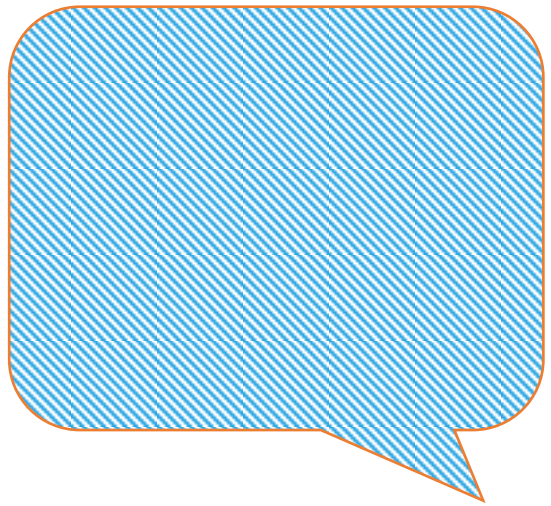
CONSTRUYENDO APLICACIONES CONFORMES AL ENS

DIEZ AÑOS FORTALECIENDO LA CIBERSEGURIDAD NACIONAL

CCN
Centro Criptológico Nacional

www.ccn-cert.cni.es



Carmen Serrano Durbá

GENERALITAT VALENCIANA

serrano_car@gva.es

Índice

La seguridad en el desarrollo de aplicaciones

Volumen de desarrollo de aplicaciones

- DGTIC: 900 aplicaciones, 6 servicios de desarrollo, 160 técnicos
- Contratación servicios externos desarrollo
- Adecuación al ENS de los sistemas existentes
- TRANSFORMACION DIGITAL (Ley 39/2015)

¿Cómo cumplimos el ENS en todo lo nuevo?

- Otras obligaciones de cumplimiento: LOPD, SGSI, ISO 27001,…

La seguridad en el desarrollo de aplicaciones

Aplicaciones cada vez **más expuestas**:

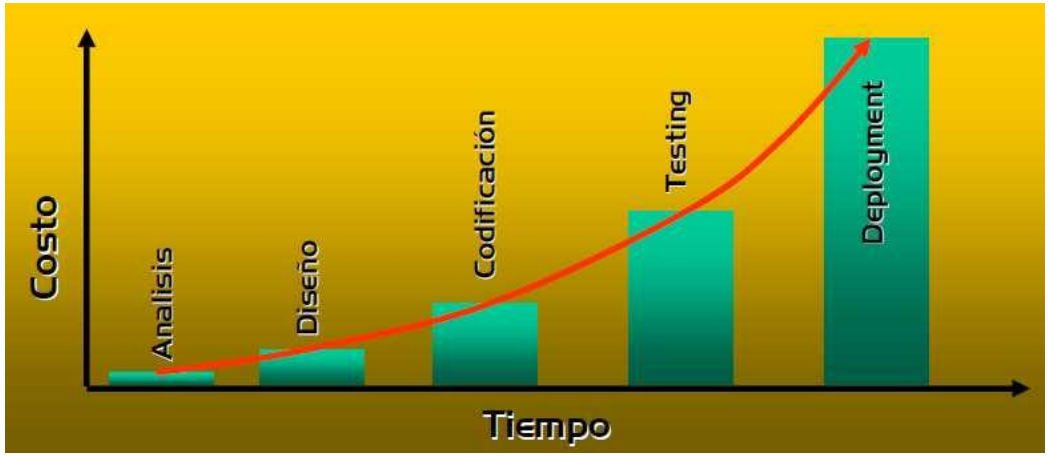
- Aplicaciones web o móviles, uso externo o compartido (democratizamos el acceso a al información). Cuidadanos, colaboradores, otras administraciones,…
- Aplicaciones dirigidas a los ciudadanos
- Aplicaciones desarrolladas para uso interno que se “abren”

Cada vez más preocupados por la seguridad

La seguridad en el desarrollo de aplicaciones

Problema:

- Los analistas y programadores priorizan la **funcionalidad y rapidez** de desarrollo
- La mayoría de los proyectos no incluyen seguridad, o bien la incluyen **al final**



- El **coste de solucionar la vulnerabilidades** es mayor cuanto más tarde se detecten las mismas
- La adecuación al cumplimiento de las normativas y marcos regulatorios al final del proyecto causa **retrasos en la implantación o incumplimiento**.

Necesidad de cambio

Cambio de Cultura:

RESPONSABLES FUNCIONALES:

- Necesidad de seguridad
- Conocedores de los Riesgos
- Conscientes obligaciones legales

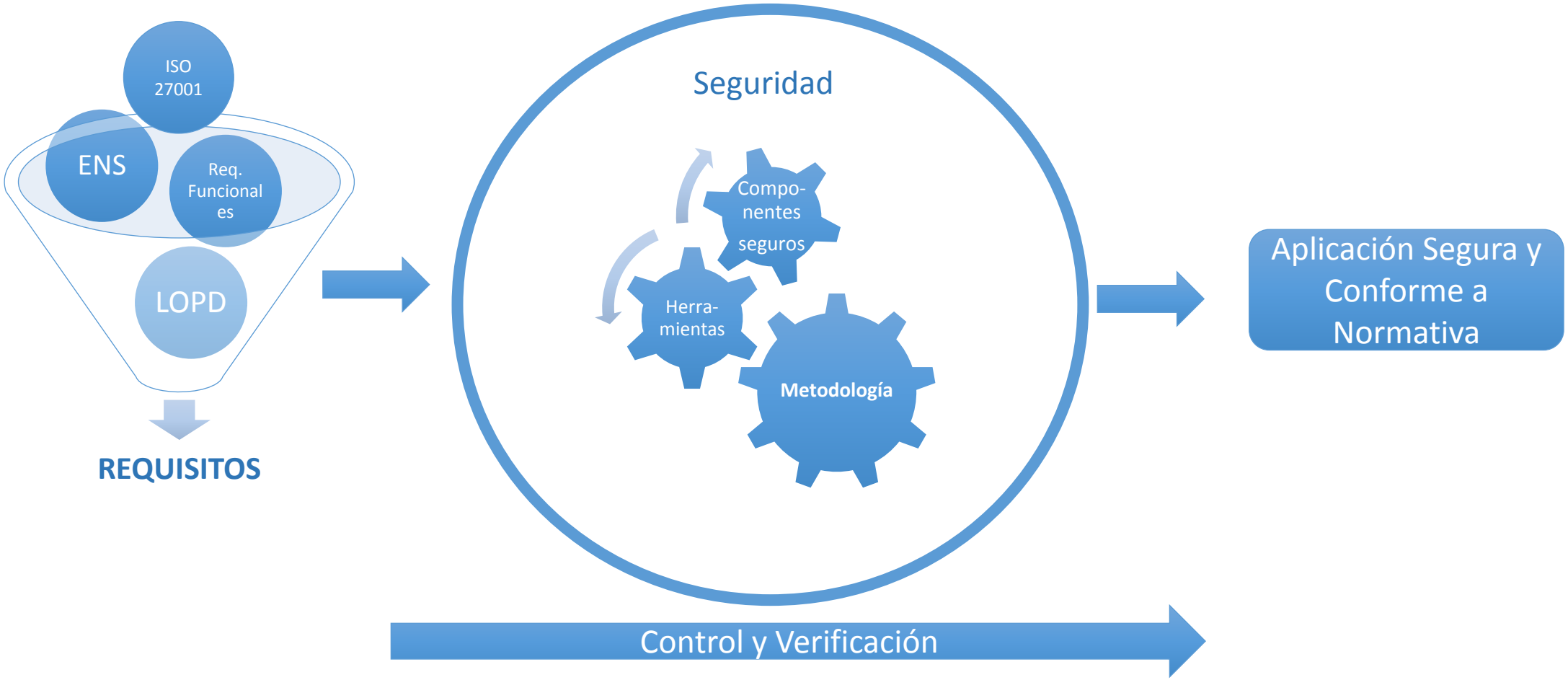
DESARROLLO:

