Seguridad por diseño con CMMI para el desarrollo

Universidad Politecnica de Madrid
Cátedra de Mejora de Procesos de Software en el espacio Iberomericano

Gonzalo Cuevas

Zacatecas, 26/10/2014

INDICE

- **Introducción**
- **Situación**
- **Antecedentes**
- **+SAFE**
- **Seguridad por diseño**

Introducción

No podemos todavía construir sistemas que estén garantizados para ser seguros o para seguir siendo seguros en un cierto plazo.

Sin embargo, los vendedores utilizan con frecuencia el término "seguro" en presentaciones del producto y literatura del producto para referirse a productos y a sistemas que tienen "cierta" seguridad incluida en su diseño y puesta en práctica.

Introducción

La cantidad de seguridad proporcionada puede variar desde algunos mecanismos, a requisitos específicos de seguridad bien definidos y a mecanismos de seguridad bien implementados para cumplir esos requisitos. Sin embargo, proporcionar requisitos de seguridad y de funcionalidad puede no ser suficiente para engendrar confianza en el sistema.

Introducción

Intuitivamente, la confianza es una creencia o deseo que una entidad computador hará lo que debería, proteger los recursos y proteger de ataques. Sin embargo en el dominio de la seguridad en el computador, la confianza tiene un significado muy específico.

Una entidad es de confianza **si hay suficiente evidencia creíble para llevar a uno a creer que el sistema cumplirá un conjunto de requisitos dados.** La confianza es una medida de la fiabilidad, basándose en las pruebas aportadas.

Introducción

Los fallos accidentales o no intencionados de los sistemas informáticos, así como las concesiones intencionadas de los mecanismos de seguridad, pueden conducir a fallos de la seguridad. Neumann describe nueve tipos de fuentes de problemas de seguridad en los sistemas de computador:

Introducción

1. Definiciones, omisiones y errores de los requisitos,
2. Defectos en el diseño sistema
3. Defectos en la implementación de hardware, tales como cableado y defectos de chip
4. Errores en la implementación del software, errores del programa y del compilador
5. Errores en el uso y operación del sistema y errores inadvertidos

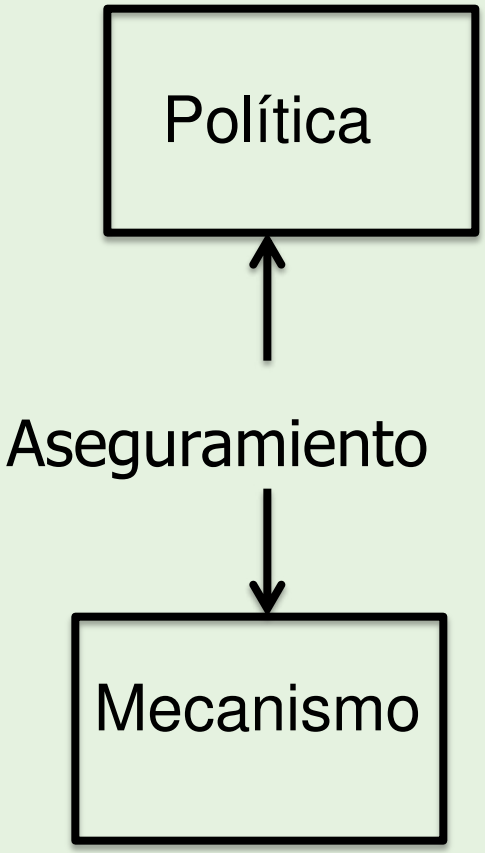
Introducción

6. Deliberado mal uso del sistema
7. Malfuncionamiento del hardware, comunicaciones u otros equipos
8. Problemas de entorno, causas naturales
9. Evolución, mantenimiento, actualizaciones defectuosas y decomisos

Introducción

- El **aseguramiento de la seguridad** es adquirido aplicando una variedad de técnicas de aseguramiento que proporcionan la justificación y la evidencia que el mecanismo, según implementado y operado, cumple los requisitos de seguridad descritos en la política de seguridad para el mecanismo (o colección de mecanismos).

Introducción



Sentencia de requisitos que define explícitamente las expectativas de seguridad del mecanismo

Proporciona la justificación de que el mecanismo cumple la política a través de la evidencia y aprobación del aseguramiento basada en la evidencia

Entidades ejecutables que son diseñadas e implementadas para cumplir los requisitos de la política

Aseguramiento de la seguridad

Introducción

La seguridad del computador descansa en 3 aspectos

Las interpretaciones de estos tres aspectos varían, como lo hacen los contextos en los cuales se presentan

Introducción

Confidencialidad

La confidencialidad es la ocultación de información o de recursos. La necesidad de mantener la información secreta surge del uso de computadores en campos sensibles tales como gobierno e industria. Por ejemplo, las instituciones militares y civiles en el gobierno restringen el acceso a la información a aquellos que necesitan esa información

Este principio también se aplica a las empresas industriales, que mantienen sus diseños patentados seguros no sea que sus competidores traten de robar los diseños.

