

DEPARTAMENTO DE SEGURIDAD

Alexandra McCulloch y Paloma Pérez de Madrid





AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas



AGENDA

- 1) **¿Quiénes somos?**
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

¿QUIÉNES SOMOS?



Directora de Seguridad

Paloma Pérez de Madrid

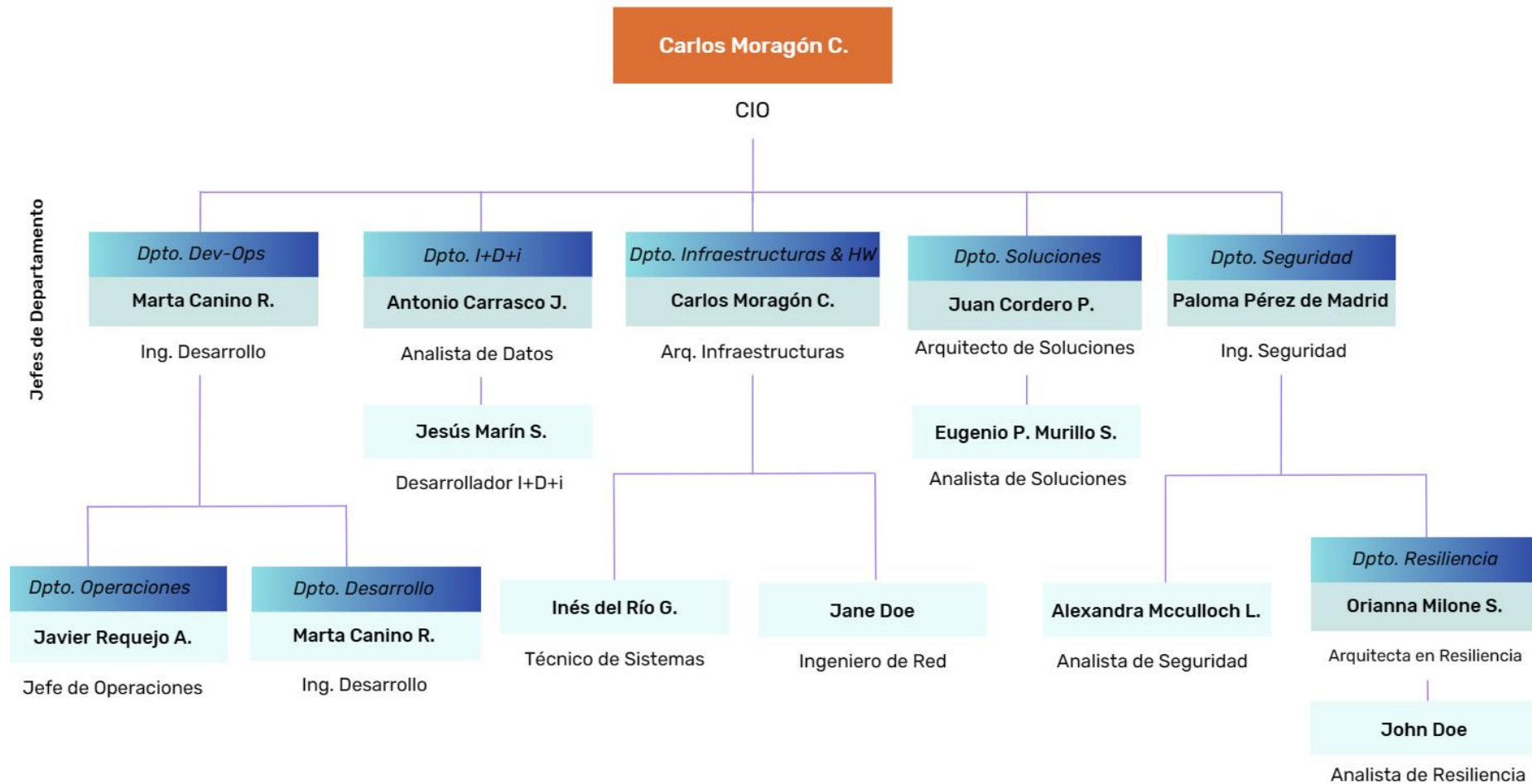


Subdirectora de Seguridad

Alexandra McCulloch

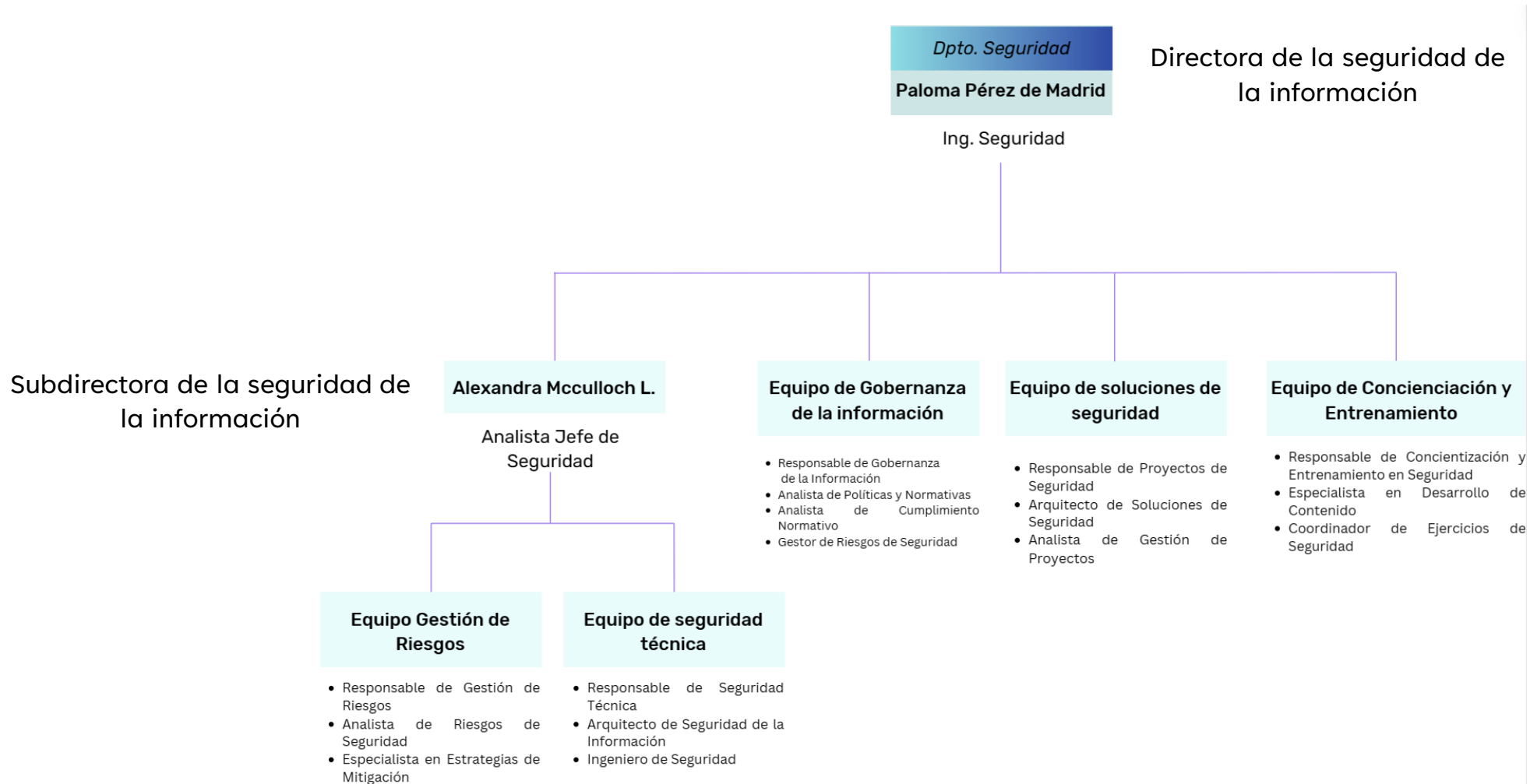
¿QUIÉNES SOMOS?

Organigrama



¿QUIÉNES SOMOS?

Organigrama



¿QUIÉNES SOMOS?

Equipos

Equipo de Gobernanza de la información

- Responsable de desarrollar y mantener **políticas, estándares y directrices** de seguridad de la información.
- Monitoreo y aseguramiento del cumplimiento de las normas de seguridad por parte de toda la organización.

Equipo de soluciones de seguridad

- Priorizar y establecer el **alcance** del proyecto
- **Orientar:** Hacer inventario de los activos y sistemas de la organización e identificar normativas aplicables, un enfoque de riesgo y las amenazas a las que la organización podría estar expuesta
- Creación del **Perfil Actual:** Realice una evaluación de riesgos
- Creación **Perfil Objetivo**
- Creación de un **plan de acción**

¿QUIÉNES SOMOS?

Equipos

Equipo de Concienciación y Entrenamiento

- Desarrollo e implementación de **programas de concientización** en seguridad para empleados
- Formación continua sobre prácticas de seguridad y políticas de la organización
- Coordinación de **simulacros** de phishing y otros ejercicios de seguridad.

Equipo Gestión de Riesgos

- Identificación y evaluación de **riesgos** de seguridad de la información.
- Desarrollo de estrategias y controles para mitigar los riesgos identificados.
- Realización de evaluaciones de riesgos periódicas y revisiones de impacto en la seguridad.

¿QUIÉNES SOMOS?

Equipos

Equipo de seguridad técnica

- Implementación y gestión de **controles técnicos** de seguridad, como firewalls, sistemas de detección de intrusiones y antivirus.
- Monitoreo de la infraestructura de TI para detectar y responder a posibles amenazas y vulnerabilidades.



AGENDA





- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) **¿Qué es la ciberseguridad?**
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

¿QUÉ ES LA CIBERSEGURIDAD?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad




↳ Esfuerzo continuo de ^{proteger}   Organizaciones de ataques digitales
Gobiernos
mediante   de Sistemas + datos en la red

¿QUÉ ES LA CIBERSEGURIDAD?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad

↳ Esfuerzo continuo de  ^{proteger}  Organizaciones de ataques digitales
Gobiernos
mediante  de Sistemas + datos en la red

3 Niveles de Protección:

telePresencia

a nivel Personal,   identidad
datos
dispositivos informáticos

ORGanizacional

a nivel Corporativo,   Reputación
Datos
clientes

Gobierno

nivel gubernamental  seguridad nacional
Estabilidad €
seguridad & bienestar 

BREAKPOINT

(si el cliente
es el Gobierno)

¿QUÉ ES LA CIBERSEGURIDAD?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad

Seguridad de la información

↓
info en 3 dimensiones

→ cifrado datos, Autenticación,
control acceso

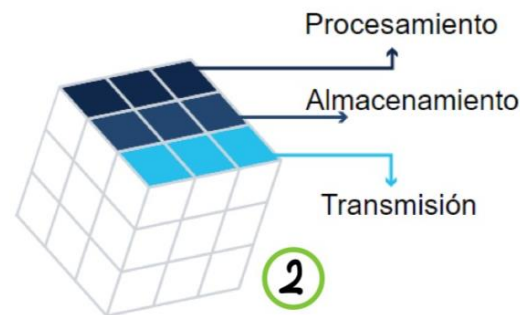
Confidencialidad

Integridad

Hash e suma
comprobación

Disponibilidad

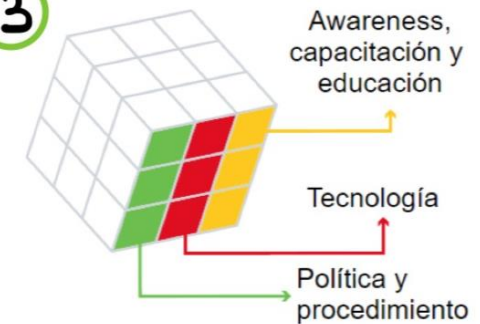
1



2

- 1) Principios Fundamentales de Sist de info.
- 2) Protección info en cada uno → estados posibles
- 3) Medidas de seguridad ⇒ Protección Datos

3



Conclusión: La protección cibernética es compleja y laboriosa

¿QUÉ ES LA CIBERSEGURIDAD?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad

¿A qué riesgos se enfrentan la mayoría de las empresas?



Spyware

Adware

BackDoor

sw q ^{especa} _{monitorea}

RansomWare

cautivo un sist
(hasta q realice €€)

StareWare

• ventanas emergentes sistema crítico ⚠
• al hacer clic → descargas sw malicioso

Virus

Troyano

Gusano



Ciberataques básicos:

- Las empresas deben de estar al día de las nuevas vulnerabilidades
- La rapidez es crucial para no comprometer los sistemas

¿QUÉ ES LA CIBERSEGURIDAD?