- Pensar en la seguridad desde el inicio del proyecto
- Ser responsables de implementar la seguridad

FORMACIÓN Y CONCIENCIACIÓN

Necesidad de cambio

Cambio en la forma de trabajar:



Proyecto: gvLogos SEG

Gestión Integral de la Seguridad en el Desarrollo de Proyectos TIC

Proceso transversal al desarrollo de proyectos TIC en el que ***se incorporan las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, garantizando la seguridad en el Ciclo de Vida del proyecto y el cumplimiento de la normativa vigente en materia de seguridad (LOPD y ENS).***

gvLOGOS-SEG

Proyecto: gvLogos SEG

Aplicando seguridad en todos los proyectos

Proyecto: gvLogos SEG

I. **Identificación temprana de las necesidades de seguridad**
II. Integración del tratamiento de la seguridad en el CVDS: METODOLOGÍA
III. Soluciones y componentes de seguridad
IV. Control y verificación
V. Desarrollo de Software Seguro

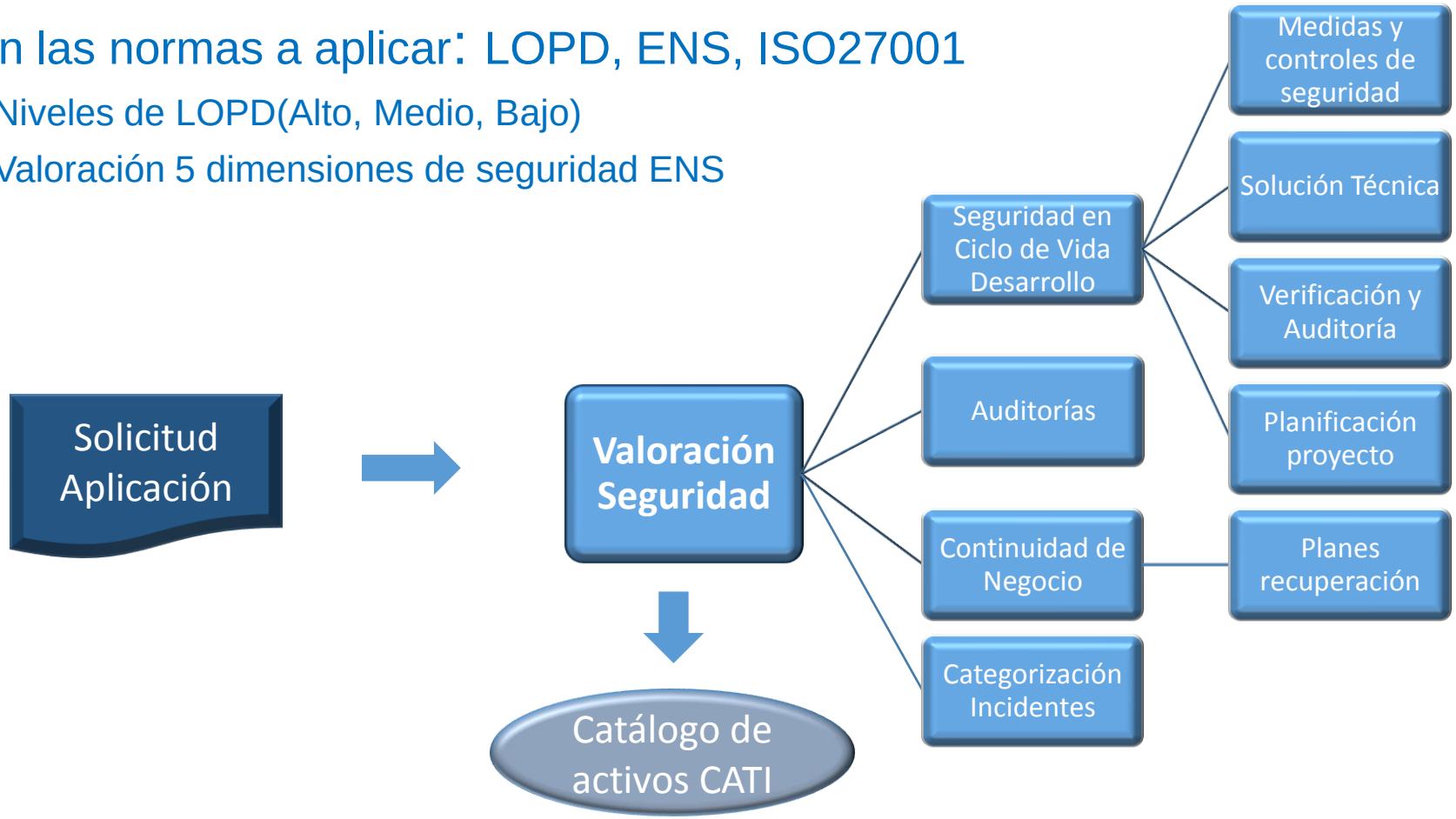
Proceso de desarrollo

Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad

Categorización según las normas a aplicar: LOPD, ENS, ISO27001

- Niveles de LOPD(Alto, Medio, Bajo)
- Valoración 5 dimensiones de seguridad ENS



Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad

Datos generales | Carac. Técnicas | Clasificaciones | Demanda | **Seguridad y Prot. datos** | ENI | Recursos Propios | Dependencias | Contratos

¿Se produce algún tratamiento de datos de carácter personal? Sí

¿Estan los datos declarados en algún fichero?: Sí ¿Cual es la calificación del nivel de las medidas de seguridad a implantar?: A (Alto)

¿Se produce alguna cesión o comunicación de datos?:

VALORACIÓN SEGÚN EL ESQUEMA NACIONAL DE SEGURIDAD

PREGUNTA	RESPUESTA
1. **CONFIDENCIALIDAD** ¿Qué consecuencias tendría la revelación de los datos a personas no autorizadas o que no necesitan conocer la información?	○ Nivel Bajo: Algún perjuicio o pérdidas económicas apreciables. ○ Nivel Medio: Daño importante aunque subsanable o pérdidas ecnonómicas importantes. ● Nivel Alto: Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas.
2. **INTEGRIDAD** ¿Qué consecuencias tendría la modificación de datos por alguien que no está autorizado para ello?	○ Nivel Bajo: Algún perjuicio o pérdidas económicas apreciables. ○ Nivel Medio: Daño importante aunque subsanable o pérdidas ecnonómicas importantes. ● Nivel Alto: Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas.
3. **AUTENTICIDAD** ¿Qué consecuencias tendría el hecho de que el origen o el destinatario de la información fuera falso?	○ Nivel Bajo: Algún perjuicio o pérdidas económicas apreciables. ● Nivel Medio: Daño importante aunque subsanable o pérdidas ecnonómicas importantes. ○ Nivel Alto: Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas.
4. **TRAZABILIDAD** ¿Qué consecuencias tendría el no poder rastrear "a posteriori" quién ha accedido o modificado una cierta información?	○ Nivel Bajo: Dificultaría la capacidad de subsanar errores o de perseguir delitos. ○ Nivel Medio: Dificultaría notablemente la capacidad de subsanar un error importarte o perseguir delitos. ● Nivel Alto: Dificultaría notablemente la capacidad de subsanar un error grave o perseguir delitos.
5. **DISPONIBILIDAD** Para valorar que consecuencias tendría el que la persona autorizada no puediera acceder a la información cuando la necesita, detallar el tiempo máximo con el servicio interrumpido.	● Nivel Bajo: Más de 5 días. ○ Nivel Medio: Entre 4 horas y un día. ○ Nivel Alto: Menor de 4 horas.

GENERALITAT VALENCIANA
CONSELLERIA D'HISENDA I MODEL ECONÒMIC

DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Castán Tobeñas, 77. Ciutat Administrativa 9 d'Octubre
46018 VALENCIA

GUÍAS METODOLÓGICAS DE ELABORACIÓN DEL DOCUMENTO DE ANÁLISIS DE ADMINISTRACIÓN ELECTRÓNICA

Unión Europea

Anexo a la Resolución de la DGTIC por la que aprueban las guías metodológicas para la elaboración de los documentos de análisis dictada en cumplimiento del artículo 94.4 del Decreto 220/2014, de 12 de diciembre por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.

VALORACIÓN SEGÚN EL ESQUEMA NACIONAL DE SEGURIDAD

Dé una respuesta para cada pregunta.

¿Qué consecuencias tendría la revelación de los datos a personas no autorizadas o que no necesitan conocer la información?

- ☐ Algún perjuicio o pérdidas económicas apreciables.
- ☐ Daño importante aunque subsanable o pérdidas económicas importantes.
- ☐ Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas

¿Qué consecuencias tendría la modificación de datos por alguien que no está autorizado para ello?

- ☐ Algún perjuicio o pérdidas económicas apreciables.
- ☐ Daño importante aunque subsanable o pérdidas económicas importantes.
- ☐ Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas

¿Qué consecuencias tendría el hecho de que el origen o el destino de la información fuera falso?

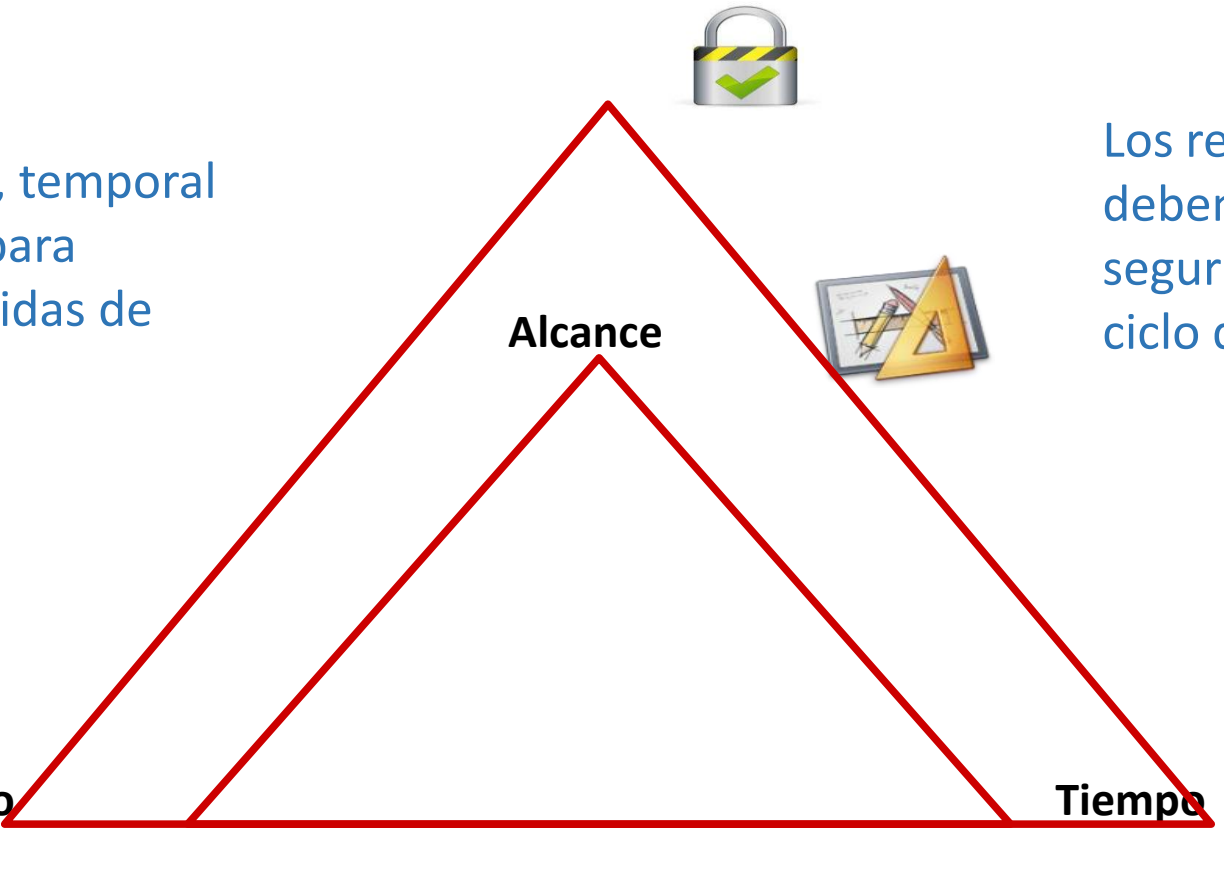
- ☐ Algún perjuicio o pérdidas económicas apreciables.
- ☐ Daño importante aunque subsanable o pérdidas económicas importantes.
- ☐ Un grave daño de difícil o imposible reparación o pérdidas económicas elevadas o alteraciones financieras significativas.