Introducción

Integridad

La integridad se refiere a la confiabilidad de los datos o recursos, y se expresa generalmente en términos de prevención del cambio incorrecto o desautorizado.

La integridad incluye la integridad de datos (el contenido de la información) y la integridad del origen (la fuente de los datos generalmente llamada autentificación).

Introducción

La **disponibilidad** se refiere a la capacidad de utilizar la información o el recurso deseado.

Introducción

Amenazas

Una amenaza es una violación potencial de la seguridad. La violación no tiene por qué ocurrir en realidad para que haya una amenaza.

Introducción

Shirey divide las amenazas en cuatro amplias clases:

1. **divulgación** o acceso no autorizado a la información;
2. **engaño** o aceptación de la información falsa;
3. **alteración o interrupción** o **prevención** de un funcionamiento correcto; y
4. **usurpación,** o control no autorizado de una parte de un sistema.

Introducción

Crítico para el estudio de seguridad es la distinción entre la política y mecanismo.

- Una **política de seguridad** es una declaración de lo que está, y no está permitido
- Un **mecanismo de seguridad** es un método, herramienta, o procedimiento para hacer cumplir una política de seguridad.

POLÍTICA DE SEGURIDAD

Es política de OMEGA Corrosion, C.A., como empresa de asesoría y servicios industriales, asegurar la ejecución de todas sus actividades en optimas condiciones de seguridad, siguiendo las normas de protección integral a fin de garantizar la integridad y bienestar de sus trabajadores, proporcionándoles equipo de protección adecuado para sus actividades, así como también las medidas de prevención para minimizar los riesgos que se encuentran involucrados con el personal, instalaciones, medio ambiente y terceros.

OMEGA Corrosion, C.A., considera a sus empleados la fuerza mas importante de la empresa, por esta razón los mismos recibirán condiciones de trabajo saludables con el apoyo y participación de todos los niveles de la organización, para así, garantizar a sus clientes un alto estándar de calidad en nuestros servicios teniendo en cuenta que de presentarse alguna urgencia laboral la primera tarea a ejecutar será la protección personal de nuestros trabajadores.

Situación

Garantía

Consideramos que en el momento actual es fundamental para el gobierno, industrias y servicios de todo tipo el tener una garantía en la utilización de su software, así como establecer mecanismos de prevención y resistencia a los ataques, y de recuperación y actuación rápida ante emergencias mitigando al máximo o incluso anulando los efectos de los incidentes tanto internos como externos.

Situación

El 65% de los responsables TI de las empresas españolas considera que no se invierte lo suficiente en el desarrollo de políticas de seguridad TI. Como consecuencia, sólo la mitad de las empresas tienen organizados los procesos para hacer frente a las amenazas.

Antecedentes

- SAFETY EXTENSION (+SAFE) es una extensión del CMMI DEV V1.2 llevada a cabo en 2007 por la Organización de Material de Defensa Australiana para evaluar y mejorar las capacidades de una organización para proporcionar productos críticos seguros.
- Esta amplificación del CMMI se llevo acabo debido a la necesidad de una mayor seguridad en áreas especializadas de ingeniería como la ingeniería de seguridad.