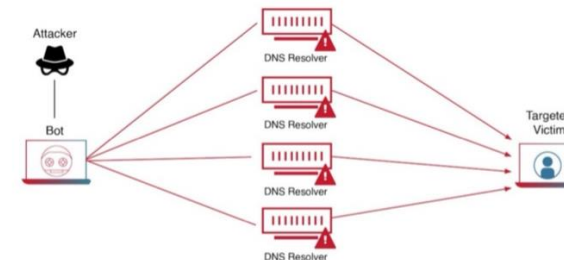
Protección Frente a :

1) Ingeniería Social

- + Pretexto: atacante llama a una A y miente → obtener acceso datos
- + Infiltración (tailgating): atacante sigue rápidamente A autorizada
- + Una cosa por otra (quid pro quo): solicita info personal a cambio de algo (regalo gratis)

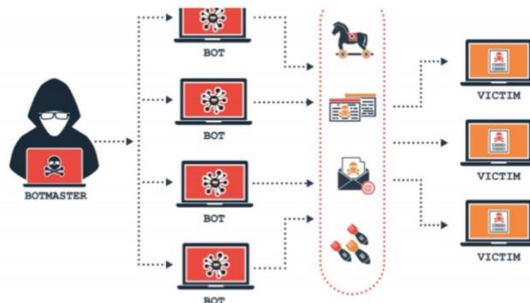
2) Denegación del Servicio (DoS)

- + Cantidad ↑↑ Tráfico
- + Paquetes maliciosos formateados



3) DoS distribuido (proviene de N fuentes)

4) Botnet (Grupo de bots)



¿cómo?

- Firewall: detecta tráfico de bots infectados
- Servicio Cisco Security Intelligence Operations (SIO): basado en la nube, filtros actualizados al Firewall → nuevos botnets conocidos



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad



¿QUÉ ES LA CIBERSEGURIDAD?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad

5) Ataques en el camino

interceptan/modifican \rightarrow entre 2 dispositivos

- Man in the Middle (MITM): usuario no lo sabe
- Man in the Mobile (MitMo): MITM para dispositivo móvil
Ej de Paquete: "Zeus"
con \rightarrow SMS

6) Envenenamiento SEO

sitio web Malicioso \rightarrow se posiciona

7) Ataques de contraseña

8) Amenazas Persistentes Avanzadas (APT) (largo plazo, múltiples fases, sigilosas, ...)





¿CUÁNTO LE CUESTA A LA
EMPRESA **PROTEGERSE** DE
ESTOS **RIESGOS BÁSICOS**?

¿QUÉ ES LA CIBERSEGURIDAD?

Vulnerabilidad	Tiempo estimado	Recursos económicos	Recursos humanos	Complejidad (1-5)
Ingeniería social	2-4 semanas	Bajos	1-2 personas	3
DoS	1-2 semanas	Medios	2-3 personas	3
DoS Distribuido	4-6 semanas	Altos	3-4 personas	4
BotNet	8-12 semanas	Altos	4-6 personas	5
Ataques de contraseñas	1-3 semanas	Medios	2-3 personas	3
Ataques Man in the middle	4-6 semanas	Medios	3-4 personas	4
Envenenamiento SEO	2-4 semanas	Bajos	1-2 personas	3
Ataques de contraseña	1-3 semanas	Medios	2-3 personas	3
Amenazas Persistentes Avanzadas (APT)	12-24 semanas	Altos	5-7 personas	5

¿QUÉ ES LA CIBERSEGURIDAD?

¿Qué hace nuestra empresa?



**BREAKPOINT
TECHNOLOGIES**

Empresa de consultoría
y soluciones de
seguridad

Al día de las últimas
vulnerabilidades

Capacitada para
asumir la
complejidad

Respuesta rápida
ante ataques

Optimización de
recursos económicos

Seguridad de la arquitectura de la empresa

- Implementación de Firewalls y Seguridad Perimetral
- Seguridad de Redes Privadas Virtuales (VPN)
- Detección y Prevención de Intrusiones (IDS/IPS)
- Seguridad de la Arquitectura en la Nube
- Respuesta a Incidentes de Seguridad
- ...

Seguridad del Software

- Pruebas de Penetración
- Gestión de Vulnerabilidades
- Seguridad del Desarrollo de Software
- Seguridad de Aplicaciones Web
- Gestión de Parches
- ...



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) **¿Qué hace el departamento de seguridad?**
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas



¿QUÉ HACE EL DEPARTAMENTO DE SEGURIDAD?

- Se dedica a **salvaguardar la seguridad en todos los niveles de la empresa**, centrándose en la **gestión y rastreo de incidentes** de seguridad.
- Esto implica **registrar, clasificar y gestionar los incidentes**, asegurando un **seguimiento exhaustivo de su resolución** y **documentando cada acción** tomada para mitigar riesgos y prevenir futuros incidentes.
- Asimismo, se encarga de **coordinar los cambios en la infraestructura de TI**, asegurando que se realicen de manera planificada y controlada para minimizar cualquier riesgo de seguridad que pueda surgir durante el proceso.

¿CÓMO LO HACE?

- Se lleva a cabo un **análisis de vulnerabilidades**, utilizando como referencia la norma ISO/IEC 29147:2018, donde se **identifican, clasifican y comunican** las vulnerabilidades utilizando los estándares CVE y CVSS.
- Para realizar **pruebas controladas de explotación de vulnerabilidades**, se adopta la metodología ISSAF.
- Posteriormente, se **solucionan estas vulnerabilidades** basándose en el ISO 27001, priorizando y coordinando la aplicación de parches y correcciones.



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) **Estándares de Seguridad**
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

ESTÁNDARES DE CIBERSEGURIDAD

Estándar / Framework	Definición
ISO 27000	Una serie de estándares que abordan aspectos relacionados con la seguridad de la información y proporcionan un marco para que las organizaciones establezcan y mantengan sistemas de gestión de seguridad de la información efectivos.
NERC	Este estándar se enfoca en desarrollar regulaciones para reforzar los sistemas eléctricos desde una perspectiva de ciberseguridad.
NIST Cyber Security Framework	Proporciona un enfoque basado en riesgos para evaluar y mejorar la ciberseguridad de una organización.
ISO 15408 (Common Criteria)	Este estándar internacional se centra en la evaluación de la seguridad de productos y sistemas de tecnología de la información . Ayuda a determinar si un producto o sistema cumple con los requisitos de seguridad establecidos.
CIS Controls	El Center for Internet Security (CIS) ofrece una lista de 20 controles críticos que las organizaciones pueden implementar para mejorar su postura de seguridad.
FAIR (Factor Analysis of Information Risk)	Proporciona un enfoque cuantitativo para evaluar y comunicar riesgos de seguridad de la información.
ISO 31000	Aunque no está específicamente centrado en ciberseguridad, es un estándar ampliamente utilizado para la gestión de riesgos en general .

ESTÁNDARES DE SEGURIDAD



ISO 27001

- Centra en la gestión integral de la seguridad de la información
- Prestigio (mejora la imagen de la empresa)
- Cumplimiento y normativa



NIST Cyber Security Framework

- Flexibilidad y adaptabilidad (diferentes sectores)
- Enfoque basado en riesgos
- Considera la seguridad desde una perspectiva integral
- Muchas organizaciones gubernamentales y privadas lo consideran como un marco confiable

ESTÁNDARES DE SEGURIDAD

ISO 27000

¿Qué es el ISO 27000?

Una serie de estándares que abordan aspectos relacionados con la seguridad de la información y proporcionan un marco para que las organizaciones establezcan y mantengan **sistemas de gestión de seguridad de la información (SGSI)** efectivos.



SGSI

Marco de políticas y procedimientos diseñado para ayudar a las organizaciones a proteger la **confidencialidad, integridad y disponibilidad** de la información que manejan



ESTÁNDARES DE SEGURIDAD

ISO 27000

27000

Familia de estándares

27001

Requisitos alto nivel

27002

Como lograr los requisitos alto nivel

27003

Guía específica para la implementación de un SGSI

27004

Pautas para la medición y evaluación de un SGSI

27005

Define como identificar, evaluar y tratar los riesgos de seguridad

ESTÁNDARES DE SEGURIDAD

ISO 27000

Controles ISO 27002 punto a punto:

Políticas de seguridad de la información

Organización de seguridad de la información

Gestión de Activos

Control de Acceso

Criptografía

Seguridad Física del entorno

Seguridad de las Operaciones

Seguridad de las Comunicaciones

Adquisición, desarrollo, mantenimiento de los Sistemas de Información

Relación con proveedores

Gestión de Incidentes de la seguridad de la información

Gestión continuidad del negocio

Cumplimiento

ESTÁNDARES DE SEGURIDAD

ISO 27000

Controles ISO 27002 punto a punto:

Políticas de seguridad de la información

Organización de seguridad de la información

Gestión de Activos

Control de Acceso

Criptografía

Seguridad Física del entorno

Seguridad de las Operaciones

Seguridad de las Comunicaciones

Adquisición, desarrollo, mantenimiento de los Sistemas de Información

Relación con proveedores

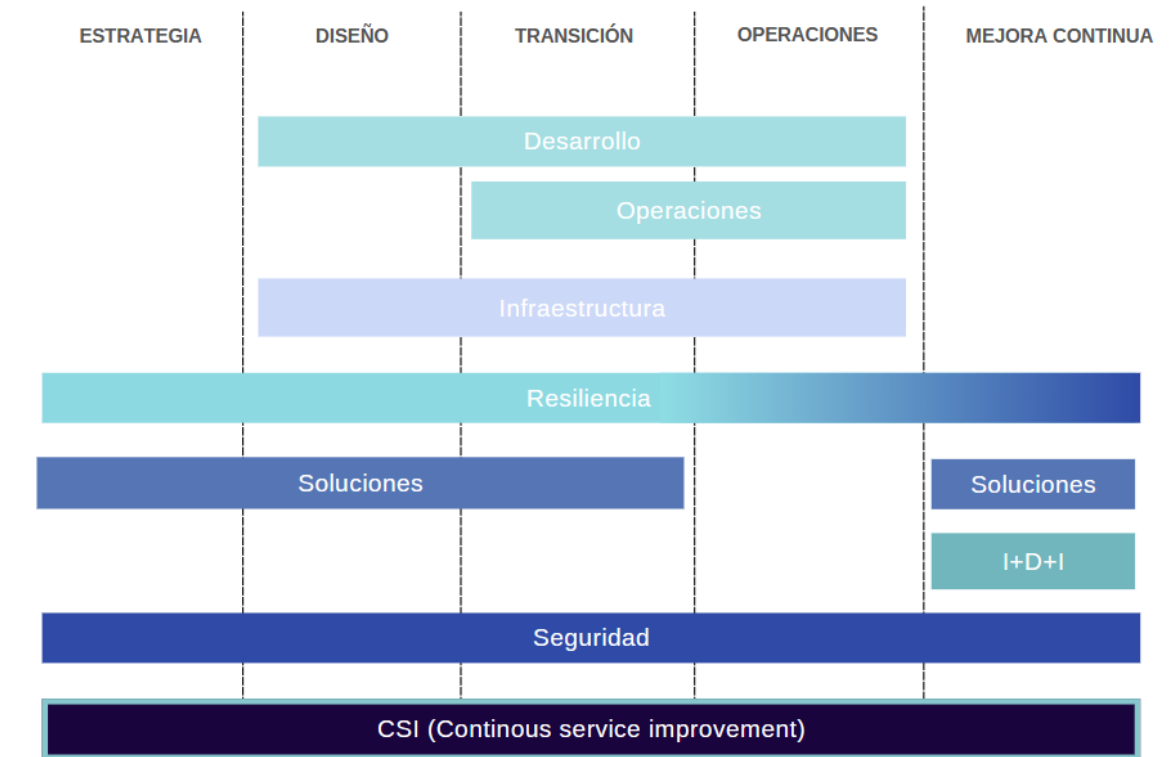
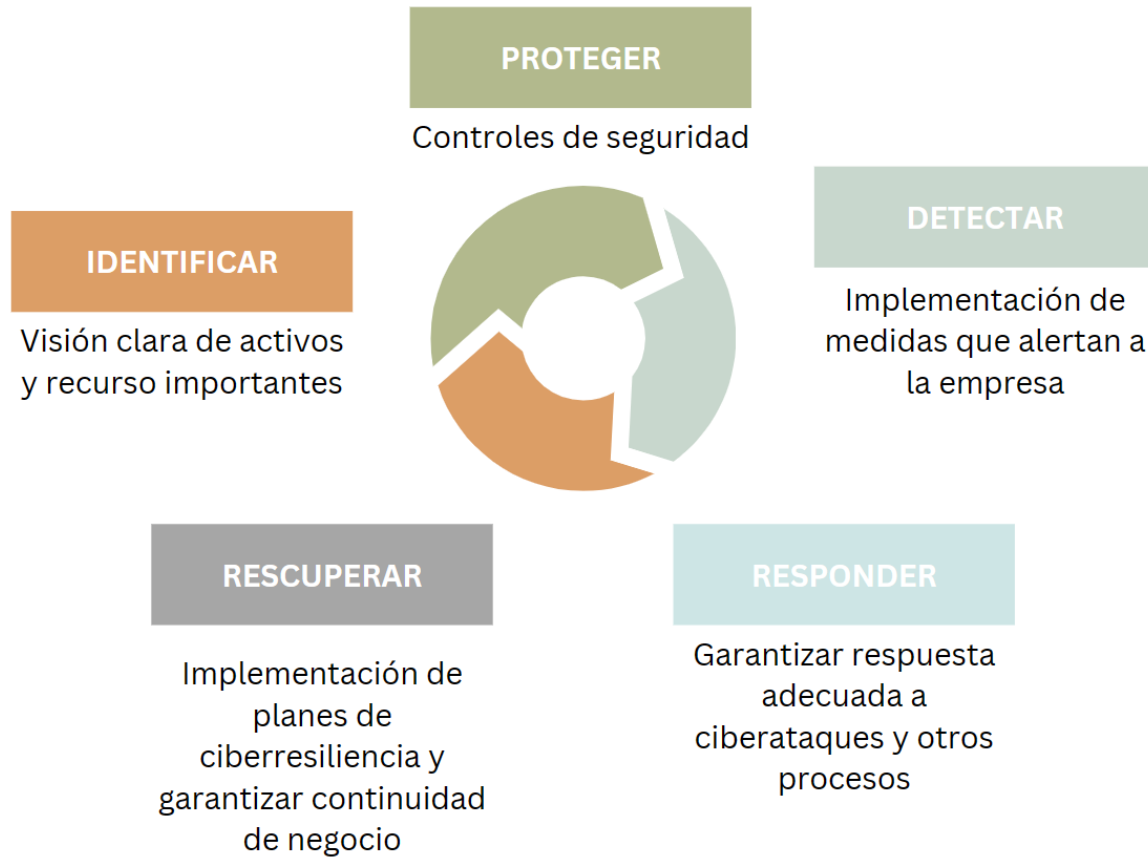
Gestión de Incidentes de la seguridad de la información