¿Qué consecuencias tendría el no poder rastrear a posteriori quien ha accedido o modificado una cierta información?

Proyecto: gvLogos SEG

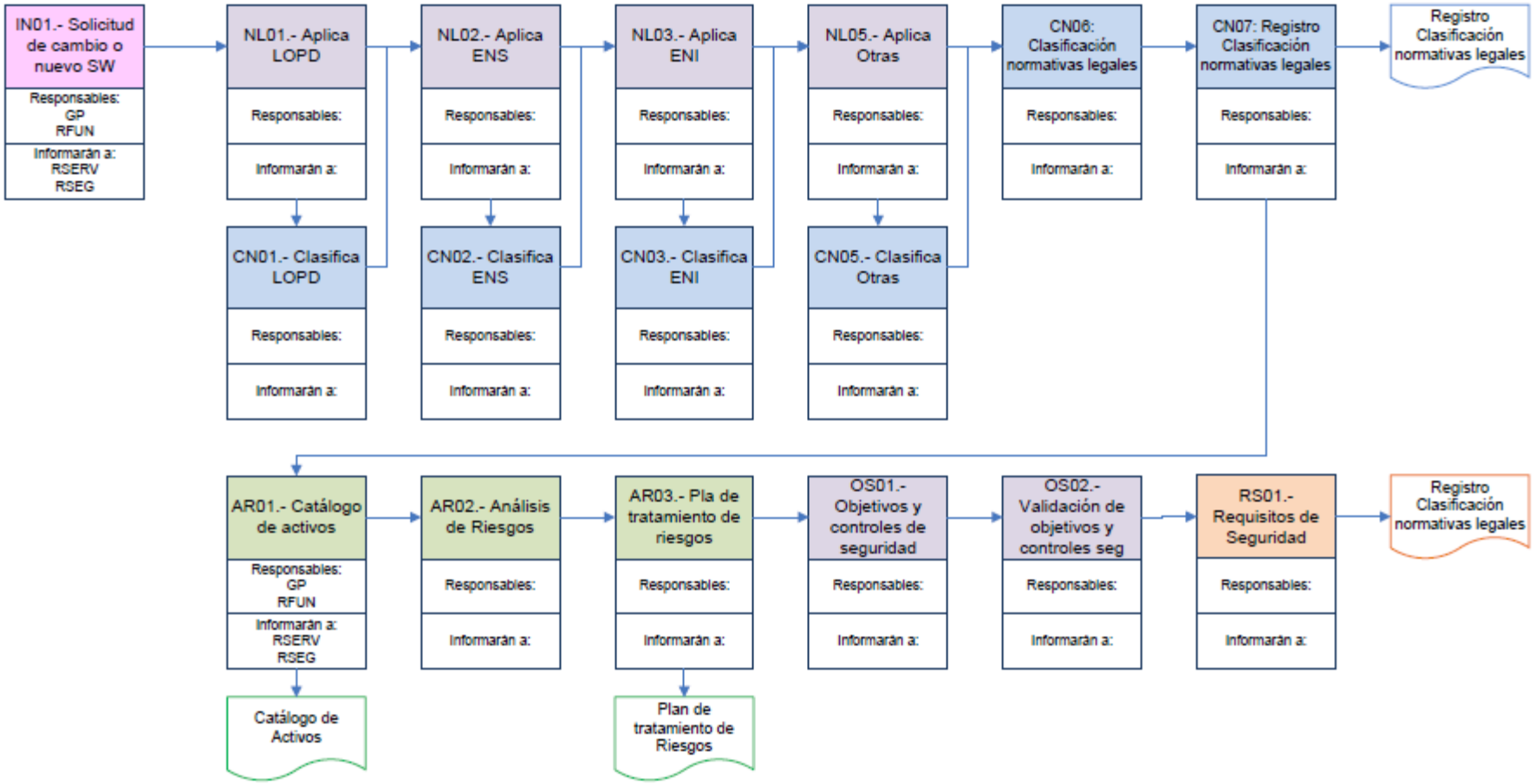
I. Identificación temprana de las necesidades de seguridad

Cobertura técnica, temporal y presupuestaria para implantación medidas de seguridad.

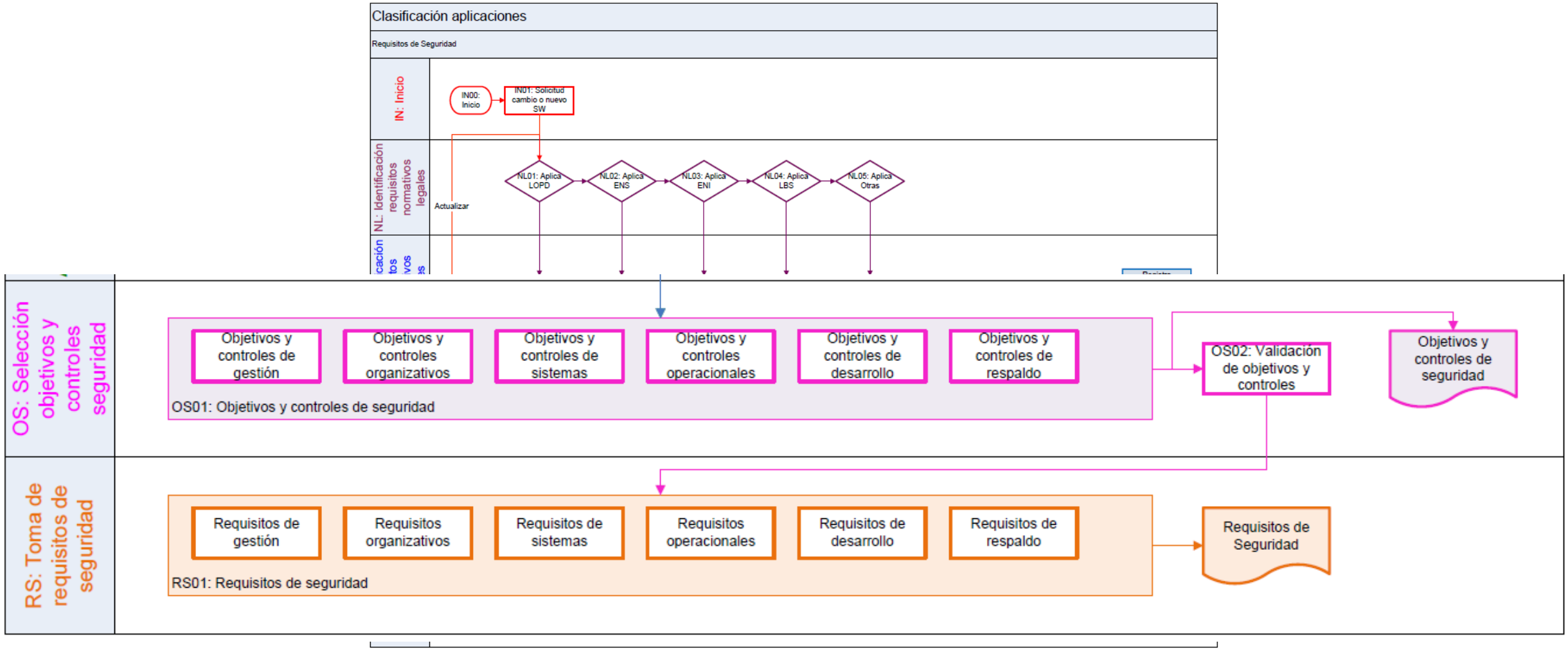


Los responsables de planificación deben tener en cuenta la seguridad en todas las fases del ciclo de desarrollo de un proyecto