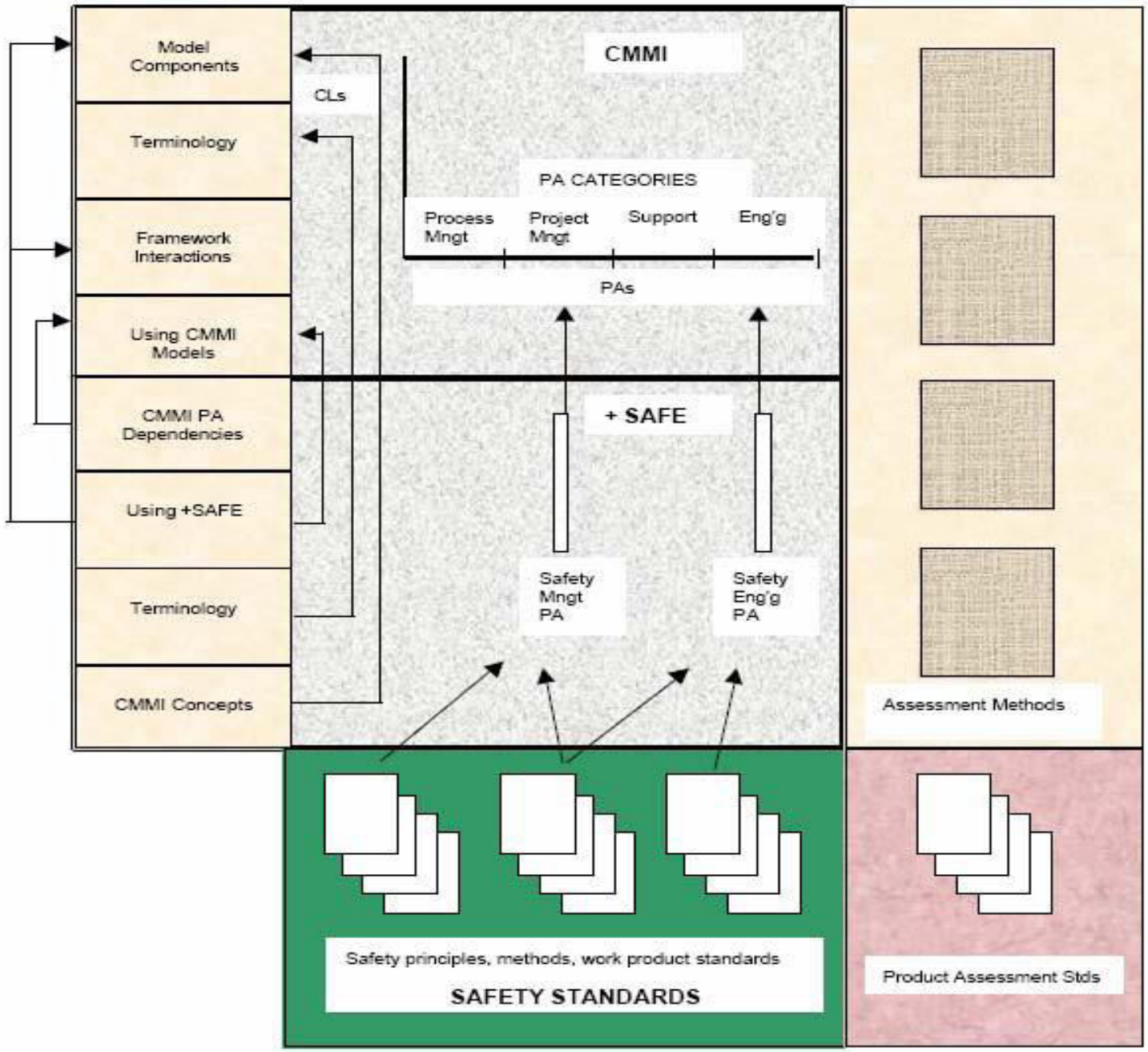
Antecedentes

Un objetivo clave de +SAFE es identificar las fortalezas y debilidades de los proveedores de productos y servicios en seguridad y tratar las debilidades identificadas pronto en el proceso de adquisición.

La extensión de seguridad fue desarrollada de modo que los evaluadores del CMMI y los usuarios redujeran su dependencia de expertos en el dominio de seguridad.

El documento de extensión +SAFE **señala como usar y evaluar la capacidad de una organización para desarrollar, sostener, mantener y gestionar la seguridad de productos críticos.**

Se desarrolló para uso independiente


Model Components
Terminology
Framework Interactions
Using CMMI Models
CMMI PA Dependencies
Using +SAFE
Terminology
CMMI Concepts
CLs
CMMI
PA CATEGORIES
Process Mngt
Project Mngt
Support
Eng'g
PAs
+ SAFE
Safety Mngt PA
Safety Eng'g PA
Assessment Methods
Safety principles, methods, work product standards
SAFETY STANDARDS
Product Assessment Stds

Seguridad por Diseño

- Cada vez ocurren más y más incidentes que son causados por ataques de hackers y ladrones de datos que tienen efectos en instalaciones importantes. **Se desea construir para resistir tales ataques *por diseño y no por casualidad.***

Seguridad por Diseño

En mayo de 2013 ante las demandas crecientes en el dominio de Seguridad, aparece "Security by Design with CMMI for Development, Version 1.3" **desarrollado por Siemens** para mejorar los procesos para productos seguros.

Desarrollar productos seguros requiere técnicas, habilidades, experiencia, y capacidades específicas de seguridad dentro de una organización.

La organización **también requiere procesos apropiados** que integren estas técnicas y capacidades en un esfuerzo sostenible para desarrollar productos seguros más allá de la prueba y error.