Gestión continuidad del negocio

Cumplimiento

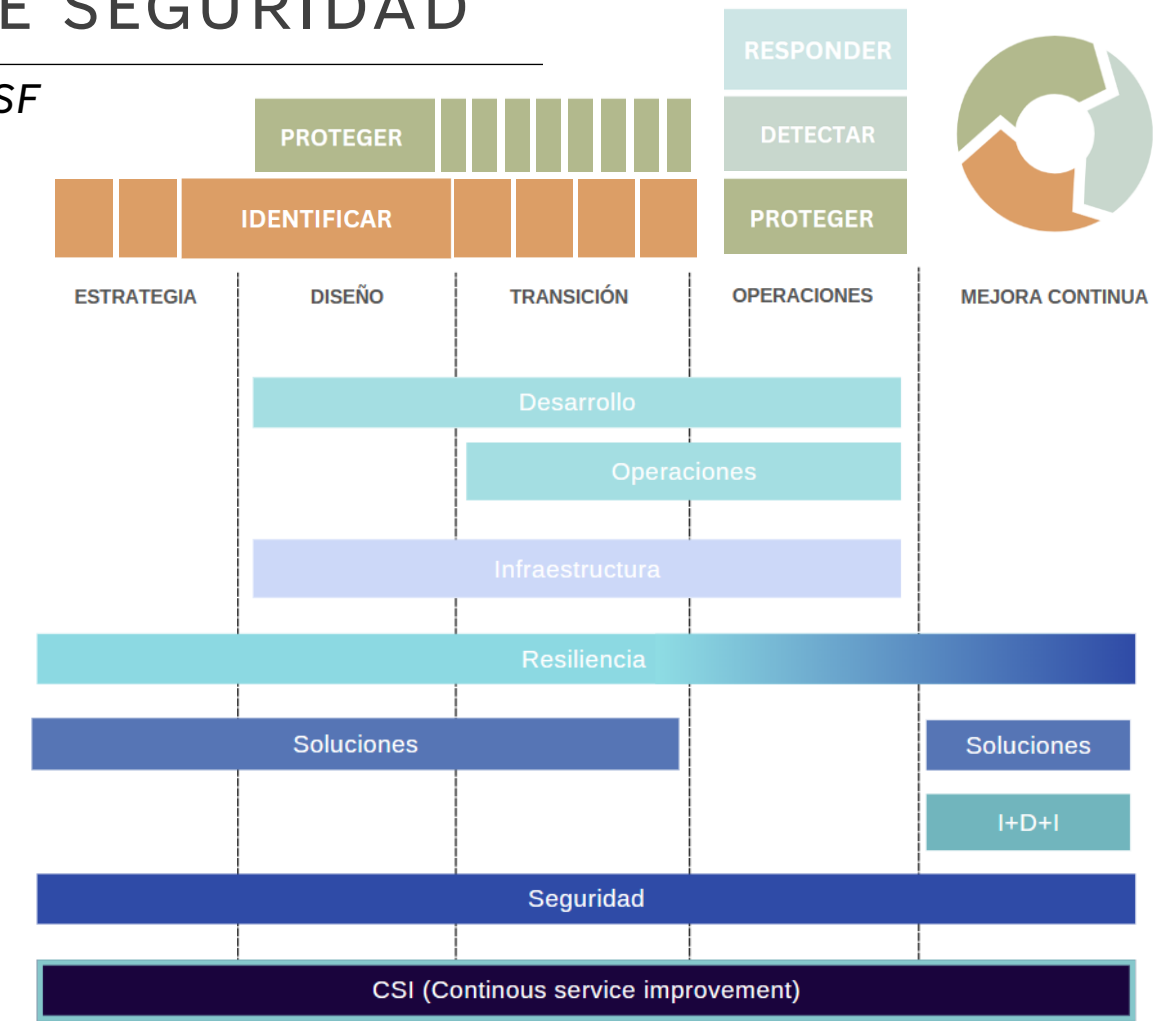
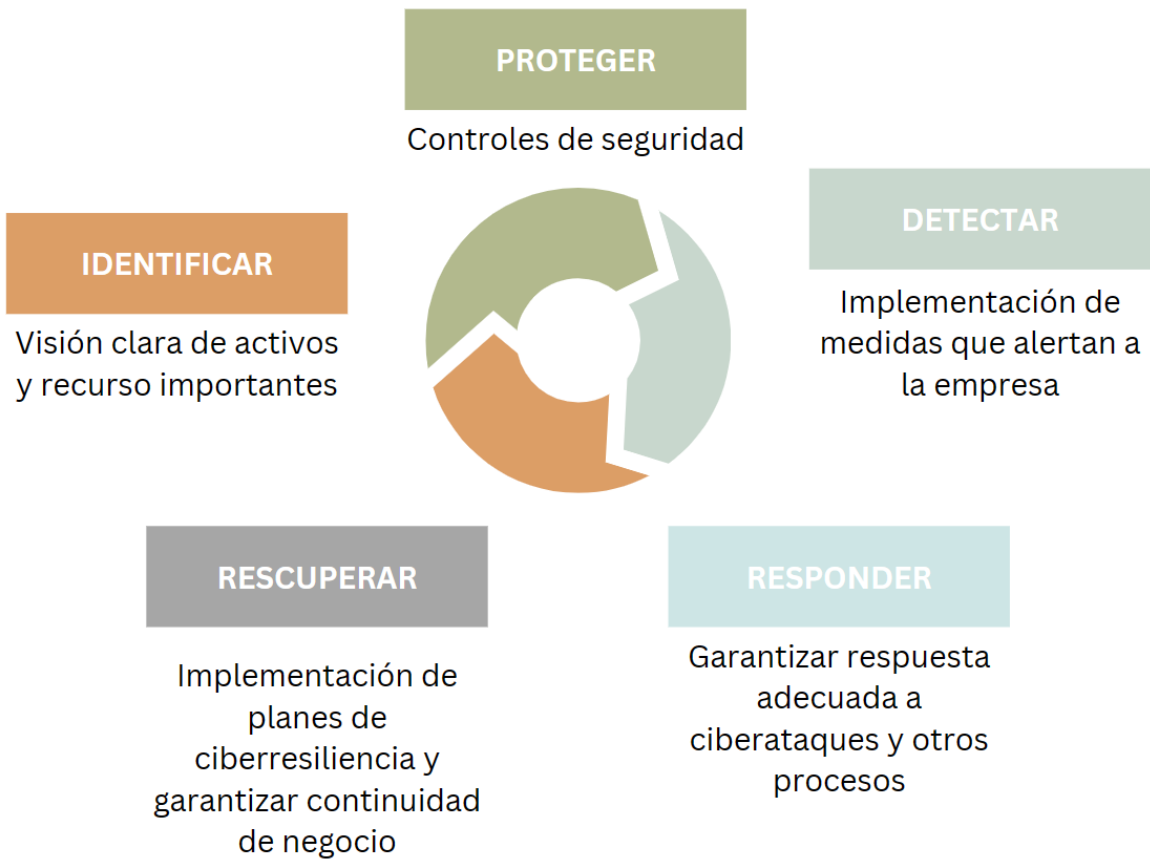
ESTÁNDARES DE SEGURIDAD

NIST CSF



ESTÁNDARES DE SEGURIDAD

NIST CSF





AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) **Leyes cibernéticas europeas y españolas**
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

LEYES CIBERNÉTICAS

ESPAÑA

Esquema Nacional de Seguridad (ENS)

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)



EUROPA

Directiva sobre la seguridad de redes y los sistemas de información (Directiva SRI)

Reglamento de la ciberseguridad de la UE

Directiva SRI 2

Nueva Propuesta: Ley de Ciber Solidaridad de la UE

LEYES CIBERNÉTICAS

Multas de hasta 10M€ o el 2% del volumen de negocios anual

Establece el marco para la certificación de ciberseguridad de las tecnologías de la información y la comunicación (TIC) y otorga un mandato permanente a la Agencia de la UE para la ciberseguridad (ENISA).



EUROPA

Directiva sobre la seguridad de redes y los sistemas de información (Directiva SRI)

Reglamento de la ciberseguridad de la UE

Directiva SRI 2

Nueva Propuesta: Ley de Ciber Solidaridad de la UE

LEYES CIBERNÉTICAS

ESPAÑA

Esquema Nacional de Seguridad (ENS)

Esta normativa se centra principalmente en el sector público y establece los requisitos mínimos de seguridad que deben cumplir los sistemas de información utilizados por las administraciones públicas españolas

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)

1. Designar un **Responsable de Protección de Datos (DPO)**.
2. Realizar **Evaluaciones de Impacto de Protección de Datos (EIPD)**.
3. Notificar brechas de seguridad a la **Agencia Española de Protección de Datos (AEPD)**.
4. Implementar **medidas técnicas y organizativas** para proteger los datos personales.



