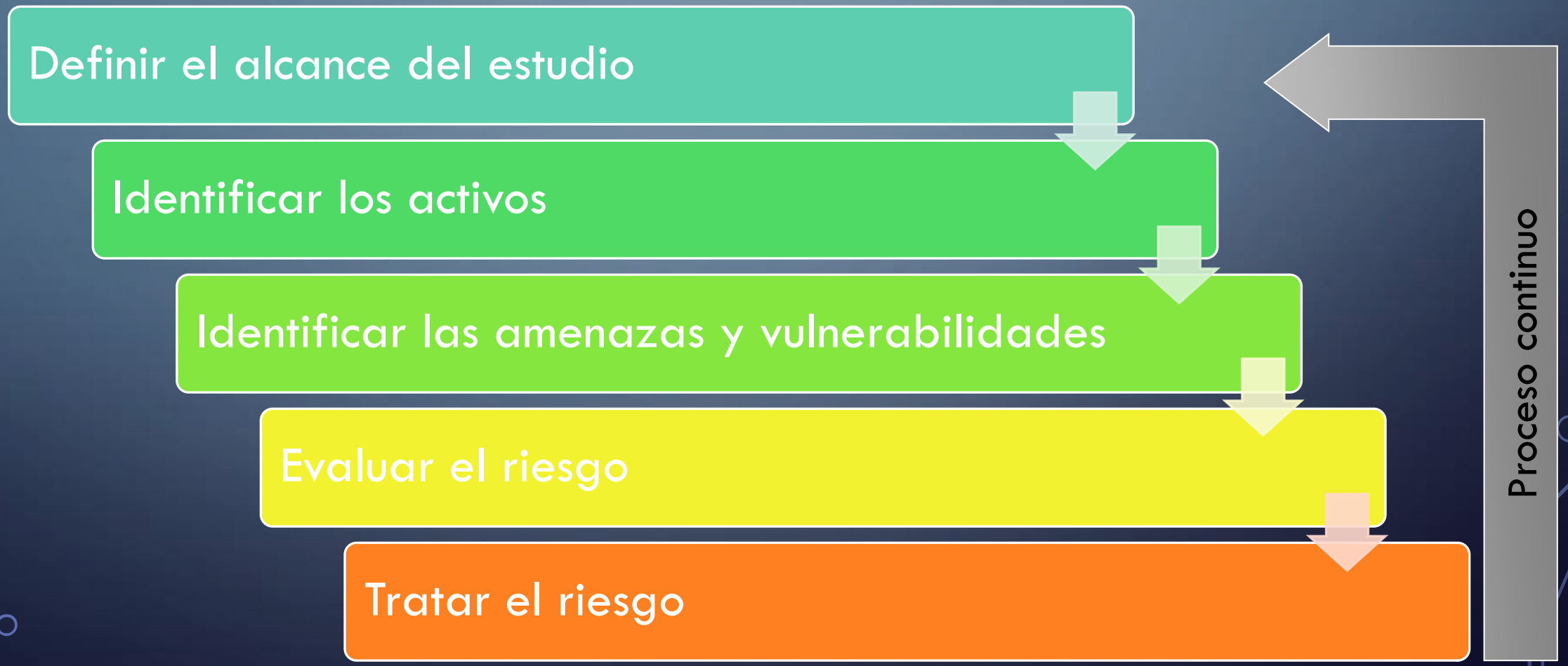
PRINCIPIOS DE LA ECONOMÍA CIRCULAR EN LA INDUSTRIA 4.0

- Antiguo paradigma: Producir, usar y tirar.
  - Hasta hace no demasiado, esa era la idea principal en la industria.
  - Descubrimos que los recursos eran limitados, y los desechos demasiados.
- Nuevo paradigma: Reducir, reusar y reciclar.
  - La digitalización y el Big Data están ayudando a cambiar la forma en que las empresas trabajan.
- La ciberseguridad se basa en este nuevo paradigma, ya que minimiza los recursos, incrementa la productividad y reutiliza toda la información para reinventarse y mejorarse.

ANÁLISIS DE RIESGOS

- Si consideramos que las herramientas tecnológicas y la información es el principal activo de nuestra empresa, analizar los riegos potenciales y actuar para minimizarlos debe ser la prioridad número 1.
- Este análisis se considera dentro del **Plan Director de Seguridad** (PDS), que es un conjunto de proyectos dirigidos a reducir los riegos de la organización, a partir de una situación inicial.
- Minimizando los riesgos, minimizamos el tiempo perdido resolviéndolos y por lo tanto, maximizamos el tiempo de trabajo útil.