Seguridad por Diseño

El objetivo de esta ampliación del CMMI para seguridad es establecer **nuevos componentes en el modelo de proceso a ser utilizados para crear y mejorar sus procesos incorporando los aspectos de seguridad.**

Cuatro áreas de proceso se incorporan para definir las características de seguridad en el proceso del desarrollo

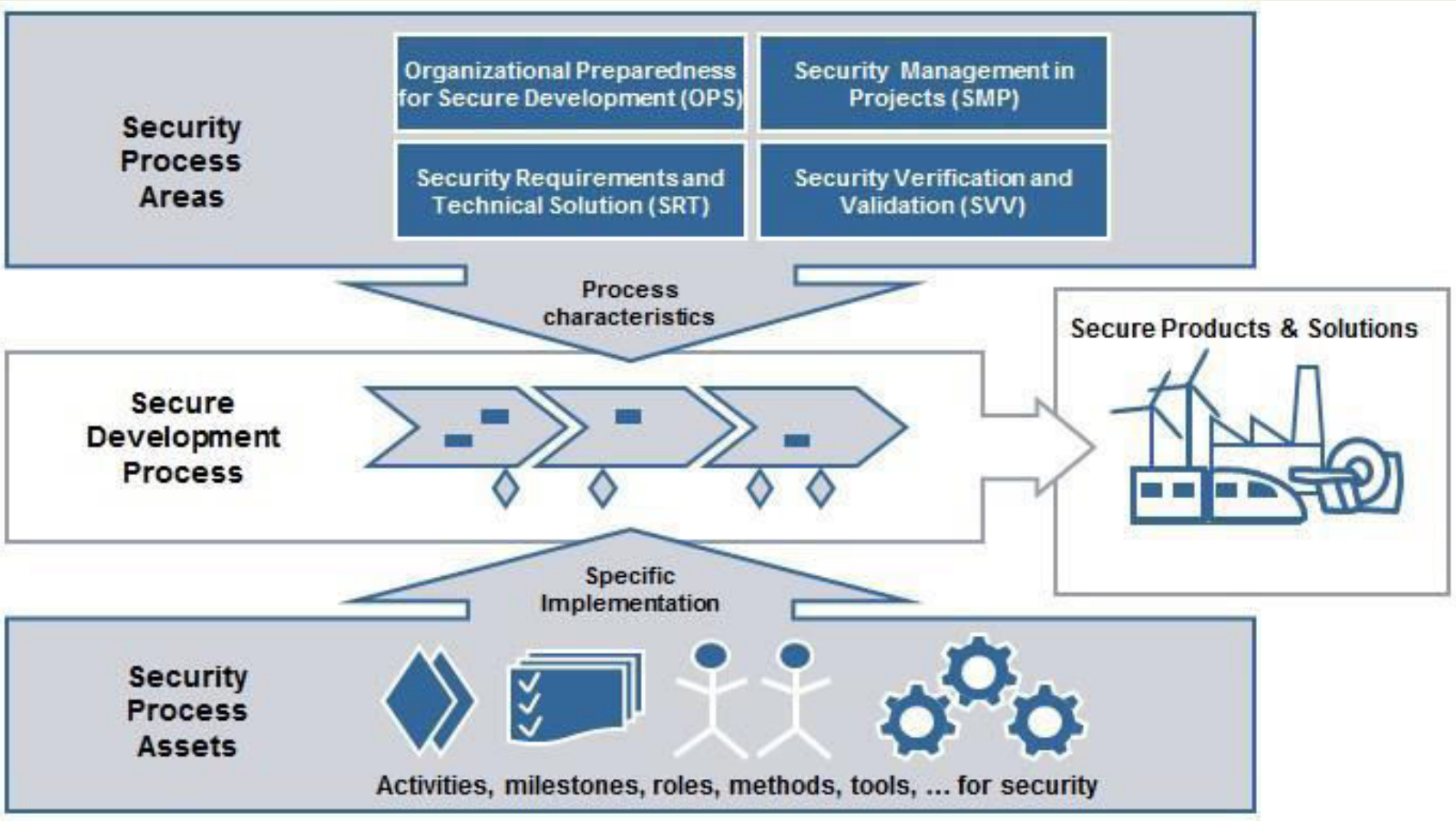
Nuevas áreas de Proceso

Incluye **dos áreas de proceso para los aspectos de seguridad en la categoría de ingeniería, una para la seguridad en la de gestión de proyectos, y una para los aspectos de seguridad en la organización (Gestión de procesos)**.

Implementando estas áreas de proceso, la organización adapta los workflows, los procesos, y los activos del proceso, por ejemplo introduciendo actividades, hitos, roles, métodos o herramientas de proceso nuevos o modificaciones de lo existentes.

Con estas actividades, la organización crea y adquiere productos que son seguros por diseño.