I. Identificación temprana de las necesidades de seguridad



I. Identificación temprana de las necesidades de seguridad



Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad

II. Integración del tratamiento de la seguridad en el CVDS: METODOLOGÍA

III. Soluciones y componentes de seguridad

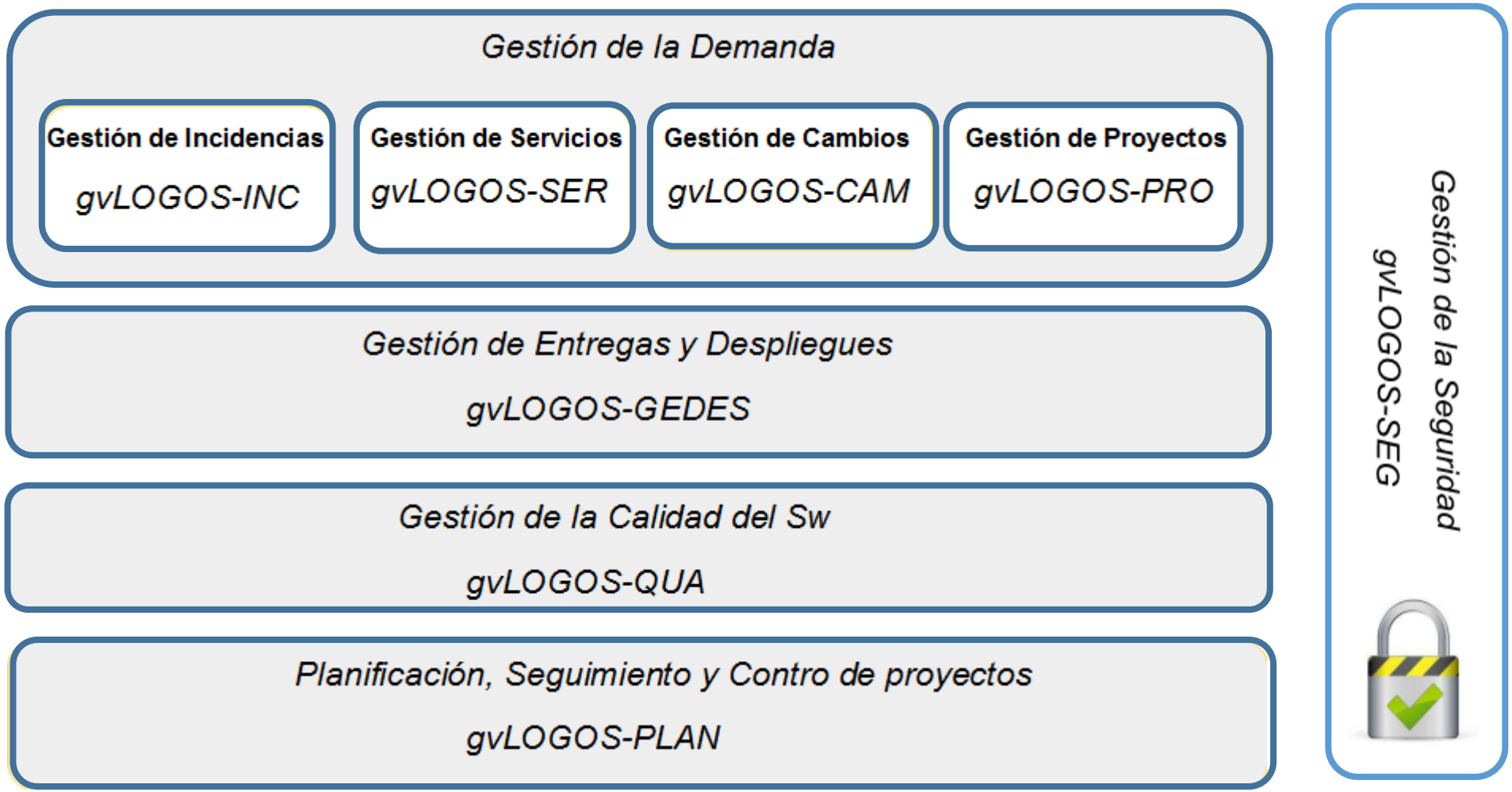
IV. Control y verificación

V. Desarrollo de Software Seguro

Proceso de desarrollo

Proyecto: gvLogos SEG

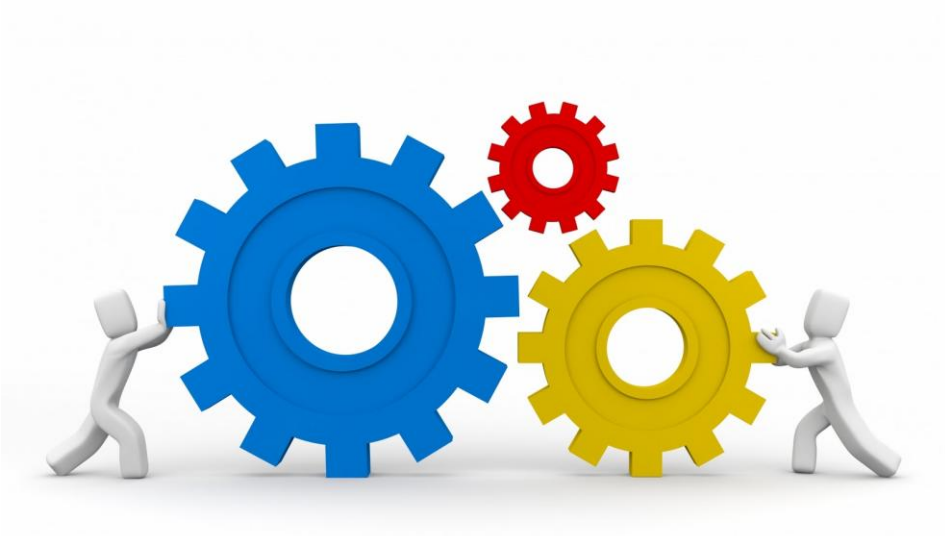
II. METODOLOGÍA



Proyecto: gvLogos SEG

II. METODOLOGÍA

1. Definir las **tareas de Seguridad** e integrarlas en la metodología en cada fase del Ciclo de Vida
   - Sincronizarlas con hitos, y documentos de la metodología GVLogos
2. Incluir los **ROLES de SEGURIDAD** y sus funciones
3. Definir los **Controles de Seguridad** y su distribución en el CV. Analizar los controles de todas las normativas a tener en cuenta (ENS, LOPD, ISO27001,…)
4. Definir **herramientas** de apoyo
5. **Documentar** la metodología
6. **Control** y seguimiento
7. **Formación**