Multas leves 400€-900€

Multas graves 40.001€-3000.000€

Multas muy graves 20M€-4% del volumen de negocios anual

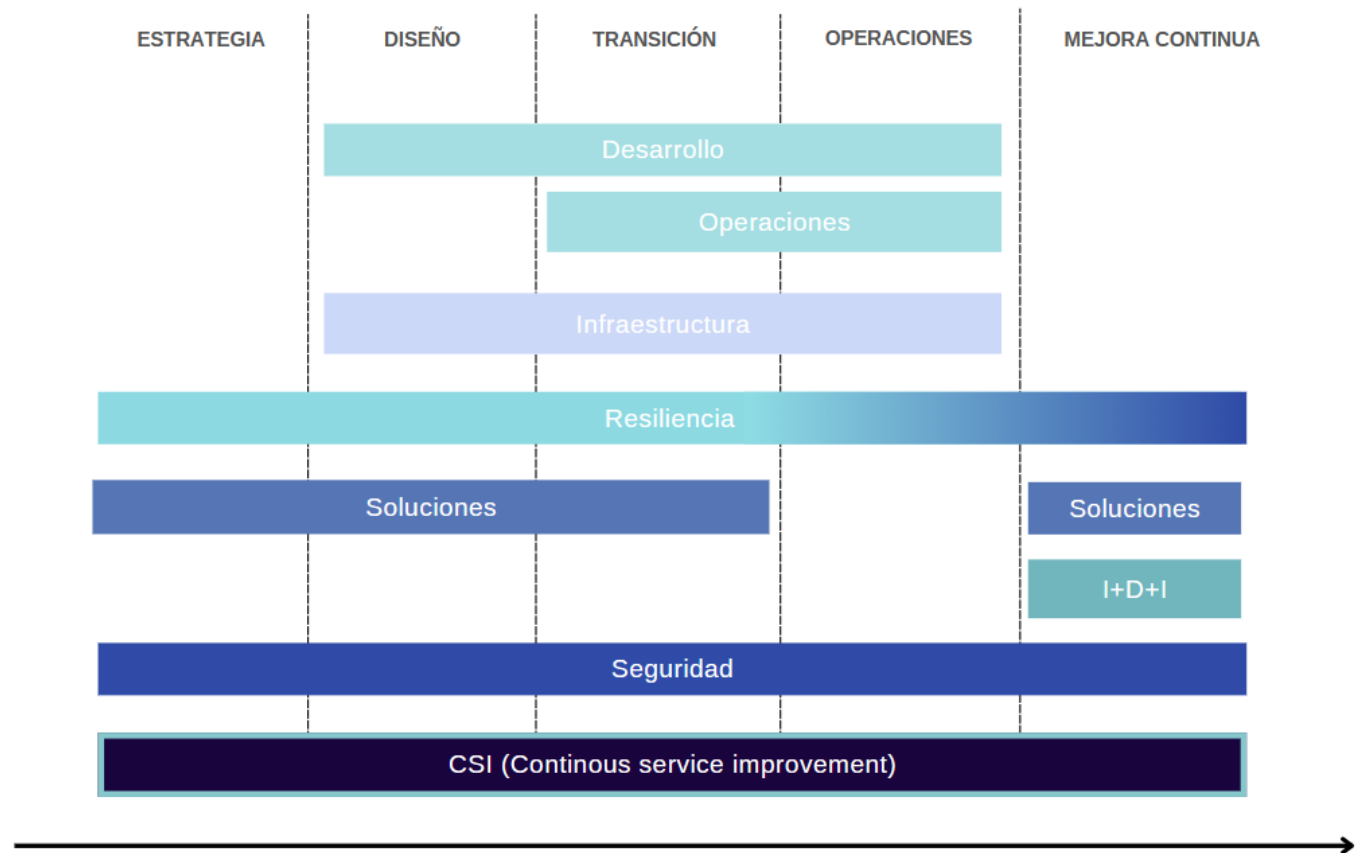


AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

- Departamento transversal
- Visión estratégica
- Colaboración

CICLO DE VIDA





AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. **Fase 1: Estrategia**
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

CICLO DE VIDA

Fase de Estrategia

- Gestión de la Demanda (DM)
- Gestión de la Cartera de Servicios (SPM)

Equipo de soluciones de seguridad

Equipo de soluciones:

- Priorizar y establecer el alcance:
 - Crear una idea clara del **alcance del proyecto** e identificar las **prioridades**.
 - Establecer los **objetivos empresariales** o de misión de alto nivel, las necesidades de la empresa y determinar la tolerancia al riesgo de la organización.
- Orientar: Hacer **inventario de los activos y sistemas** de la organización e identificar normativas aplicables, un **enfoque de riesgo** y las **amenazas** a las que la organización podría estar expuesta

**IBM
MAXIMO**

Inventario Centralizado

Gestión de configuración

Seguimiento
Incidentes/Problemas

Monitorización

Basado en el NIST

CICLO DE VIDA

Fase de Estrategia



1. Inventario de Activos:

- Activos físicos (como servidores, computadoras, dispositivos de red)
- Activos digitales (como software, licencias, bases de datos).
- IBM Maximo --> registrar y rastrear estos activos. Puedes clasificarlos según su tipo, importancia, sensibilidad, complejidad, ubicación, fecha de adquisición...

2. Seguridad de Activos Digitales:

- Los activos digitales son críticos en una empresa de ciberseguridad. Protección de sistemas, aplicaciones y datos.
- IBM Maximo --> gestionar licencias de software, controlar el acceso a sistemas y aplicaciones, y realizar auditorías de seguridad.

CICLO DE VIDA

Fase de Estrategia



3. Gestión de Vulnerabilidades:

- Identifica y evalúa las vulnerabilidades en tus activos digitales. Esto incluye escanear sistemas en busca de vulnerabilidades conocidas.
- IBM Maximo --> priorizar y remediar estas vulnerabilidades. Puedes asignar tareas de parcheo o actualización a los equipos responsables.

4. Gestión de Contratos y Garantías:

- Administra los contratos de mantenimiento y garantías de tus activos físicos y digitales.
- Departamento de Soluciones

5. Seguimiento de Incidentes y Problemas:

- Registra cualquier incidente o problema relacionado con los activos (fallos en el hardware, problemas de software o brechas de seguridad)
- IBM Maximo--> te ayuda a documentar y resolver estos problemas de manera eficiente.

CICLO DE VIDA

Fase de Estrategia



6. Gestión de Proyectos y Cambios:

- Si realizas cambios en los activos (como actualizaciones de software, reemplazo de hardware o cambios en la infraestructura), IBM Maximo --> planificar y ejecutar estos proyectos.
- Realiza un seguimiento de los cambios y asegúrate de que se realicen de manera controlada y documentada.

7. Documentación y Auditoría:

- Mantén registros detallados de tus activos. Esto es esencial para la auditoría, la toma de decisiones y la planificación a largo plazo.
- IBM Maximo --> te permite generar informes personalizados para evaluar el rendimiento y la eficiencia de tus activos.
- Departamento Q&A

EJEMPLO CON EL CLIENTE

Bufete de Abogados

CICLO DE VIDA

Fase de Estrategia

Ejemplo con el cliente:



LegalGuard

Bufete de Abogados

Antecedentes:

LegalGuard es un bufete de abogados con una amplia base de clientes y una reputación sólida en el campo legal. Recientemente, han experimentado un **aumento en los ataques cibernéticos** dirigidos a firmas legales, lo que ha aumentado su preocupación por la seguridad de la información confidencial de sus clientes y la integridad de sus sistemas.

Desafíos:

LegalGuard reconoce que necesita mejorar su postura de seguridad cibernética, pero **carece de los recursos internos** y la experiencia especializada para hacerlo eficazmente. Además, quieren asegurarse de cumplir con las regulaciones legales relacionadas con la protección de datos.

CICLO DE VIDA

Fase de Estrategia

Ejemplo con el cliente:



Bufete de Abogados

Comprender la organización y su contexto

- Comunicación y Consultas
- El contexto del SGSI
- El Contexto de la Gestión de Riesgos
- Definición de criterios del riesgo

Comprender las necesidades y expectativas de las partes interesadas

Determinación del Alcance del Sistema de Gestión

- Propósito del Alcance del SGSI
- Como definir los limites el SGSI
- Cuestionario para definir el Alcance del SGSI
- Ejemplo de Alcance del SGSI

CICLO DE VIDA

Fase de Estrategia

Ejemplo con el cliente:



Bufete de Abogados

Buscan un outsourcing de su ciberseguridad

No tienen recursos internos

Importante adecuarse a las leyes vigentes españolas y europeas

La confidencialidad y la integridad cobra más importancia que la disponibilidad

Es importante la capacitación a los empleados, en concreto ante ataques de phishing

Seguridad de la comunicación es crucial

Gestión de identidad y acceso es crucial



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño**
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

CICLO DE VIDA

Fase de Diseño

- Gestión de la seguridad de la Información (ISM)

Equipo de soluciones de seguridad

Equipo de soluciones de seguridad:

- **Creación del perfil actual:** cómo la organización está **gestionando el riesgo en la actualidad**, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).
- **Realizar una evaluación de riesgos:** evaluación el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la **probabilidad y gravedad** de un evento de ciberseguridad que pueda afectar a la organización.
- **Creación un perfil objetivo:** la **meta** de gestión de riesgos del equipo de seguridad de la información.
- **Creación de un plan de acción :** hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Basado en el NIST

CICLO DE VIDA

Fase de Diseño

Plan a Seguir

ISO 27000



CICLO DE VIDA

Fase de Diseño

- Gestión de la seguridad de la Información (ISM)

Equipo de soluciones de seguridad

Equipo de soluciones de seguridad:

- **Creación del perfil actual:** cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).
- **Realizar una evaluación de riesgos:** evaluación el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la probabilidad y gravedad de un evento de ciberseguridad que pueda afectar a la organización.
- **Creación un perfil objetivo:** la meta de gestión de riesgos del equipo de seguridad de la información.
- **Creación de un plan de acción :** hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Basado en el NIST

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

- **Creación del perfil actual:** cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).

ISO 27001:

Arquitectura del Sistema

Componentes del Sistema

Categorías del NIST:



CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:

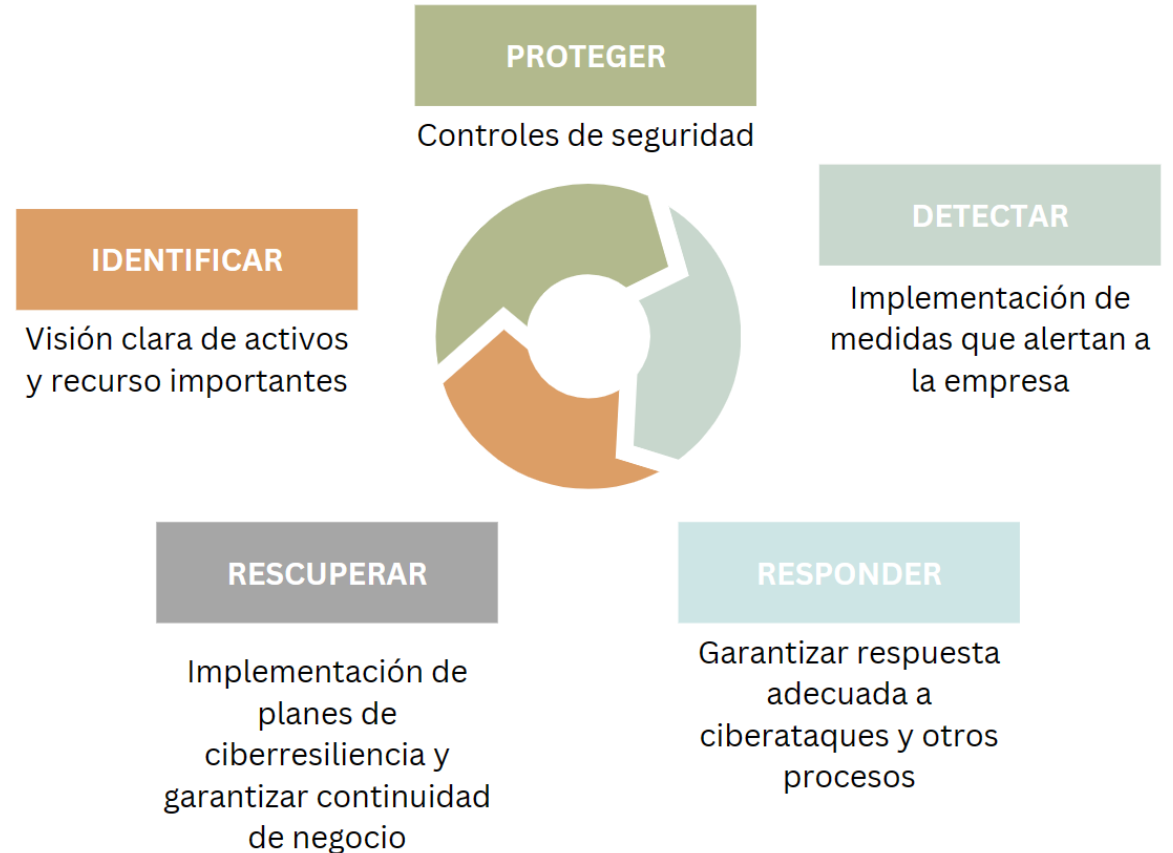


Bufete de Abogados

Creación del perfil actual:

Subcategorías Identificar:

- Asset Management (AM)
- Business Environment (BE)
- Governance (GV)
- Risk Assessment (RA)
- Risk Management Strategy (RS)
- Supply Chain Risk Management (SC)



CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Creación del perfil actual

Arquitectura del Sistema

•Asset Management (AM):

- LegalGuard tiene un **inventario básico (Excel)** de activos de TI, pero carece de un sistema formal de gestión de activos para rastrear y mantener registros actualizados de todos los dispositivos y recursos de la red.