Seguridad por diseño define características de seguridad para el proceso de desarrollo



Áreas de proceso de seguridad

Áreas de proceso de seguridad	Propósito
Preparación de la organización para el desarrollo seguro	El propósito de preparación de la organización para el desarrollo seguro (OPSD) es establecer y mantener capacidades para desarrollar productos seguros y para reaccionar a las vulnerabilidades reportadas.
Gestión de la seguridad en proyectos	El propósito de la gestión de la seguridad en los proyectos (SMP) es establecer, identificar, planificar, y gestionar actividades relacionadas con la seguridad a lo largo del ciclo de vida del proyecto y gestionar riesgos de seguridad del producto

Áreas de proceso de seguridad

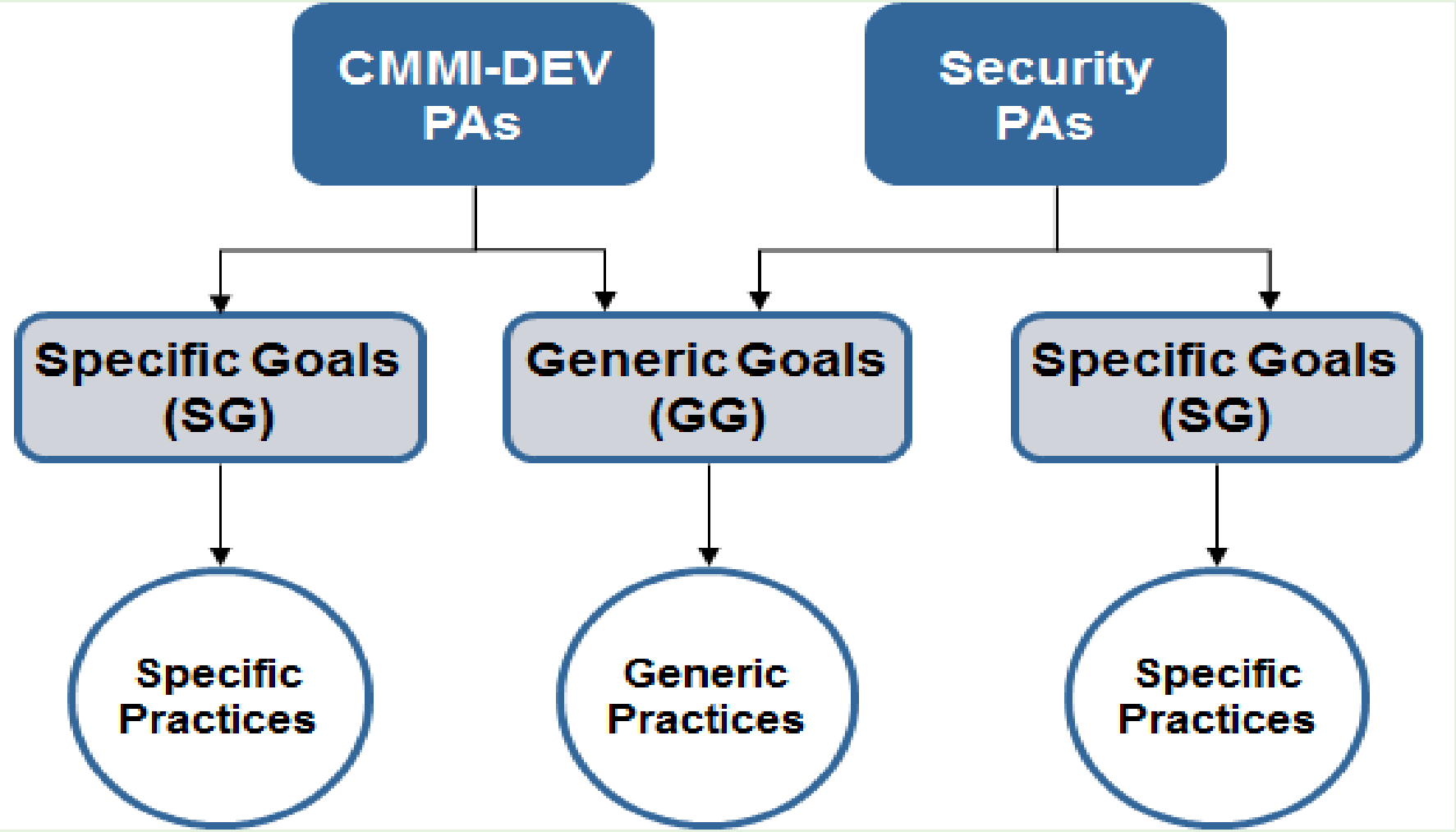
Áreas de proceso de seguridad	Propósito
Requisitos de seguridad y solución técnica	El propósito de requisitos de seguridad y la solución técnica (SRTS) es establecer requisitos de seguridad y un diseño seguro y asegurar la implementación de un producto seguro.
Verificación y validación de la seguridad	El propósito de la verificación y de la validación de la seguridad(SVV) es asegurar que los productos de trabajo seleccionados cumplen sus requisitos especificados de seguridad y demostrar que el producto o componente de producto satisface las expectativas de seguridad cuando está colocado en su entorno operacional previsto.