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
NOMBRE DEL CONTROL
APLICABLE LOPD/ENS

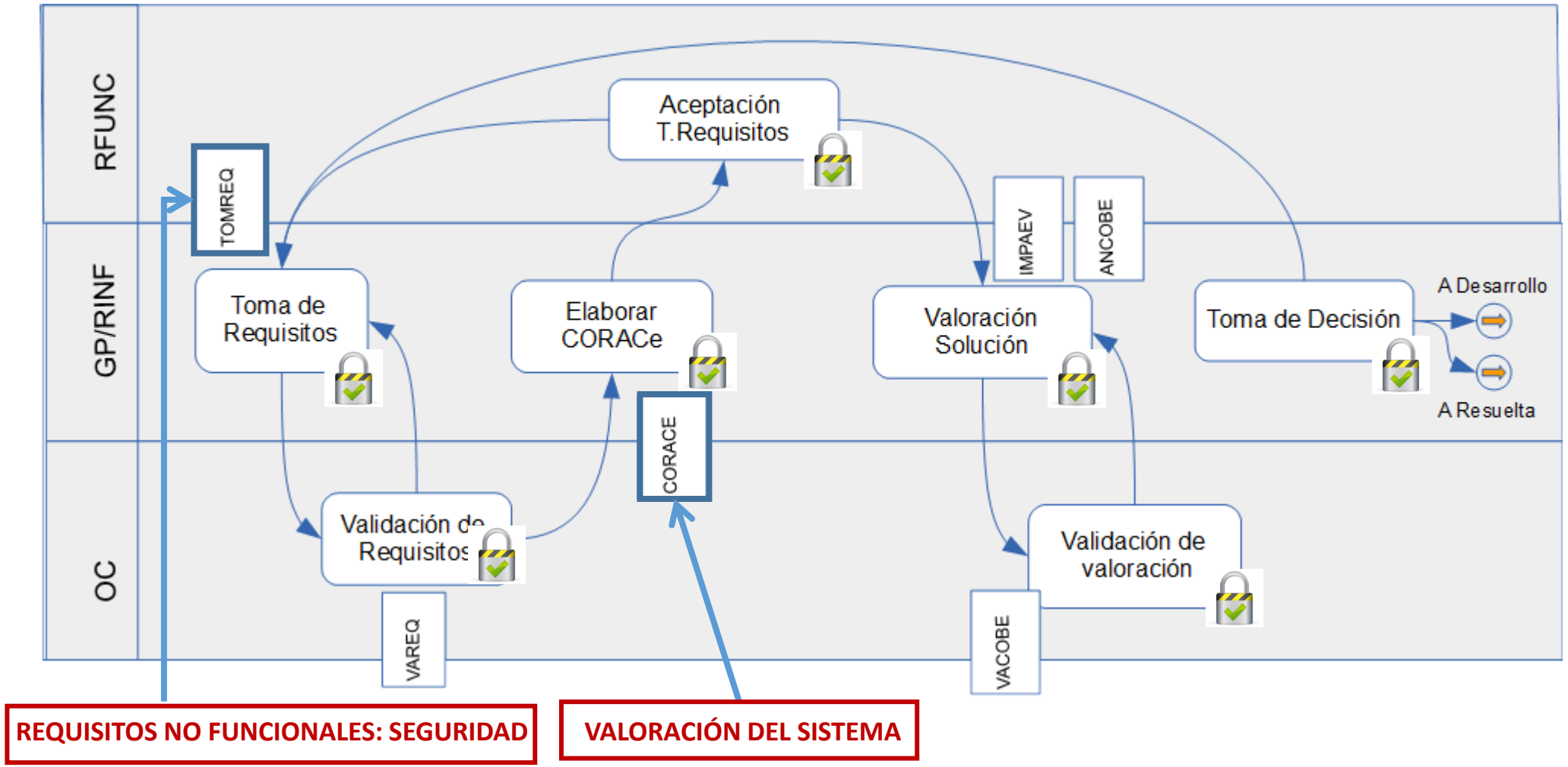
Nº	NOMBRE DEL CONTROL	PMOD	CONTROL C C S	LOPD B M A	ENS	MACI	FASE 1	FASE 2	DONDE	NORMAS ENS	NORMAS LOPD	NORMAS RIMS	NORMAS LBS-SAN	NORMAS OTRAS	Comentario	III PD ENS
	ORGANIZATIVO/LEGAL															
1	Definición Política de Seguridad	D	X		X X X	RSEG CON CS	EST	EST		art.11 org.1			1.1.1.1		Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente	Organizativo / Legal
2	Definición Política de Organización de la seguridad	D	X					EST		org.1			1.2.1.1		Definir los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.	Organizativo / Legal
3	Normativa de Seguridad. Uso correcto de equipos	D	X					EST		org.2					Debe figurar: a. El uso correcto. b. Lo que se considerará uso indebido. c. La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas de acuerdo con la legislación vigente.	Organizativo / Legal
4	Normativa de Seguridad. Uso correcto de servicios														ecto. considerará uso indebido. abilidad del personal con respecto al cumplimiento estas normas: derechos, deberes y medidas de acuerdo con la legislación vigente.	Organizativo / Legal
5	Normativa de Seguridad. Uso correcto de instalaciones														ecto. considerará uso indebido. abilidad del personal con respecto al cumplimiento estas normas: derechos, deberes y medidas de acuerdo con la legislación vigente.	Organizativo / Legal
6	Proceso formal de autorizaciones sobre utilización de instala alternativas.															Organizativo / Legal
7	Proceso formal de autorizaciones sobre entrada de equipos														equipos que involucren criptografía	Organizativo / Legal
8	Proceso formal de autorizaciones sobre entrada de aplicacio															Organizativo / Legal
9	Proceso formal de autorizaciones sobre establecimiento de comunicaciones con otros sistemas															Organizativo / Legal
10	Proceso formal de autorizaciones sobre utilización de medio habituales y alternativos															Organizativo / Legal
11	Proceso formal de autorizaciones sobre utilización de soport															Organizativo / Legal
12	Proceso formal de autorizaciones sobre utilización de equip														portátiles, PDA, u otros de naturaleza análoga	Organizativo / Legal
13	Proceso formal de autorizaciones sobre acceso a ficheros U														ne el personal autorizado para ello en el documento podrá conceder, alterar o anular el acceso bre los recursos, conforme a los criterios por el responsable del fichero	Organizativo / Legal
14	Credencial de seguridad por usuario (para acceso a aplicaci														n para ver la estructura	Organizativo / Legal
15	Procedimiento de Gestión de Credenciales de Seguridad														d de la credencial y actualización de la credencial ante cambios de privilegios en accesos	Organizativo / Legal
16	Funciones de control o autorizaciones delegadas por Responsable Fichero	P	X	X X X				EXP			riopd.1.5.9					Organizativo / Legal
17	Difusión normas seguridad a personal encargado tratamiento	P	X	X X X				EXP			riopd.1.5.9					Organizativo / Legal
18	Difusión responsabilidades a personal encargado tratamiento	P	X	X X X				EXP			riopd.1.5.9					Organizativo / Legal
19	Identificación de datos de carácter personal y asignación del nivel de seguridad	T	X	X X X				ANA		mp.info.2	riopd.0.50 riopd.0.51		1.4.1.1 1.4.1.2		Bajo, Medio o Alto	Organizativo / Legal
20	Identificación de ficheros o tratamientos datos personales	T	X	X X X				ANA		mp.info.1	lopd.20 riopd.0.52 riopd.0.54		1.4.2.1			Organizativo / Legal
21	Identificación origen y procedencia de los datos personales y posibles cesiones	T	X	X X X				EXP					1.4.2.2			Organizativo / Legal
22	Declaración de ficheros de datos personales afectados	T	X	X X X		RSLOPD RSEG		SYS	EXP		lopd.20 riopd.0.52 riopd.0.54		1.4.2.1			Organizativo / Legal