•Business Environment (BE):

- LegalGuard opera en un entorno empresarial con un alto enfoque en la confidencialidad y la integridad de la información, pero **carece de una cultura de seguridad sólida** y de un **compromiso** claro por parte de la alta dirección.

•Governance (GV):

- No hay un marco formal de gobierno de seguridad de la información establecido en LegalGuard. **Las políticas y procedimientos de seguridad son mínimos** y no se aplican de manera consistente en toda la organización.

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Creación del perfil actual

Componentes del Sistema

Servidores:

- Los servidores de LegalGuard almacenan información altamente confidencial de los clientes, como detalles legales y financieros. Sin embargo, no se implementan medidas adecuadas de control de acceso. Por ejemplo, no hay una política clara de quién tiene acceso a qué datos y no se lleva un registro de los cambios en la configuración del servidor.

Ordenadores de Escritorio y Portátiles:

- Los empleados de LegalGuard utilizan computadoras de escritorio y portátiles para acceder a sistemas y datos confidenciales. Sin embargo, muchos dispositivos carecen de software de inventario instalado y **no se aplican políticas de seguridad de TI**, como la encriptación de datos o la autenticación multifactor, aumentando el riesgo de acceso no autorizado.

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Creación del perfil actual

Componentes del Sistema

Dispositivos Móviles:

Algunos abogados y personal administrativo utilizan sus dispositivos móviles personales para acceder a correos electrónicos y documentos de trabajo. Sin embargo, estos dispositivos no están gestionados por la empresa y carecen de medidas de seguridad, como el cifrado de datos o la aplicación de políticas de seguridad móvil, lo que aumenta el riesgo de pérdida o robo de datos confidenciales.

Software:

LegalGuard utiliza una variedad de software para la gestión de casos legales y la comunicación interna. Sin embargo, no se realizan actualizaciones de seguridad de manera regular. Por ejemplo, el software antivirus en algunas estaciones de trabajo puede estar desactualizado, dejando al sistema vulnerable a las últimas amenazas de malware.

CICLO DE VIDA

Fase de Diseño

- Gestión de la seguridad de la Información (ISM)

Equipo de soluciones de seguridad

Equipo de soluciones de seguridad:

- **Creación del perfil actual:** cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).
- **Realizar una evaluación de riesgos:** evaluación el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la probabilidad y gravedad de un evento de ciberseguridad que pueda afectar a la organización.
- **Creación un perfil objetivo:** la meta de gestión de riesgos del equipo de seguridad de la información.
- **Creación de un plan de acción :** hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Basado en el NIST

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Realice una evaluación de riesgos

ISO 27005

Identificación Amenazas & vulnerabilidades



Análisis de riesgos

Impacto

Probabilidad



Calificación de los riesgos

Equipo Gestión de Riesgos

Nessus

Wireshark

PhishMe

Malwarebytes

Microsoft Baseline Security Analyzer (MBSA)

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Realice una evaluación de riesgos

Equipo Gestión de
Riesgos

CALIFICACION DEL RIESGO	DESCRIPCIÓN
Muy alto (7-9)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir estos riesgos y mitigar los riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir el riesgo y los riesgos de mitigación deberían implementarse lo antes posible.
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir los riesgos y mitigar los peligros deberían incluirse en los planes y presupuestos futuros.
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir aún más el riesgo o mitigar los peligros junto con otras mejoras de seguridad y mitigación.

ISO 27005

CICLO DE VIDA

Fase de Diseño

- Gestión de la seguridad de la Información (ISM)

Equipo de soluciones de seguridad

Equipo de soluciones de seguridad:

- **Creación del perfil actual:** cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).
- **Realizar una evaluación de riesgos:** evaluación el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la probabilidad y gravedad de un evento de ciberseguridad que pueda afectar a la organización.
- **Creación un perfil objetivo:** la meta de gestión de riesgos del equipo de seguridad de la información.
- **Creación de un plan de acción :** hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Basado en el NIST

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

- **Creación un perfil objetivo:** la meta de gestión de riesgos del equipo de seguridad de la información

ISO 27001:

Arquitectura del Sistema

Componentes del Sistema

Políticas y Controles

Categorías del NIST:



CICLO DE VIDA

Fase de Diseño

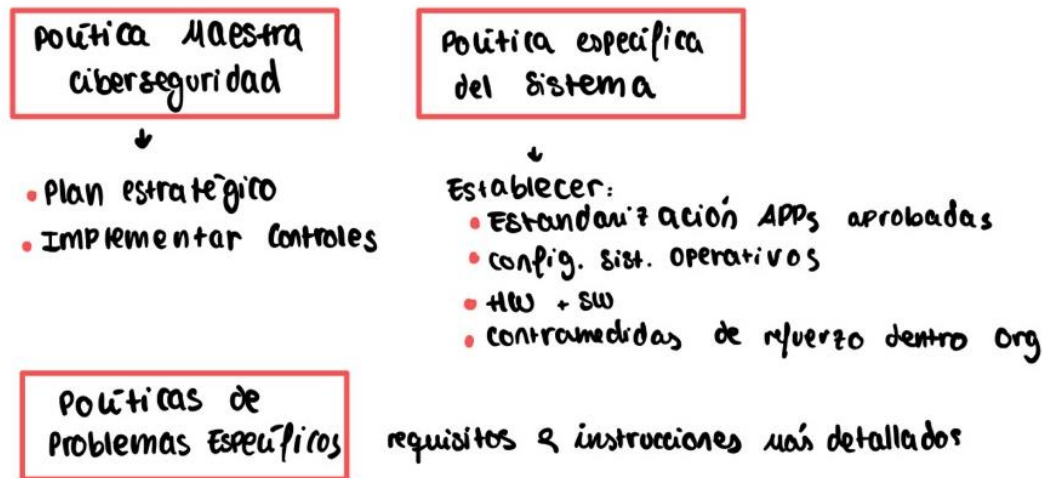
Ejemplo con el cliente:



Bufete de Abogados

Equipo de Gobernanza
de la información

- Creación un perfil objetivo



CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Equipo de Gobernanza
de la información

- Creación un perfil objetivo

Política Maestra
ciberseguridad



- Plan estratégico
- Implementar controles

Política específica
del sistema



Establecer:

- Estandarización APPs aprobadas
- Config. sist. operativos
- HW + SW
- Contramedidas de refuerzo dentro org

Políticas de
Problemas Específicos

requisitos & instrucciones más detallados

Tipos de Políticas de Seguridad

- ⊕ P. de identificación y autenticación
- ⊕ P. de contraseñas
- ⊕ P. de uso Aceptable → acceso y uso recursos red + consecuencias infracción
- ⊕ P. de acceso remoto
- ⊕ P. de mantenimiento de la red
- ⊕ P. de manejo de incidentes
- ⊕ P. de datos
- ⊕ P. de credenciales
- ⊕ P. organizacionales → admin cambios, activos, control cambios, ...

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

Equipo de Gobernanza
de la información

Controles críticos de Seguridad CIS → Centro Seguridad Internet

+ Controles Básicos

- Inventario y control de activos de hardware
- Inventario y control de activos de software
- Administración continua de vulnerabilidades
- Uso controlado de privilegios administrativos
- Configuraciones seguras para hardware y software
- Mantenimiento, monitoreo y análisis de registros de auditoría

+ Controles Fundamentales

- Protección para correo electrónico y navegadores web
- Defensa contra malware
- Limitación y control de puertos de red, protocolos y servicios
- Capacidades de recuperación de datos
- Configuraciones seguras para dispositivos de red
- Defensa del límite
- Protección de datos
- Acceso controlado basado en el principio de 'necesidad de saber'
- Control de acceso inalámbrico
- Monitoreo y control de cuentas

+ Controles Organizacionales

- Un programa de concientización y capacitación en seguridad.
- Seguridad del software de aplicación
- Administración y respuesta ante incidentes
- Pruebas de penetración y ejercicios de equipo rojo (ejercicios de ataque simulados para medir las capacidades de seguridad de una organización)

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.

- 5.1.1 Conjunto de políticas para la seguridad de la información.
- 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.

- 6.1.1 Asignación de responsabilidades para la segur. de la información.
- 6.1.2 Segregación de tareas.
- 6.1.3 Contacto con las autoridades.
- 6.1.4 Contacto con grupos de interés especial.
- 6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.

- 6.2.1 Política de uso de dispositivos para movilidad.
- 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.

- 7.1.1 Investigación de antecedentes.
- 7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.

- 7.2.1 Responsabilidades de gestión.
- 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
- 7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.

- 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.

- 8.1.1 Inventario de activos.
- 8.1.2 Propiedad de los activos.
- 8.1.3 Uso aceptable de los activos.
- 8.1.4 Devolución de activos.

8.2 Clasificación de la información.

- 8.2.1 Directrices de clasificación.
- 8.2.2 Etiquetado y manipulado de la información.
- 8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.

- 8.3.1 Gestión de soportes extraíbles.
- 8.3.2 Eliminación de soportes.
- 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.

- 9.1.1 Política de control de accesos.
- 9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.

- 9.2.1 Gestión de altas/bajas en el registro de usuarios.
- 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
- 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
- 9.2.4 Gestión de información confidencial de autenticación de usuarios.
- 9.2.5 Revisión de los derechos de acceso de los usuarios.
- 9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.

- 9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

- 9.4.1 Restricción del acceso a la información.
- 9.4.2 Procedimientos seguros de inicio de sesión.
- 9.4.3 Gestión de contraseñas de usuario.
- 9.4.4 Uso de herramientas de administración de sistemas.
- 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.

- 10.1.1 Política de uso de los controles criptográficos.
- 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.

- 11.1.1 Perímetro de seguridad física.
- 11.1.2 Controles físicos de entrada.
- 11.1.3 Seguridad de oficinas, despachos y recursos.
- 11.1.4 Protección contra las amenazas externas y ambientales.
- 11.1.5 El trabajo en áreas seguras.
- 11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.

- 11.2.1 Emplazamiento y protección de equipos.
- 11.2.2 Instalaciones de suministro.
- 11.2.3 Seguridad del cableado.
- 11.2.4 Mantenimiento de los equipos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa.
- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
- 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
- 11.2.8 Equipo informático de usuario desatendido.
- 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.

12.1 Responsabilidades y procedimientos de operación.

- 12.1.1 Documentación de procedimientos de operación.
- 12.1.2 Gestión de cambios.
- 12.1.3 Gestión de capacidades.
- 12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.

- 12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.

- 12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.

- 12.4.1 Registro y gestión de eventos de actividad.
- 12.4.2 Protección de los registros de información.
- 12.4.3 Registros de actividad del administrador y operador del sistema.
- 12.4.4 Sincronización de relojes.

12.5 Control del software en explotación.

- 12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.

- 12.6.1 Gestión de las vulnerabilidades técnicas.
- 12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.

- 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.

- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.

- 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.

- 15.1.1 Política de seguridad de la información para suministradores.
- 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.

- 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

- 16.1.1 Responsabilidades y procedimientos.
- 16.1.2 Notificación de los eventos de seguridad de la información.
- 16.1.3 Notificación de puntos débiles de la seguridad.
- 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
- 16.1.5 Respuesta a los incidentes de seguridad.
- 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
- 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.

- 17.1.1 Planificación de la continuidad de la seguridad de la información.
- 17.1.2 Implantación de la continuidad de la seguridad de la información.
- 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.

- 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.

- 18.1.1 Identificación de la legislación aplicable.
- 18.1.2 Derechos de propiedad intelectual (DPI).
- 18.1.3 Protección de los registros de la organización.
- 18.1.4 Protección de datos y privacidad de la información personal.
- 18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.

- 18.2.1 Revisión independiente de la seguridad de la información.
- 18.2.2 Cumplimiento de las políticas y normas de seguridad.
- 18.2.3 Comprobación del cumplimiento.