Seguridad por diseño: áreas de proceso

Las cuatro áreas de proceso de seguridad adicionales a CMMI-DEV proporcionan **una base explícita y enfocada para mejorar o valorar las capacidades de una organización para desarrollar productos con un nivel adecuado de seguridad.**

Se puede **utilizar independientemente** como colección de metas y de prácticas si se piensa para tratar aspectos de la seguridad en una organización que utilice ya procesos maduros.

Seguridad por diseño: Propósito y alcance



Estructura de la seguridad por diseño

CMMI-DEV Categoría Área de Proceso	***Área Proceso Seguridad***	***Metas Específicas***
Gestión Proceso	Preparación Organización para Desarrollo Seguro	SG1 Establecer una Capacidad de la Organización para Desarrollar Productos Seguros
Gestión Proyecto	Gestión Seguridad en Proyectos	SG1 Preparar y Gestionar Actividades de Proyecto para Seguridad
		SG2 Gestionar Riesgos de Seguridad de los Productos

Estructura de la seguridad por diseño

CMMI-DEV Categoría Área de Proceso	***Área Proceso Seguridad***	***Metas Específicas***
Ingeniería	Requisitos de Seguridad y Solución Técnica	SG1 Desarrollar Requisitos de Seguridad del Cliente y Arquitectura y Diseño de Seguridad
		SG2 Implementar el Diseño Seguro
Ingeniería	Verificación y Validación de la Seguridad	SG1 Realizar la Verificación de Seguridad
		SG2 Realizar la Validación de Seguridad

Expertos en seguridad

Para los programas de mejora, **los expertos de seguridad pueden desarrollar los planes apropiados de la mejora para los procesos de seguridad y también soportarlos durante la implementación**. La creación de los activos de proceso relacionados (ej., definiciones de proceso, políticas, actividades, métodos, herramientas de proceso) podría facilitarse por los expertos en seguridad.

Expertos en seguridad

Los **expertos en seguridad** que **intentan integrar actividades de seguridad sostenibles en la organización y en el proceso de desarrollo deben tener conocimientos adecuados de la mejora de proceso**.

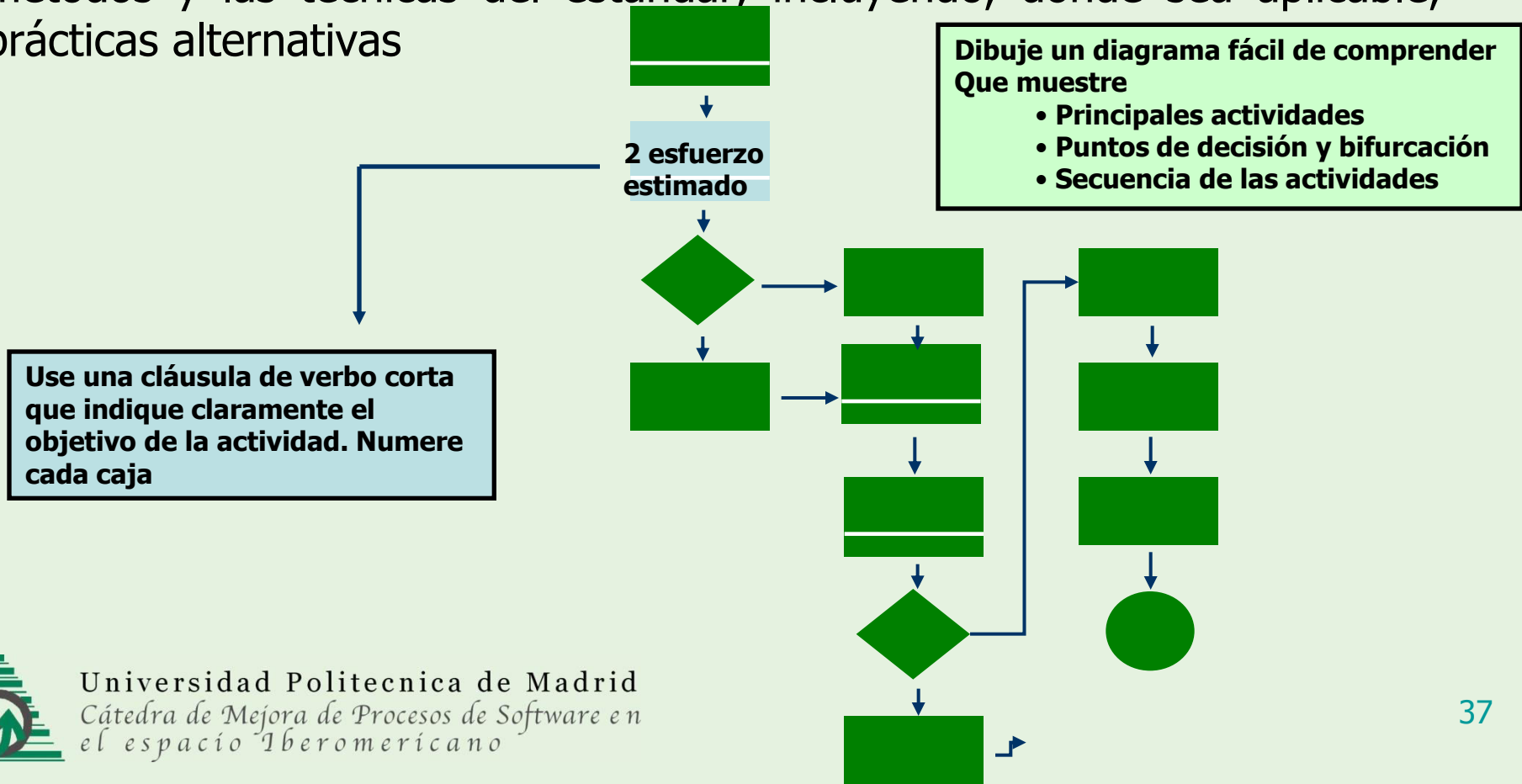
En las evaluaciones, pueden participar como **miembros del equipo de evaluación** centrándose en prácticas y productos de trabajo de seguridad. Los expertos en seguridad pueden también desarrollar recomendaciones apropiadas de mejora en la alineación de seguridad por diseño.