FASES DEL ANÁLISIS DE RIESGOS



FASE 1: DEFINIR EL ALCANCE DEL ESTUDIO

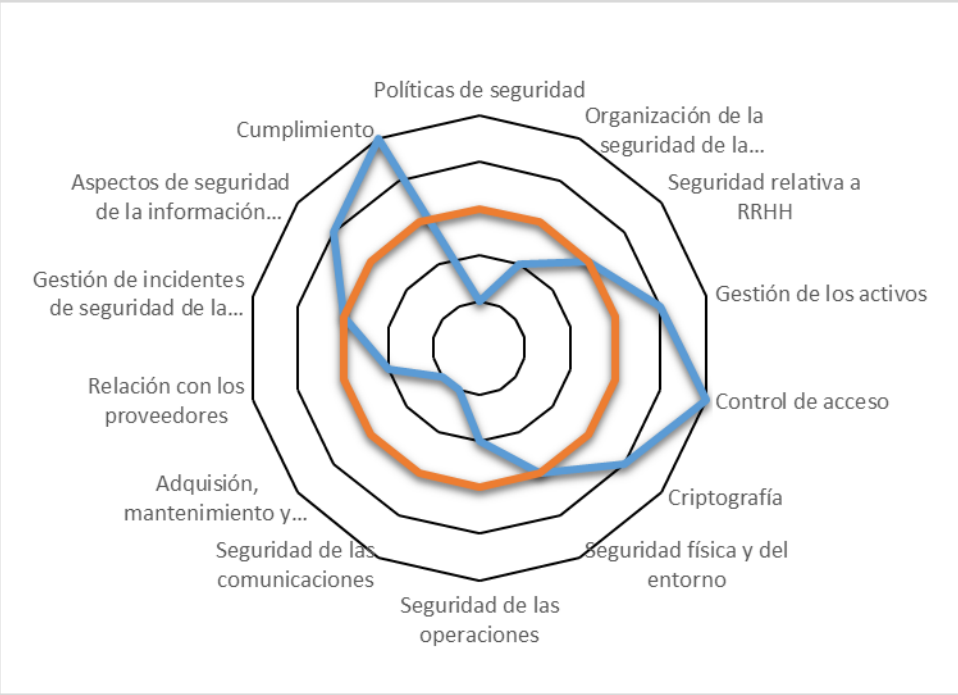
Capítulo 1: Políticas de seguridad de la información	Capítulo 2: Organización de la Seguridad de la Información	Capítulo 3: Seguridad relativa a los recursos humanos	Capítulo 4: Gestión de los activos
Capítulo 5: Control de acceso	Capítulo 6: Criptografía	Capítulo 7: Seguridad física y del entorno	Capítulo 8: Seguridad de las operaciones
Capítulo 9: Seguridad de las comunicaciones	Capítulo 10: Adquisiciones, desarrollo y mantenimiento de los sistemas de información	Capítulo 11: Relación con los proveedores	Capítulo 12: Gestión de incidentes de seguridad de la información
	Capítulo 13: Aspectos de seguridad de la información para la gestión de la continuidad del negocio	Capítulo 14: Cumplimiento	

Conjunto de normas ISO/IEC 27002:2017

Se aplicarían solo las que encajen con el negocio

FASE 1: DEFINIR EL ALCANCE DEL ESTUDIO

Dominio	Puntuación [1-5]	Objetivo [1-5]
Políticas de seguridad	1	3
Organización de la seguridad de la información	2	3
Seguridad relativa a RRHH	3	3
Gestión de los activos	4	3
Control de acceso	5	3
Criptografía	4	3
Seguridad física y del entorno	3	3
Seguridad de las operaciones	2	3
Seguridad de las comunicaciones	1	3
Adquisición, mantenimiento y desarrollo de los Sistemas de la Información	1	3
Relación con los proveedores	2	3
Gestión de incidentes de seguridad de la información	3	3
Aspectos de seguridad de la información para la gestión de la continuidad del negocio	4	3
Cumplimiento	5	3



ACTIVIDAD 1

- Realizar la actividad de Moodle: Plan de securización: Fase 1.
  - Se valorará:
    - Un correcto trabajo con la herramienta Excel.
    - NOTA: para hacer los gráficos radiales se puede consultar algún vídeo de Youtube, ejemplo: https://www.youtube.com/watch?v=hKe_jp6dqo4
  - Penaliza:
    - Alejarse demasiado del tipo de gráfica solicitada.