CICLO DE VIDA

Fase de Diseño

- Gestión de la seguridad de la Información (ISM)

Equipo de soluciones de seguridad

Equipo de soluciones de seguridad:

- **Creación del perfil actual:** cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF (CyberSecurity Framework, NIST).
- **Realizar una evaluación de riesgos:** evaluación el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la probabilidad y gravedad de un evento de ciberseguridad que pueda afectar a la organización.
- **Creación un perfil objetivo:** la meta de gestión de riesgos del equipo de seguridad de la información.
- **Creación de un plan de acción :** hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Basado en el NIST

CICLO DE VIDA

Fase de Diseño

Ejemplo con el cliente:



Bufete de Abogados

- **Creación de un plan de acción** : hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas

Hito	Descripción	Tiempo	Personal	Presupuesto
Despliegue de Infraestructura Segura	<ul style="list-style-type: none">• Evaluación de proveedores de servicios en la nube que cumplan con los requisitos de seguridad del NIST.• Implementación de controles de acceso basados en la autenticación multifactor (MFA) para todos los sistemas en la nube.• Configuración de registros de auditoría para monitorear y registrar actividades de usuario en la infraestructura de nube.	6 meses	<ul style="list-style-type: none">• Departamento Infraestructura• Departamento Resiliencia	100.000€



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. **Fase 3: Transición**
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

CICLO DE VIDA

Fase de Transición

Equipo Gestión de Riesgos

- **Recopilación de datos y evaluación de riesgos:** Se utiliza la metodología NIST SP800-30, compuesta por 9 fases.
- **Evaluación de vulnerabilidades:** Se identifican, evalúan y priorizan las debilidades y fallas en los sistemas, aplicaciones, y redes de la organización que podrían ser aprovechadas por un eventual ciberataque (estándares CVE, CVSS).
- **Ejecución de pruebas controladas:** Para la explotación de vulnerabilidades (metodología ISSAF).

CICLO DE VIDA

Fase de Transición

1. Recopilación de datos y evaluación de riesgos

Caracterización del sistema: Implica **identificar y documentar los activos de información** críticos, así como los sistemas, redes y procesos asociados. También implica **comprender el contexto operativo de la organización**, incluyendo su **estructura organizativa**.

Permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa, lo que ayuda a **enfocar los esfuerzos de evaluación en áreas específicas que son más relevantes para la seguridad** de la información de la organización. Esto asegura que la **evaluación de riesgos sea efectiva** y se alinee adecuadamente con los objetivos y necesidades del negocio.

CICLO DE VIDA

Fase de Transición

1. Recopilación de datos y evaluación de riesgos

Identificación de amenazas: Se definen las **diferentes fuentes de motivación** de las mismas, basándose en lo ocurrido en el pasado.

Identificación de vulnerabilidades: para su identificación se desarrolla una lista de defectos o debilidades para conocer las posibles intrusiones de una amenaza.

Análisis de controles: Analizar controles actuales y controles planificados.

Determinación de probabilidades: Conocer a través del estudio cuales son las **motivaciones para los ataques, capacidad de las amenazas, y la naturaleza de las vulnerabilidades.**

CICLO DE VIDA

Fase de Transición

1. Recopilación de datos y evaluación de riesgos

Análisis del impacto: Hay que evaluar el **riesgo real** en el sistema de información.

Determinación del riesgo: Debemos conocer **qué probabilidad de explotación de las amenazas**, magnitud de los impactos, adecuación de los controles actuales y planificados nos podemos encontrar. Con dicho análisis estableceremos **qué nivel de riesgo tiene la organización** pudiendo ser: bajo, medio o alto.

Recomendación de controles: Para tener nuestro sistema seguro debemos realizar **revisiones de las políticas de seguridad, actualizaciones periódicas del antivirus**, un cambio de contraseñas periódicas, instalación de firewalls o en caso de incumplimiento de la normativa vigente, sanciones.

Documentación de resultados: Según los riesgos de la organización proceder a la elaboración de un **informe detallado de valoración de los riesgos**.

CICLO DE VIDA

Fase de Transición

Ejemplo con el cliente:



Bufete de Abogados

- Se revisa el historial de ataques de LegalGuard. Aquí se busca **introducción de virus en los sistemas, corrupción de datos o incumplimientos legales intencionados**, para identificar los puntos débiles.
- Se **estudian informes de evaluaciones de riesgos anteriores**, como resultados de **auditorías y pruebas de seguridad**, para obtener una lista de potenciales vulnerabilidades.
- Se analiza el **resultado de los informes históricos** para obtener posibles **motivaciones para los ataques**, la capacidad de las amenazas, y la naturaleza de las vulnerabilidades, y así se genera un **rating de probabilidades**.

CICLO DE VIDA

Fase de Transición

Ejemplo con el cliente:



Bufete de Abogados

- Analizar **controles actuales y controles planificados**, por ejemplo: el control del número de personas que tiene acceso al equipo informático diariamente, registro de información confidencial para la que se requiere uso de contraseñas, etc.
- Se realiza una **valoración de la criticidad de activos**, y la **criticidad y sensibilidad de datos**, para generar un **rating de impactos**.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Vulnerabilidad vs. Amenaza

- Según el ISO 27001 hay una diferencia entre vulnerabilidad y amenaza.
- Las **vulnerabilidades son defectos o debilidades en un activo.**
- Las **amenazas pueden desencadenar o explotar una vulnerabilidad para comprometer algún aspecto del activo.**
- Amenazas más comunes mencionadas en el ISO 27001:
 - Acceso a la red o al sistema de información por personas no autorizadas.
 - Comprometer información confidencial.
 - Desastre natural, incendio, inundación, rayo.
 - Divulgación de contraseñas.
 - Errores de software.
 - Etc.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Vulnerabilidad vs. Amenaza

- Vulnerabilidades más comunes mencionadas en el ISO 27001:
 - Sensibilidad del equipo a la humedad, temperatura o contaminantes.
 - Inadecuada gestión de red.
 - Falta de documentación interna.
 - Mala selección de datos de prueba.
 - Empleados desmotivados.
 - Etc.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: ¿Por qué?

- Saber identificar las amenazas y vulnerabilidades es de obligado conocimiento para los profesionales en seguridad de la información de acuerdo a lo establecido en el ISO 27001.
- Fundamental para garantizar la **seguridad de los datos** y la **protección contra amenazas**
- Permite **identificar y corregir los riesgos potenciales** antes de que se conviertan en problemas reales.
- Se reducen las posibilidades de sufrir brechas de seguridad y se **minimiza el impacto de los ataques**.
- Las organizaciones que no realizan un análisis de vulnerabilidades están **expuestas a un mayor riesgo de sufrir ciberataques y comprometer la confidencialidad**, integridad y disponibilidad de la información.
- Proporciona una **visión clara de las debilidades presentes en los sistemas**.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: ¿Por qué?

- Al realizar un análisis exhaustivo, se puede **anticipar y mitigar riesgos potenciales** de ataques cibernéticos
- Protegiendo así sus activos digitales, la información confidencial de sus clientes y su reputación en línea.
- Un análisis de vulnerabilidades **ayuda a cumplir con las regulaciones de seguridad y privacidad de datos**, fortaleciendo la **confianza de los clientes** y socios comerciales de la empresa.
- Invertir en análisis de vulnerabilidades es una medida proactiva que puede **salvar** a una empresa **de costosos ataques cibernéticos** y **garantizar su continuidad operativa**.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades:

- Utilizaremos CVE (Common Vulnerabilities and Exposures), es una lista pública de datos sobre las vulnerabilidades comunes que se han reportado de todos los softwares.
- Utilizaremos CVSS (Common Vulnerability Scoring System), es un sistema de puntuación que permite definir numéricamente el nivel de gravedad de un fallo de seguridad.
- Utilizaremos la base de datos del NIST, llamada NVD, donde se pueden buscar vulnerabilidades por nombre de CVE, y se obtiene más información sobre la vulnerabilidad, junto con el grado de severidad CVSS.
- El NVD es el repositorio del gobierno de EE. UU. de datos de gestión de vulnerabilidades basados en estándares representados mediante el Protocolo de automatización de contenido de seguridad (SCAP).

CICLO DE VIDA

Fase de Transición

Ejemplo con el cliente:



Bufete de Abogados

- Una adecuada gestión de los riesgos de acuerdo al ISO 27001 pasa por la implantación de **controles de seguridad, capacitación del personal, plan de contingencia, auditorías de seguridad, actualización periódica de sistemas y aplicaciones y la realización de pruebas de penetración y simulaciones de ataques.**
- Se realizan escáneres de vulnerabilidades automatizados, utilizaremos Nessus, esta herramienta escanea los sistemas y redes de LegalGuard, en busca de posibles vulnerabilidades conocidas, como **puertos abiertos, servicios desactualizados, configuraciones inseguras y otros puntos de debilidad.**
- Evaluaremos la **resistencia de la empresa a los ataques**, utilizando la herramienta **Wireshark**, que simula ataques reales contra los sistemas y redes de LegalGuard.

CICLO DE VIDA

Fase de Transición

Ejemplo con el cliente:



Bufete de Abogados

- Firewalls, y sistemas de detección y prevención de intrusiones (IDS/IPS): Ayudaremos a **proteger los sistemas y redes de la empresa contra ataques externos**, y a **detectar posibles intrusiones en tiempo real**, utilizando la herramienta **Palo Alto Networks**. Los **firewalls filtran el tráfico de red según reglas predefinidas**, mientras que los sistemas **IDS/IPS analizan el tráfico en busca de patrones sospechosos** o comportamiento malicioso.
- Utilizaremos **Nexpose** para **gestionar y priorizar las vulnerabilidades** identificadas, así como coordinar las acciones de remediación necesarias.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: NESSUS

- Cuenta con la confianza de más de **27.000 organizaciones en todo el mundo**, automatiza las evaluaciones a un momento dado para ayudar a **identificar y reparar con rapidez las vulnerabilidades, incluso fallas de software, parches faltantes, malware y configuraciones erróneas**, en diversos sistemas operativos, dispositivos y aplicaciones.
- Tiene el índice de **falsos positivos más bajo de la industria** con una precisión de six sigma (medido en 0,32 defectos por 1 millón de escaneos).
- Nessus tiene la cobertura más amplia y completa, con más de 100.000 complementos, **cobertura para más de 45.000 CVE** y el lanzamiento de más de 100 nuevos complementos cada semana dentro de las 24 horas de la revelación de vulnerabilidades.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: WIRESHARK

- Wireshark se basa en la captura de paquetes: **intercepta y analiza el tráfico de la red en tiempo real**. La herramienta es capaz de capturar paquetes de diferentes protocolos, como TCP, UDP, ICMP, HTTP, FTP, DNS y muchos otros. Además, puede leer y decodificar datos de los protocolos más utilizados, lo que facilita la interpretación del tráfico capturado.
- Además de analizar el tráfico en tiempo real, Wireshark **permite cargar archivos de captura previamente almacenados, útil para investigar incidentes pasados**.
- Es **aplicable en pruebas de penetración y análisis de vulnerabilidades** para evaluar la seguridad de una red o sistema. Al analizar el tráfico capturado, Wireshark puede identificar posibles vulnerabilidades, como contraseñas en texto claro o datos confidenciales transmitidos sin cifrar.
- Algunas empresas que utilizan Wireshark son Panasonic Corp y eBay Inc.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: ¿Que riesgos queremos evaluar?

- **Errores en la gestión de recursos:** Mal uso o la **asignación inadecuada de recursos** del sistema, como memoria, **espacio en disco** o ancho de banda, lo que podría llevar a **problemas de rendimiento** o a la exposición de datos sensibles.
- **Factor humano:** Errores, descuidos o acciones maliciosas cometidas por empleados u otras personas dentro de la organización. Esto puede incluir la **divulgación accidental de información confidencial**, el uso de **contraseñas débiles** o la **falta de capacitación en seguridad**.
- **Error de configuración:** Configuraciones incorrectas o inseguras en sistemas, aplicaciones o dispositivos de red. Por ejemplo, dejar **configuraciones predeterminadas sin cambiar**, no aplicar parches de seguridad o no configurar adecuadamente cortafuegos y políticas de acceso.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: ¿Que riesgos queremos evaluar?

- **Acceso al directorio:** Intentos de acceder a **información confidencial almacenada en directorios de archivos o bases de datos protegidas**. Esto puede incluir intentos de **robo de credenciales**, ataques de fuerza bruta o explotación de vulnerabilidades en el acceso a sistemas de archivos.
- **Validación de entrada:** **Manipulación de datos de entrada por parte de un atacante para ejecutar código malicioso** o realizar acciones no autorizadas en una aplicación o sistema. Esto puede incluir ataques de inyección SQL, XSS (Cross-Site Scripting) o manipulación de parámetros de URL.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: ¿Que riesgos queremos evaluar?