Los procesos de seguridad son altamente dependientes de la calidad de implementación de las áreas de proceso


CMMI PAs
Security PAs
Process Management
Organizational Process Definition (OPD)
Organizational Training (OT)
Organizational Preparedness for Secure Development (OPS)
Project Management
Project Planning (PP)
Supplier Agreement Management (SAM)
Integrated Project Management (IPM)
Security Management in Projects (SMP)
Engineering
Requirements Development (RD)
Technical Solution (TS)
Security Requirements and Technical Solution (SRT)
Verification (VER)
Validation (VAL)
Security Verification and Validation (SVV)

Consideraciones de mejora de proceso

La seguridad por diseño, como modelo de proceso de referencia, no requiere el uso de estándares específicos de seguridad. Si una organización ha seleccionado tales estándares específicos, o si estos estándares son impuestos por un contrato, una ley, o cuerpos reguladores, la seguridad por diseño se piensa para acomodar los métodos y las técnicas del estándar, incluyendo, donde sea aplicable, prácticas alternativas



Aspectos de valoración

La valoración de la seguridad se puede llevar a cabo con los métodos de valoración aplicables a CMMI (ej., SCAMPI un documento MDD V1.3 [SEI] de la descripción, o SCAMPI B/C v1.1 [SEI a 2005]).

Comparación de niveles de capacidad y Madurez

La valoración de la seguridad se puede llevar a cabo con los métodos de valoración aplicables a CMMI (ej., SCAMPI un documento MDD V1.3 [SEI] de la descripción, o SCAMPI B/C v1.1 [SEI a 2005]).

Nivel	Niveles Capacidad Representación Continua	Niveles Madurez Representación Etapas
Nivel 0	Incompleto	
Nivel 1	Ejecutado	Inicial
Nivel 2	Gestionado	Gestionado
Nivel 3	Definido	Definido
Nivel 4		Gestionado Cuantitativamente
Nivel 5		Optimizando

Aéreas de proceso y metas y practicas específicas

Requisitos de Seguridad y Solución Técnica (SRTS)

Propósito

El propósito de los requisitos de seguridad y solución técnica (SRTS) es establecer requisitos de seguridad y un diseño seguro y asegurar la implementación de un producto seguro.

Sumario de metas y practicas específicas

- SG 1 Desarrollar Requisitos de Seguridad del Cliente y Arquitectura y Diseño Seguros
  - SP 1.1 Desarrollar Requisitos de Seguridad del Cliente
  - SP 1.2 Diseñar el Producto Conforme a los Principios de Arquitectura y Diseño Seguros
  - SP 1.3 Seleccionar Tecnologías Apropiadas Utilizando Criterios de Seguridad
  - SP 1.4 Establecer estándares para Configuración Segura del Producto
- SG 2 Implementar el Diseño Seguro
  - SP 2.1 Utilizar estándares de Seguridad para la Implementación
  - SP 2.2 Añadir Seguridad a la Documentación de Soporte del Producto

Metas y practicas genéricas: elaboraciones particulares

Información común para todas las áreas de proceso incorporando detalles diferenciales elaborados para las cuatro áreas de proceso de seguridad por diseño

Metas y Practicas genéricas GG y GP

GG 1 ***Lograr las metas específicas***

Las metas específicas del área de proceso están soportadas por el proceso mediante la transformación de los productos de trabajo de entrada identificables en productos de trabajo de salida identificables.