FASE 2: IDENTIFICAR LOS ACTIVOS

- Una vez tenemos el alcance del estudio definido, averiguamos los activos más importantes asociados.

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

ACTIVIDAD 2

- Realizar la actividad de Moodle: Plan de securización: Fase 2.
  - Se valorará:
    - Identificar correctamente todos los elementos relevantes del texto.
  - Penaliza:
    - Rellenar la tabla de forma incorrecta.

FASE 3: IDENTIFICAR LAS AMENAZAS Y VULNERABILIDADES

- Conocidos los activos, ahora toca intentar anticiparse a las amenazas a las que pueden estar expuestos.
- **Una vulnerabilidad** es algún punto débil que pueda tener el activo.
- **Las amenazas** son muchas y muy variadas, por lo que en todo momento se debe tener un enfoque práctico:
  - Un servidor podría ser derribado por un helicóptero Apache, pero no por ello vamos a incluir esa amenaza en nuestra lista, ya que es muy poco probable.

FASE 3: IDENTIFICAR LAS AMENAZAS Y VULNERABILIDADES

- Si existe la amenaza y existe la vulnerabilidad, entonces SÍ que tenemos un riesgo, y hay que anotarlo.
- Ejemplo: Servidor donde se guardan los datos de los clientes.

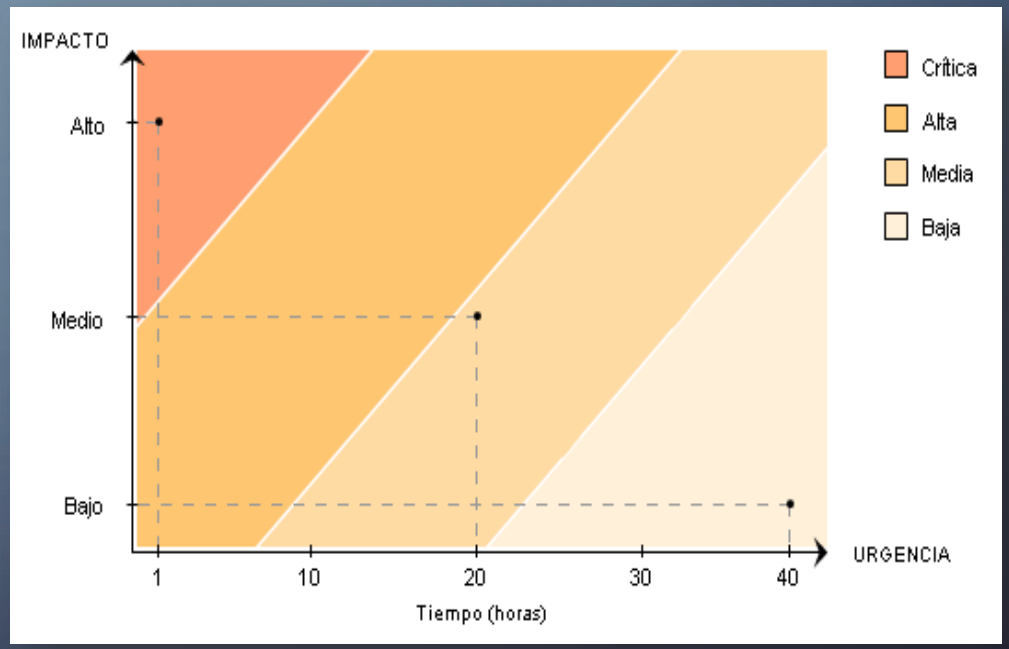
Amenaza	Vulnerabilidad	¿Riesgo?
Pico de tensión	Servidores con protectores de sobretensión	NO
Equipos están en una habitación bien aislados	Poca protección frente a golpes	NO
Ataque de fuerza bruta	Clave de administrador débil	**SI**

ACTIVIDAD 3

- Realizar la actividad de Moodle: Plan de securización: Fase 3.
  - Se valorará:
    - La capacidad de imaginar diferentes y variados riesgos y vulnerabilidades.
  - Penaliza:
    - Listar menos de tres amenazas/vulnerabilidades por activo.