- **Permisos, privilegios y/o control de acceso:** Intentos de **usuarios no autorizados para obtener acceso a recursos o funcionalidades que no les corresponden**. Esto puede incluir el robo de credenciales, el uso de técnicas de ingeniería social o la explotación de vulnerabilidades en la gestión de permisos.
- **Fallos en la protección y gestión de permisos:** **Debilidades** en los mecanismos de protección y **gestión de permisos que permiten a un atacante eludir restricciones de seguridad** y obtener **acceso no autorizado a sistemas o datos sensibles**. Esto puede incluir la **falta de cifrado de datos**, la ausencia de autenticación multifactorial o la **mala gestión de roles y privilegios**.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Metodología

1. **Recopilación de información:** Recabar datos sobre la infraestructura de TI de la empresa: información sobre sistemas operativos, aplicaciones, dispositivos de red, configuraciones de seguridad, y políticas de acceso.
2. **Identificación de activos y riesgos:** Evaluación exhaustiva de los activos críticos de la empresa: servidores, bases de datos, aplicaciones web y datos sensibles, y **se identifican los riesgos potenciales asociados a cada uno de ellos**, como ataques de denegación de servicio, robo de datos o acceso no autorizado.
3. **Escaneo de vulnerabilidades:** Utilizando una **herramienta automatizada de escaneo de vulnerabilidades**, se examinan los sistemas y redes en busca de posibles puntos de debilidad, como puertos abiertos, servicios desactualizados o configuraciones inseguras que podrían ser explotadas por atacantes.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Metodología

- 4. **Análisis manual:** Los expertos en seguridad realizan una **revisión manual de los resultados del escaneo automático** para validar la existencia de vulnerabilidades y buscar posibles fallos que no puedan ser detectados de manera automatizada.
- 5. **Priorización de riesgos:** Se evalúa la **gravedad y el impacto potencial de cada vulnerabilidad identificada**, considerando factores como la probabilidad de explotación, el acceso a recursos críticos y el impacto en la continuidad del negocio, para priorizar las acciones de remediación.
- 6. **Remediación:** Se desarrollan e implementan **medidas para corregir o mitigar las vulnerabilidades identificadas**. Esto incluye la aplicación de **parches de seguridad**, la **reconfiguración de sistemas**, la **actualización de software**, o la implementación de controles de acceso adicionales.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Metodología

- 7. **Verificación y validación:** Se realiza una **verificación final para asegurarse de que las vulnerabilidades han sido adecuadamente corregidas y que no se han introducido nuevas vulnerabilidades durante el proceso de remediación.** Esto puede implicar **pruebas adicionales de penetración** o evaluaciones de seguridad para confirmar la efectividad de las medidas de mitigación.
- 8. **Documentación y reporte:** Se **documentan todos los hallazgos del análisis de vulnerabilidades**, junto con las acciones tomadas para remediarlos. Este informe suele incluir recomendaciones para mejorar la postura de seguridad de la empresa y prevenir futuros ataques.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Beneficios

- **Identificación temprana:** Este análisis puede detectar y alertar sobre las vulnerabilidades en la seguridad de la red o del software de una organización.
- **Ahorro de tiempo:** Las herramientas de evaluación de vulnerabilidades escanean una gran cantidad de sistemas y aplicaciones en un corto período de tiempo.
- **Precisión:** Las herramientas de evaluación de vulnerabilidades pueden proporcionar una evaluación más precisa y detallada de las vulnerabilidades de seguridad en comparación con las evaluaciones manuales.

CICLO DE VIDA

Fase de Transición

2. Evaluación de vulnerabilidades: Beneficios

- **Cumplimiento normativo:** Pueden ayudar a las organizaciones a **cumplir con los requisitos de cumplimiento normativo** y las regulaciones de seguridad, ya que pueden **demostrar que se han tomado medidas para identificar y abordar las vulnerabilidades** de seguridad.
- **Ahorro de costos:** Al detectar y solucionar las vulnerabilidades tempranamente, las organizaciones pueden ahorrar costos en términos de daños reputacionales, pérdida de datos o tiempos de inactividad

CICLO DE VIDA

Fase de Transición

3. Ejecución de pruebas controladas

- ISSAF (Information Systems Security Assessment Framework) es una metodología extensa y detallada para llevar a cabo pruebas de penetración. Desarrollada por el Open Information Systems Security Group (OISSG), ISSAF se basa en tres fases y consta de nueve pasos
- Implementa controles de IEC/ISO 27001:2005

Fase I: Planificación y Preparación

- En esta fase, se establece un **acuerdo de evaluación para proteger legalmente** a ambas partes.
- Se identifican las **personas de contacto** de ambas organizaciones.
- Se confirma el **alcance, el enfoque y la metodología**.
- Se aceptan **casos de prueba específicos y caminos de escalada de privilegios**.

CICLO DE VIDA

Fase de Transición

Fase II: Evaluación

- Recopilación de **información sobre la organización y su red.**
- **Mapeo de redes para obtener una topología probable:** es una **técnica para comprender la estructura y la conectividad de una red** mediante la recopilación de información sobre los dispositivos activos y sus relaciones.
- **Identificación de vulnerabilidades** mediante análisis y verificación.
- **Prueba de penetración** para intentar ganar acceso no autorizado.
- **Escalada de privilegios** para obtener acceso administrativo.

Fase III: Informe y seguimiento

- **Documentación** de hallazgos y recomendaciones.
- Presentación de **resultados al cliente.**
- Seguimiento para **verificar la implementación de soluciones.**

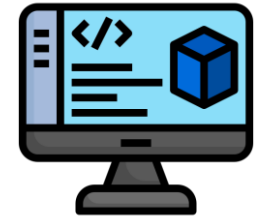


AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones**
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

CICLO DE VIDA

Fase de Operaciones



Implementar la solución del sistema

Directora de seguridad:

- **Dirigir la implementación del plan de acción** (definido en la fase de diseño)

Subdirectora de Seguridad:

- **Análisis de vulnerabilidades** (ISO/IEC 29147:2018): se identifican, clasifican y comunican las vulnerabilidades de manera confidencial, manteniendo la integridad del mensaje
- **Solución de estas vulnerabilidades** (ISO 27001)
- Configuración de dispositivos de **seguridad, monitoreo de red**, e implementación de medidas de seguridad en datos y sistemas

CICLO DE VIDA

Fase de Operaciones

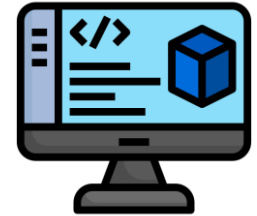
Implementar la solución del sistema

Directora de seguridad:

- **Dirigir la implementación del plan de acción** (definido en la fase de diseño)
 1. Comunicación clara
 2. Asignación de tareas
 3. Seguimiento del progreso
 4. Gestión de recursos
 5. Resolución de problemas
 6. Adaptación según sea necesario
 7. Celebración de logros

**Equipo de Gobernanza
de la información**

**Equipo de Concienciación y
Entrenamiento**



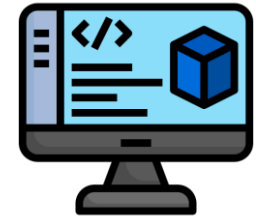
CICLO DE VIDA

Fase de Operaciones

Implementar la solución del sistema

Directora de seguridad:

- **Dirigir la implementación del plan de acción** (definido en la fase de diseño)



Ejemplo con el cliente:



Bufete de Abogados

Implementación de
controles de Acceso
Reforzado

Actualización y Parcheo
de Sistemas y Software

Mejorar la seguridad de
la Red

Capacitación y
Concientización del
Personal

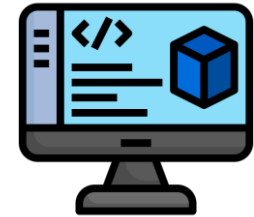
Establecimiento de un
equipo de respuesta a
incidentes

Establecimiento de un
equipo de gestión del
cambio

HITOS

CICLO DE VIDA

Fase de Operaciones



Implementar la solución del sistema

Directora de seguridad:

- **Dirigir la implementación del plan de acción** (definido en la fase de diseño)

Subdirectora de Seguridad:

- **Análisis de vulnerabilidades** (ISO/IEC 29147:2018): se identifican, clasifican y comunican las vulnerabilidades de manera confidencial, manteniendo la integridad del mensaje
- **Solución de estas vulnerabilidades** (ISO 27001)
- Configuración de dispositivos de **seguridad, monitoreo de red**, e implementación de medidas de seguridad en datos y sistemas

CICLO DE VIDA

Fase de Operaciones

Análisis de vulnerabilidades

Se define una política clara para **identificar, clasificar y comunicar las vulnerabilidades de manera confidencial**, manteniendo la integridad del mensaje.

Ser capaz de **recibir, responder y, en última instancia, corregir un informe de vulnerabilidad** es esencial para proporcionar productos y servicios. Recibir informes de vulnerabilidad ayuda a mitigar dos riesgos:

1. El riesgo de que las vulnerabilidades sean descubiertas por los adversarios y explotadas.
2. **Si no se proporciona una ruta de divulgación de vulnerabilidades, los buscadores que descubran vulnerabilidades podrían divulgarlas públicamente, lo que resultará en daño a la reputación.**

CICLO DE VIDA

Fase de Operaciones

Análisis de vulnerabilidades

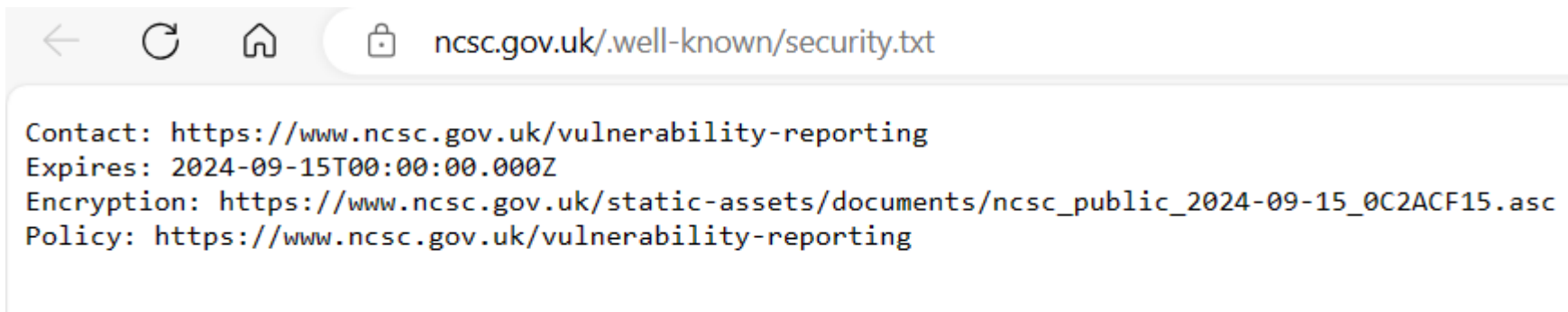
- Al proporcionar una **política clara de manejo de vulnerabilidades**, se define lo **que se espera al recibir un informe de una vulnerabilidad**, así como **qué se hará en respuesta**.
- La norma en que nos basamos, ISO/IEC 29147:2018, define los **requisitos mínimos para una política de divulgación de vulnerabilidades**:
 - Cómo desea la empresa con la que se está trabajando que se le contacte
 - Opciones de comunicación segura
 - Qué información incluir en el informe

CICLO DE VIDA

Fase de Operaciones

Análisis de vulnerabilidades

- Security.txt es un estándar de Internet propuesto, y describe un **archivo de texto que anuncia a la organización el proceso de divulgación de vulnerabilidades** para que cualquiera pueda encontrar rápidamente toda la información necesaria para informar una vulnerabilidad.
- El archivo contiene dos campos clave:
 - **CONTACTO:** Cómo los buscadores deben informar las vulnerabilidades. Por ejemplo, correo electrónico o formulario web seguro.
 - **POLÍTICA:** Un enlace a la política de divulgación de vulnerabilidades de la organización.