FASE 1	FASE 2
PROD	CONTROL
D	X
R	X
R	X

Nº	NOMBRE DEL CONTROL
120	Mecanismos de autenticación: Claves concertadas (algo que se sabe)
121	Mecanismos de autenticación: Claves concertadas no permitidas en sistemas de nivel medio y alto
122	Mecanismos de autenticación: Dispositivos físicos (tokens) (algo que se tiene)
123	Mecanismos de autenticación: Dispositivos físicos (tokens) no permitidos en sistemas de nivel alto
124	Mecanismos de autenticación: Dispositivos físicos personalizados + algoritmos CCN
125	Mecanismos de autenticación: Certificados software (algo que se tiene)
126	Mecanismos de autenticación: Certificados software no permitidos en sistemas de nivel alto

Proyecto: gvLogos SEG

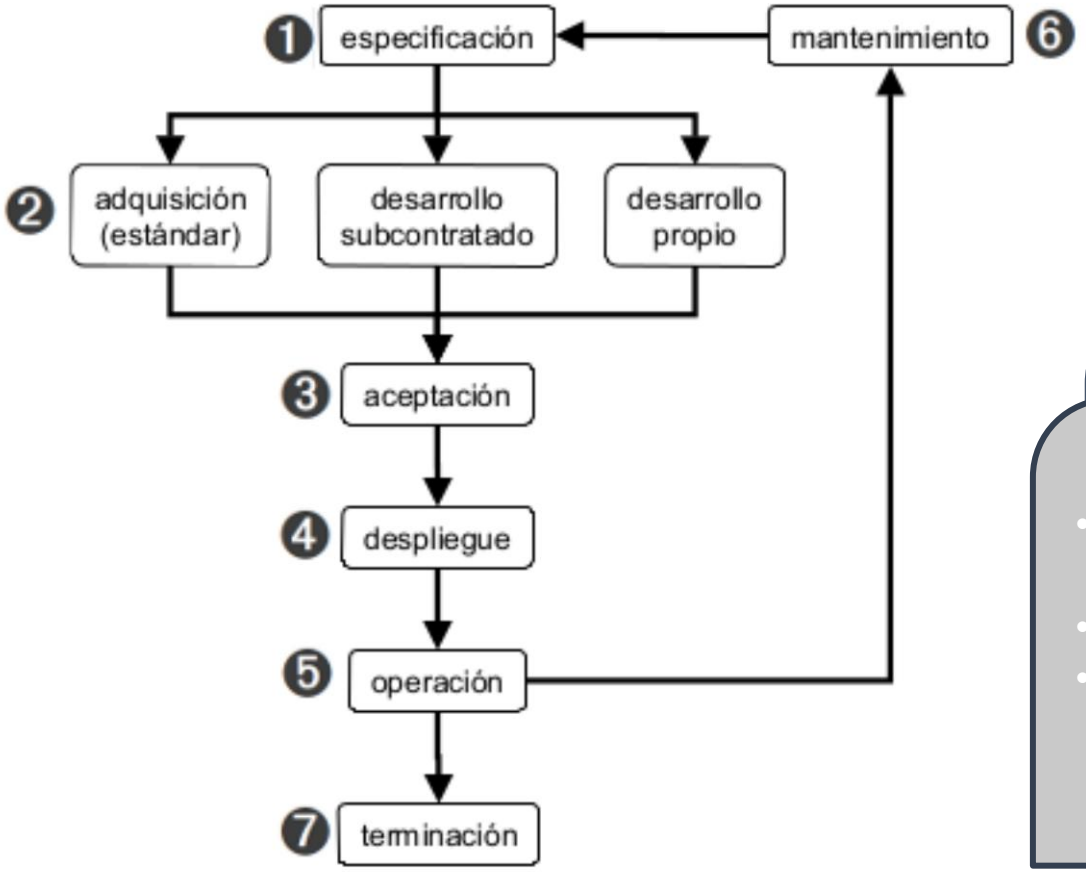
Fase de propuesta

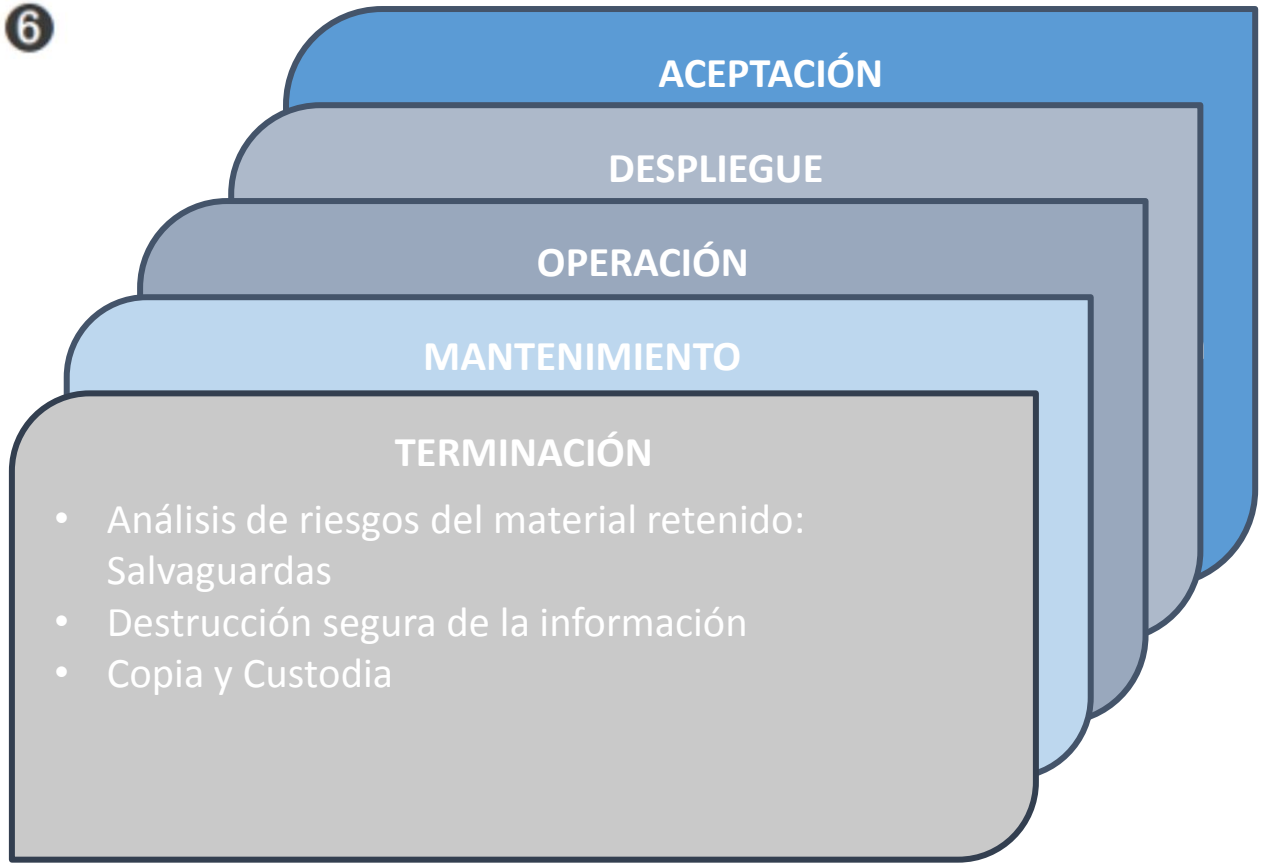


Proyecto: gvLogos SEG

II. METODOLOGÍA

En todas las fases del CVDS





Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad
II. Integración del tratamiento de la seguridad en el CVDS: METODOLOGÍA
III. Soluciones y componentes de seguridad
IV. Control y verificación
V. Desarrollo de Software Seguro

Proceso de desarrollo

Proyecto: gvLogos SEG

III. Soluciones y Componentes de seguridad

CERTIFICACIÓN DE COMPONENTES

Tipo Componente	Nombre	LOPD	DIMENSIONES					CATEGORIA ENS
			D	I	C	T	A	
OPERACIONALES								
Control de Acceso – Módulos de Autenticación	gvAut2012	M		M	M	M	M	M
	gvAut2016	M		M	M	M	M	M
	gvAut2017	A		A	A	A	A	A
Explotación – Auditoría Acceso	AudAcc_PHP					A		
MEDIDAS DE PROTECCIÓN								
Protección Aplicaciones Informáticas – Frameworks	OracleDev	M		M	M	M	M	
	JavaDev	A		A	A	A	A	
	PHPDev	M		M	M	M	M	
	AccessDev	B		B	B	B	B	
Protección de la Información - Módulos Seguridad	MSEG_java2.0	M						
	MSEG_java3.0	A		A	A	A	A	
	AudAcc_PHP	A		A	A	A	A	
Protección de la Información – Instancias Bases de Datos	Inst1_Oracle	M	A	M	M	M	M	
	Inst2_OracleVAULT	A	A	A	A	A	A	
	Inst3_PostgreSQL9	M	M	M	M	M	M	
	Inst3_PostgreSQL9 + LibCryp	A	M	A	A	A	A	
Instalaciones - Centros Proceso Datos	CPD CA90		A					A
	CPD CMIG		M					M

Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad
II. Integración del tratamiento de la seguridad en el CVDS: METODOLOGÍA
III. Soluciones y componentes de seguridad
IV. Control y verificación
V. Desarrollo de Software Seguro

Proceso de desarrollo

Proyecto: gvLogos SEG

IV. Control y Verificación

- **Auditoría ligada al desarrollo.** Embebida en el proceso de desarrollo de software, en el paso de cada una de las fases
  - Análisis de Código