FASE 4/5: EVALUAR/TRATAR EL RIESGO

- Una vez tenemos toda la documentación anteriormente creada, ya estamos en condiciones de ordenar los riesgos según su probabilidad de aparición.
- Usaremos una tabla donde los clasificaremos por **impacto** (bajo, medio, alto) y por el **tiempo que se tardarían en resolver** (por horas).
- Finalmente daremos medidas a aplicar para mitigarlos, atendiéndolos según su nivel.



ACTIVIDAD 4

- Realizar la actividad de Moodle: Plan de securización: Fases 4 y 5.
  - Se valorará:
    - La capacidad de generar la tabla y rellenarla.
  - Penaliza:
    - Organizar los riesgos de forma poco realista.

CUERPO DOCUMENTAL DE SEGURIDAD

POLÍTICA	PROCEDIMIENTO	GUÍA
• Es la visión que la dirección de la empresa tiene sobre cómo se deben proteger los activos. • Debe ser captada por todos los miembros de la empresa. • Es muy general, y no entra en aspectos concretos.	• Explican cómo se hace algo paso a paso, aunque no entran al detalle en la tecnología usada. • Pueden listar paso a paso la implementación de una política.	• Especifican los pasos definidos por los procedimientos, pero en este caso, ya lo hacen sobre un.a tecnología definida
Todos los trabajadores de la empresa deben identificarse antes de acceder a las instalaciones.	*Es necesario hacer uso de las tarjetas de identificación siempre que se entra en la oficina.*	*Cada vez que un empleado entra por la puerta, debe pasar su tarjeta identificativa por la zona amarilla del lector RFID que se encuentra en la pared, y esperar que el LED se ilumine en verde, que significará que el proceso se ha completado satisfactoriamente.*

POLÍTICAS DE SECURIZACIÓN MÁS HABITUALES

Control de acceso	Dispositivos móviles	Relaciones con los proveedores
Clasificación y manejo de la información	Restricciones en el uso/instalación del software	Gestión de incidentes de ciberseguridad
Seguridad física y ambiental	Copias de respaldo	Plan de continuidad del negocio
Uso adecuado de activos	Protección ante software malicioso	Formación y concienciación en ciberseguridad
Transferencia de la información	Gestión de vulnerabilidades	Seguridad en las operaciones

ACTIVIDAD 5

- Realizar la actividad de Moodle: Ejemplos de políticas de securización.
  - Se valorará:
    - La capacidad de imaginar diferentes y variadas políticas.
  - Penaliza:
    - Que las políticas no tengan sentido o sean de imposible aplicación.

LAS INCIDENCIAS

- **Recuerda**: El análisis de riesgos nos sirve para minimizar las incidencias.
- Sin embargo, **ni el mejor trabajo nos asegurará al 100% que hayan desaparecido**, por lo que la empresa debe contar también con protocolos para atender a las incidencias que sucedan día a día.
- Lo normal también es que las incidencias **sucedan de forma concurrente**, por ello es importante saber clasificarlas, y así actuar de forma ordenada y eficiente.

DOCUMENTACIÓN EN PROTOCOLO DE ESCALADO

1. **Registro de la incidencia**: Debe hacerse lo antes posible, ya que con el paso del tiempo puede resultar más costoso o incluso hacer que aparezcan otras nuevas.
2. **Clasificación de la incidencia**: Recopilar toda la información relevante
   - Categorización.
   - Establecer el nivel de prioridad.
   - Asignar recursos.
   - Monitorizar el estado y el tiempo de respuesta.
3. **Documentar** análisis, resolución y cierre (MUY IMPORTANTE).

ESCALADOS EN ATENCIÓN A INCIDENCIAS

- En ocasiones, el departamento encargado de gestionar incidencias puede verse incapaz de resolverla. En esos casos es necesario tener previsto un plan para que **la incidencia suba al siguiente nivel**.
- Existen dos tipos de escalado:
  - Escalado funcional: El departamento no escala la incidencia, pero sí que necesita apoyo de un especialista de más alto nivel.
  - Escalado jerárquico: Es necesario pasar la incidencia al siguiente nivel, ya que se deben tomar decisiones que se escapan a las atribuciones que tiene el nivel actual.