CICLO DE VIDA

Fase de Operaciones

Ejemplo con el cliente:



Bufete de Abogados

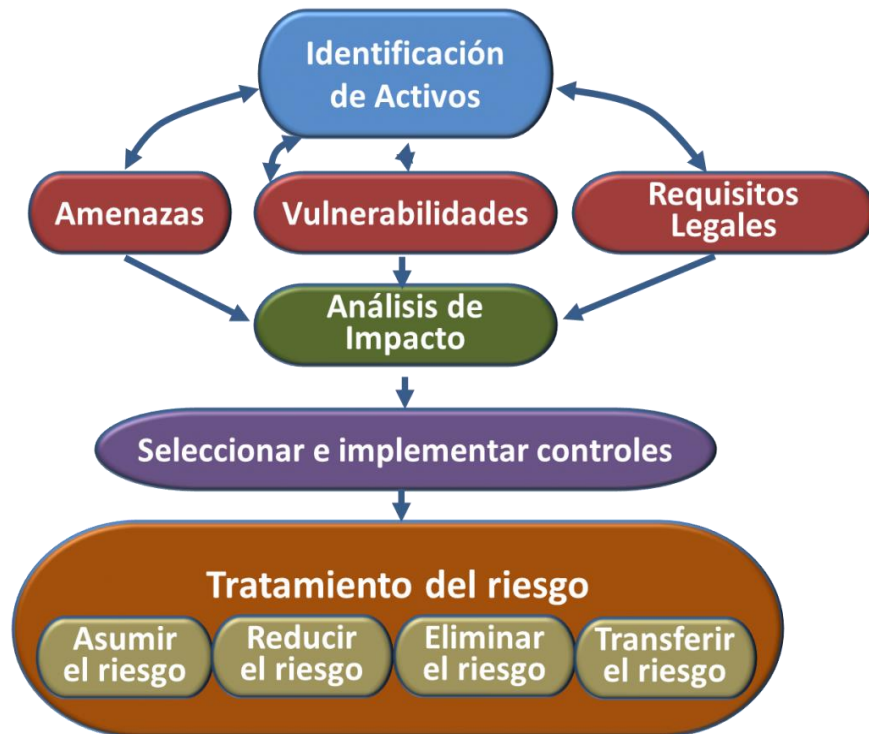
Análisis de vulnerabilidades: Se tendrá un **formulario web de contacto** para **garantizar que la información sobre vulnerabilidades llega al equipo adecuado**, y que sea fácil para LegalGuard informar sobre una vulnerabilidad.
En cuanto nos llega un reporte de vulnerabilidad:

1. **Pasaremos el informe a quien sea responsable** del servicio afectado.
2. Analizar **si se necesita más información** para solucionar el problema, y en caso de ser así, solicitarla.
3. Una vez que haya decidido el curso de acción, **se informa a la empresa que el problema se está gestionando**.
4. Una vez que se solucione el problema, se informa a la empresa.
5. **Se documenta todo lo ocurrido**, para que pueda ser analizado y buscar la raíz del problema, para que no vuelva a ocurrir a futuro.

CICLO DE VIDA

Fase de Operaciones

Utilizando la norma 27001, implementaremos la siguiente metodología de evaluación de riesgos:



1. **Identificación de Activos:** todo lo que tenga valor para la gestión de la seguridad de la organización:

- **Hardware:** Ordenadores de escritorio, ordenadores portátiles, impresoras, tabletas, servidores, teléfonos móviles, dispositivos extraíbles USB, discos externos, etc.
- **Software:** Hace referencia al **software contratado por la organización**, pero también a las aplicaciones preinstaladas en los equipos.

CICLO DE VIDA

Fase de Operaciones

1. Identificación de Activos:

- **Información:** Bases de datos, archivos en cualquier formato (texto, imagen, hoja de cálculo, información almacenada en medios digitales, pero también plasmada en otras formas no digitales)
- **Infraestructura:** Todo aquello que, en un momento dado, **pueda impedir el acceso a la información, deteriorarla o destruirla**. Las **instalaciones físicas**, el **servicio de electricidad**.
- **Recursos Humanos:** Las personas que tienen la **capacidad y los permisos necesarios para modificar la información**.
- **Servicios subcontratados:** Legales, de limpieza, proveedores de Internet, de cuentas de correo electrónico, de mantenimiento y actualización

CICLO DE VIDA

Fase de Operaciones

2. Identificación de Vulnerabilidades

3. **Identificación de amenazas:** Aquellas cosas que **puedan suceder y dañar el activo de la información**, tales como desastres naturales, incendios, ataques de virus, espionaje etc.

4. **Identificación de requisitos legales y contractuales** que la organización está obligada a cumplir con sus clientes, socios o proveedores.

5. **Identificar los riesgos:** Definir para cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo puedan causar un daño total o parcial al activo de la información, en relación a su disponibilidad, confidencialidad e integridad del mismo.

CICLO DE VIDA

Fase de Operaciones

6. Evaluación del riesgo: Haremos una evaluación de riesgos cualitativa.

Este tipo de evaluación, dentro del análisis de riesgos en ISO 27001, se puede llevar a cabo de dos formas diferentes: **Evaluación de riesgos simple**, o **Evaluación detallada de riesgos**.

- Usaremos ***Evaluación de riesgos simple***: evaluaremos las consecuencias y las probabilidades directamente. Una vez que identificamos los riesgos, utilizamos una escala para evaluar por separado las consecuencias y las probabilidades de cada uno de ellos.

CICLO DE VIDA

Fase de Operaciones

Criterios utilizados para el cálculo de la probabilidad:

- **Baja:** La probabilidad de que ocurra es como máximo cada año
- **Media:** La probabilidad de que ocurra es como máximo cada trimestre
- **Alta:** La probabilidad de que ocurra es como máximo cada mes

Criterios para el cálculo del impacto:

- **Bajo:** El impacto no tiene consecuencias relevantes para la Organización
- **Medio:** El impacto tiene consecuencias reseñables para la Organización
- **Alto:** El impacto tiene consecuencias graves para la Organización

		IMPACTO ⁽²⁾		
		Bajo	Medio	Alto
PROBABILIDAD ⁽¹⁾	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Riesgo = impacto x probabilidad de la amenaza. Con este procedimiento determinamos los riesgos que deben ser controlados con prioridad.

CICLO DE VIDA

Fase de Operaciones

7. Tratamiento del riesgo:

- Eliminarlo: Evitar el riesgo eliminándolo por completo.
- Reducirlo: Modificar el riesgo, poniendo en marcha controles de seguridad.
- Transferirlo: Compartir el riesgo o trasladarlo a un tercero.
- Asumirlo: Retener el riesgo, solo si se trata de un nivel aceptable.



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) **Ciclo de vida**
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua**
- 7) Casos de estudio
- 8) Conclusiones
- 9) Preguntas teóricas

CICLO DE VIDA

Fase de Mejora Continua

- **Recopilación** de datos y **evaluación** de riesgos (ISO/IEC 27001)
- Evaluar **nuevas** vulnerabilidades utilizando estándares CVE y CVSS

1. **Recopilación de datos y evaluación de riesgos: ¿Por qué es importante durante esta fase?**

1. Identifica **dónde es necesario implantar controles y sistemas de seguimiento.**
2. **Previene los incidentes** y mejora su gestión en caso de producirse.
3. Se **supervisa continuamente el proceso o la mitigación del riesgo**, y que se estén tomando las medidas adecuadas.

CICLO DE VIDA

Fase de Mejora Continua

Ejemplo con el cliente:



Bufete de Abogados

Recopilación de datos:

- **Utilizaremos Jira para gestionar tickets**, y dar soporte para la gestión de solicitudes de servicio, incidentes, problemas y cambios. Se centra en el soporte de alta velocidad, y ofrece una aplicación móvil para mayor flexibilidad.
- **Si la empresa enfrenta problemas en la calidad del servicio por ejemplo, se podrían recopilar datos como la cantidad de solicitudes de soporte, el número de tickets abiertos**, el tiempo promedio de respuesta, etc. para tener una idea de qué está causando una mala experiencia del cliente. Es a través de esta información que **reconoceremos necesidades, problemas y oportunidades de cambio**.

CICLO DE VIDA

Fase de Mejora Continua

2. Evaluar nuevas vulnerabilidades:

¿Cuáles son las más comunes? Nos basamos en ellas para hacer el análisis durante esta fase.

- **Vulnerabilidades de software:** Estas son **debilidades en el diseño, implementación o configuración del software** utilizado en su empresa. Pueden incluir errores de codificación, fallos de seguridad o falta de actualizaciones.
- **Vulnerabilidades de red:** Se refieren a los **puntos débiles en la infraestructura de red** de su empresa, como **firewalls mal configurados, puertos abiertos no seguros o falta de cifrado** en las comunicaciones.
- **Vulnerabilidades de aplicaciones web:** Estas son fallas específicas en las aplicaciones web, como inyecciones SQL, cross-site scripting (XSS) o autenticación deficiente.

CICLO DE VIDA

Fase de Mejora Continua

- **Vulnerabilidades de sistemas operativos:** Son debilidades en los sistemas operativos utilizados en sus dispositivos, servidores o estaciones de trabajo. Esto puede incluir **falta de parches de seguridad, configuraciones por defecto inseguras o permisos incorrectos.**
- **Vulnerabilidades de hardware:** Estas son **debilidades físicas en los dispositivos**, como puertos USB no seguros o dispositivos mal configurados.
- **Vulnerabilidades de Ingeniería Social:** Se refieren a **técnicas utilizadas por los atacantes para manipular a las personas y obtener acceso no autorizado a sistemas o información confidencial.**



AGENDA

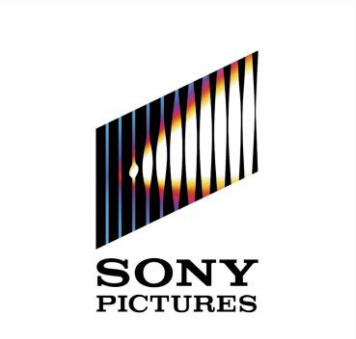

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) **Casos de estudio**
- 8) Conclusiones
- 9) Preguntas teóricas

CASOS DE ESTUDIO



Empresa	Caso de éxito
	Alcanzar niveles de seguridad óptimos para proteger sus activos, personas y recursos.
	Ha ayudado a la empresa a mantener una reputación sólida en cuanto a la seguridad de sus productos y servicios, y ha incrementado la confianza de sus clientes .
	Proporciona una variedad de servicios para destruir documentos no deseados de manera segura. La evolución de las tecnologías de la información ha obligado a la empresa a certificarse

CASOS DE ESTUDIO

Empresa	Consecuencia por no implementar normas de seguridad, como ISO 27001
	<p>En 2014, sufrió un ataque cibernético masivo que resultó en la filtración de información confidencial, incluyendo correos electrónicos, documentos internos y detalles de empleados. Este incidente provocó daños significativos a la reputación de la empresa y a sus operaciones comerciales.</p>
	<p>En 2018, sufrió una violación de seguridad que afectó a alrededor de 500,000 clientes. Los atacantes pudieron obtener datos sensibles, como números de tarjetas de crédito, nombres y direcciones. La falta de medidas adecuadas de seguridad de la información llevó a la aerolínea a enfrentar críticas y sanciones regulatorias.</p>



AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones**
- 9) Preguntas teóricas

CONCLUSIONES



**BREAKPOINT
TECHNOLOGIES**



Departamento de Seguridad

- ✓ Seguridad transversal de una empresa o una aplicación
- ✓ Fiabilidad → Certificación del ISO 270001 y basado en el NIST CSF
- ✓ Departamento presente en todo el ciclo de vida del cliente
- ✓ Estructura organizativa clara
- ✓ Enfoque en la gestión de riesgos
- ✓ Capacitación y concientización
- ✓ Enfoque de la seguridad de la información basado en un SGSI





AGENDA

- 1) ¿Quiénes somos?
 - Organigrama
 - Roles
 - Equipo
- 2) ¿Qué es la ciberseguridad?
- 3) ¿Qué hace el departamento de seguridad?
- 4) Estándares de Seguridad
- 5) Leyes cibernéticas europeas y españolas
- 6) Ciclo de vida
 - I. Fase 1: Estrategia
 - II. Fase 2: Diseño
 - III. Fase 3: Transición
 - IV. Fase 4: Operaciones
 - V. Fase 5: Mejora Continua
- 7) Casos de estudio
- 8) Conclusiones
- 9) **Preguntas teóricas**

¿QUÉ ES UN SISTEMA
DE GESTIÓN DE LA
SEGURIDAD DE LA
INFORMACIÓN?

Marco de políticas y procedimientos diseñado para ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de la información que manejan

¿CUÁLES SON LAS 5
FASES DEL NIST
CYBER SECURITY
FRAMEWORK?

Identificar – Proteger – Detectar – Responder – Recuperar

DIME AL MENOS
UNA RAZÓN PARA
UTILIZAR EL ISO
27001

- Se centra en la gestión integral de la seguridad de la información
- Prestigio (mejora la imagen de la empresa)
- Cumplimiento y normativa

SEGÚN ISO 27001, ¿CUALES
SON LOS PASOS A SEGUIR
PARA LA EVALUACIÓN DE
RIESGOS?

1. Identificación de activos
2. Identificación de vulnerabilidades
3. Identificación de amenazas
4. Identificación de requisitos legales y contractuales
5. Identificar los riesgos
6. Evaluación del riesgo

PREGUNTAS TEÓRICAS

MUCHAS
GRACIAS

Por su atención