  - Implantación de medidas de seguridad
  - Verificaciones de seguridad **previas a la entrada en servicio**
    - Análisis de Vulnerabilidades
    - Pruebas de Penetración
- **Auditoría periódica de la plataforma.** Al finalizar la implantación en producción, de forma periódica para detectar las vulnerabilidades publicadas, errores en el proceso de mantenimiento de la aplicación, etc.

Proyecto: gvLogos SEG

I. Identificación temprana de las necesidades de seguridad
II. Integración del tratamiento de la seguridad en el CVDS: METODOLOGÍA
III. Soluciones y componentes de seguridad
IV. Control y verificación
V. Desarrollo de Software Seguro

Proceso de desarrollo

Proyecto: gvLogos SEG

V. Desarrollo seguro

- **Seguridad en aplicaciones Web y Móvil**: recomendaciones en base a las capas de una aplicación Web y a los niveles de complejidad.
- **Seguridad en la lógica de negocio**: recomendaciones de seguridad que se aplican a las bases de datos y servidores de aplicaciones.
- **Seguridad en las** aplicaciones desarrolladas en las distintas **tecnologías** (Developer, Java, .NET, PHP, etc.)

Formación

GUÍAS DE BUENAS PRÁCTICAS

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Conclusiones

DIFICULTADES

- Falta de medios humanos y económicos
- Cambio cultural de RF > RNF a RF = RNF
- Se prioriza la creación de funcionalidades, el rendimiento, frente a la seguridad o la calidad
- Resistencia al cambio de la forma de trabajar
- Desconocimiento técnico
- Pensar que es imposible conseguirlo
- Necesidad de coordinación entre servicios y funciones e implicación de diferentes servicios

Conclusiones

FORTALEZAS

- Necesidad real de disponer de una metodología
- Complejidad de proyectos
- Volumen de proyectos
- Reorganización de las funciones
- Implicación del Servicio de Calidad
- Consciencia de la necesidad de la seguridad creciente
- Nuevo contrato CSIRT-CV

Conclusiones

FINAL

- La identificación temprana de las necesidades de seguridad y la integración de la seguridad a lo largo de todas las etapas del ciclo de vida ahorra tiempo y dinero y sobretodo **Facilita la incorporación de la seguridad en las aplicaciones.**
- Integrando la seguridad en la metodología garantizamos que la seguridad es tenida en cuenta **en todo el proyecto, por todos los equipos de desarrollo** (internos y externos) y el cumplimiento de la normativa: (ENS, LOPD, ISO27001)

Siguiendo todo el proceso obtenemos APLICACIONES SEGURAS Y CONFORMES

E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Síguenos en