GP 1.1 ***Realizar las prácticas específicas***

Realizar las prácticas específicas del área de proceso para desarrollar productos de trabajo y proporcionar servicios para lograr las metas específicas del área de proceso

Metas Practicas y genéricas GG y GP

GG 2 ***Institucionalizar un proceso gestionado***

El proceso está institucionalizado como un proceso gestionado.

GP 2.1 ***Establecer una política de la organización***

Establecer y mantener una política de la organización para planificar y realizar el proceso.

Practicas genéricas (GP2.1)

Elaboración SRTS

Esta política establece las expectativas de la organización para recoger y elicitar necesidades de seguridad de las partes interesadas relevantes y analizar amenazas y riesgos de la seguridad del producto. También trata de la seguridad durante el desarrollo del diseño e implementación y las expectativas con respecto a la seguridad de las tecnologías aplicadas y usadas para el desarrollo

Practicas genéricas

GP 2.2 Planificar el proceso

- ***Establecer y mantener el plan para realizar el proceso.***

GP 2.3 Proporcionar recursos

Proporcionar recursos adecuados para realizar el proceso, desarrollar los productos de trabajo y proporcionar los servicios del proceso.

Para algunos proyectos y actividades críticos puede requerirse utilizar al personal que ha experimentado la investigación apropiada de seguridad y otros controles de seguridad.

Practicas genéricas

GP 2.4 Asignar responsabilidad

- ***Asignar la responsabilidad y la autoridad para realizar el proceso, desarrollar los productos de trabajo y proporcionar los servicios del proceso.***

GP 2.5 Formar al personal

- ***Formar a las personas para realizar o dar soporte al proceso según sea necesario***

GP 2.6 Controlar los productos de trabajo

- ***Poner los productos de trabajo seleccionados del proceso bajo los niveles de control apropiados.***

Practicas genéricas

GP 2.7 Identificar e involucrar a las partes interesadas relevantes

- ***Identificar e involucrar a las partes interesadas relevantes del proceso, según lo planificado***

GP 2.8 Monitorizar y controlar el proceso

- ***Monitorizar y controlar el proceso frente al plan para realizar el proceso y tomar las acciones correctivas apropiadas.***

GP 2.9 Evaluar objetivamente la adherencia

- ***Evaluar objetivamente la adherencia del proceso y de los productos de trabajo seleccionados frente a la descripción del proceso, estándares y procedimientos, y tratar las no conformidades.***

Practicas genéricas

GP 2.10 Revisar el estado con el nivel directivo

- ***Revisar con el nivel directivo las actividades, el estado y los resultados del proceso y resolver las cuestiones.***

Metas y Practicas genéricas

GG 3 Institucionalizar un proceso definido

- ***El proceso está institucionalizado como un proceso definido.***

GP 3.1 Establecer un proceso definido

- ***Establecer y mantener la descripción de un proceso definido.***

GP 3.2 Recoger experiencias relativas al proceso

- ***Recoger experiencias relativas al proceso procedentes de la planificación y realización del proceso para dar soporte al uso futuro y a la mejora de los procesos y de los activos de proceso de la organización.***

Practicas genéricas (GP 3.1 GP 3.2)

Elaboración para todas las áreas de proceso de seguridad

- **Los activos y otros conocimientos relacionados con la seguridad (ej. vulnerabilidades, aproximaciones a la resolución de incidentes, utilidad, eficacia, e impacto en el proceso) se obtienen de una manera regular y oportuna y se ponen disponibles en una manera adecuada y proactiva para el resto de los proyectos** porque la velocidad y la puntualidad son esenciales debido a la naturaleza de los tópicos.

Practicas genéricas (GP 3.1 GP 3.2)

- **Elaboración para todas las áreas de proceso de seguridad**
- **Algunos activos de proceso (ej., creados por un proyecto) para el desarrollo seguro (ej., biblioteca de autentificación, componentes centrales de validación de la entrada y muestras de código seguro) pueden requerir la aprobación antes de ser utilizados por otros proyectos** para incrementar la seguridad, eficiencia y mantenibilidad. Todas las lecciones aprendidas, los productos ejemplares del trabajo, resultados de valoraciones y la experiencia relacionada con el proceso, etc. se registran y proactivamente se comparten con otros proyectos.

Practicas genéricas (GP 3.1 GP 3.2)

Elaboración SRTS

Algunos ejemplos de experiencias relativas al proceso son:

- Número de requisitos de seguridad introducidos en cada fase del ciclo de vida del proyecto
- Resultados de aplicar nuevos métodos y herramientas de seguridad
- Estándares desarrollados de arquitectura y diseño seguros
- Criterios desarrollados de evaluación de la tecnología
- Resultados del análisis de seguridad de la tecnología
- Estándares seguros de configuración desarrollados
- Estándares desarrollados para implementación segura

gcuevas@fi.upm.es