MÓDULO 1 MF0490_3: GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

1 Gestión de la seguridad de la información

core networks

1 Gestión de la seguridad y normativas

1.1 Gestión de la seguridad de la información

core networks

ISO 27002

La ISO 27002 se caracteriza por ser un código de buenas prácticas, ya que la que certifica la seguridad de la información es la ISO 27001.

Establece como controles esenciales:

- Protección de datos y privacidad de la información personal.
- Protección de registros organizacionales.
- Derechos de propiedad horizontal.

core networks

ISO 27002

Figura 1.1. *Categorías de seguridad de la norma ISO 27002*

SGSI

Un Sistema de Gestión de la Seguridad de la Información (SGSI), es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

¿Qué categorías de la ISO 27002 son críticas en el desarrollo de software y sistemas?

- Gestión de activos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso
- Gestión de incidentes
- Gestión de la continuidad

1 Gestión de la seguridad y normativas

1.2 Metodología ITIL

core networks

ITIL

ITIL es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

core networks

Conceptos clave

- Gestión de niveles de servicio (Acuerdos de nivel de servicio)
- Gestión de la capacidad
- Gestión de la disponibilidad

Alternativas a ITIL en cuanto a metodología

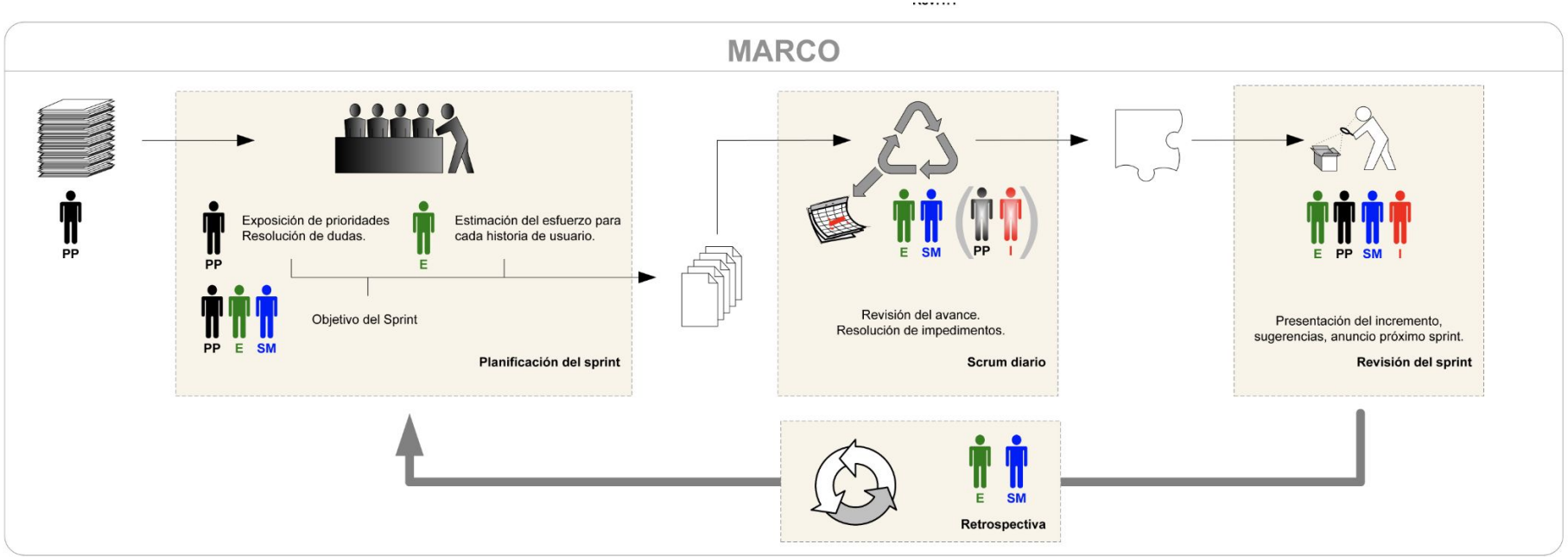
Metodologías ágiles

El desarrollo ágil de software envuelve un enfoque para la toma de decisiones en los proyectos de software, que se refiere a métodos de ingeniería del software basados en el desarrollo iterativo e incremental, donde los requisitos y soluciones evolucionan con el tiempo según la necesidad del proyecto. Así el trabajo es realizado mediante la colaboración de equipos autoorganizados y multidisciplinarios, inmersos en un proceso compartido de toma de decisiones a corto plazo.

SCRUM

Cada iteración del ciclo de vida incluye planificación, análisis de requisitos, diseño, codificación, pruebas y documentación. Adquiere una gran importancia el concepto de "finalizado" (done), ya que el objetivo de cada iteración no es agregar toda la funcionalidad para justificar el lanzamiento del producto al mercado, sino incrementar el valor por medio de "software que funciona" (sin errores).

SCRUM


MARCO
PP
PP
Exposición de prioridades
Resolución de dudas.
E
Estimación del esfuerzo para
cada historia de usuario.
PP E SM
Objetivo del Sprint
Planificación del sprint
E SM
PP I
Revisión del avance.
Resolución de impedimentos.
Scrum diario
E PP SM I
Presentación del incremento,
sugerencias, anuncio próximo sprint.
Revisión del sprint
E SM
Retrospectiva

SCRUM

ROLES

PROPIETARIO DEL PRODUCTO

Determina las prioridades.
Una sola persona.

EQUIPO DE DESARROLLO

Construye el producto.

SCRUM MASTER

Gestiona y facilita la ejecución de las reglas de Scrum

INTERESADOS

Resto de implidados. Asesoran y observan.

ARTEFACTOS

PILA DEL PRODUCTO

Relación de requisitos del producto, no es necesario excesivo detalle. Priorizados. Lista en evolución y abierta a todos los roles. El propietario del producto es su responsable y quien decide.

PILA DEL SPRINT

Requisitos comprometidos por el equipo para el sprint con nivel de detalle suficiente para su ejecución.

INCREMENTO

Parte del producto desarrollada en un sprint, en condiciones de ser usada (pruebas, codificación limpia y documentada).

EVENTOS

PLANIFICACIÓN DEL SPRINT

1 jornada de trabajo (máx.) El propietario del producto explica las prioridades. El equipo estima el esfuerzo de los requisitos prioritarios y se elabora la pila del sprint. El equipo define en una frase el objetivo del sprint.

SPRINT

Ciclo de desarrollo básico en el marco estándar de scrum, de duración recomendada inferior a un mes y nunca mayor de 6 semanas.

SCRUM DIARIO

15 minutos máximo. Responsabilidad del equipo. Cada miembro expone: Lo que hizo ayer. Lo que va a hacer hoy, si tiene o prevé problemas. Se actualiza la pila del sprint.

REVISIÓN DEL SPRINT

Informativa, máx. 4 horas, presentación del incremento, planteamiento de sugerencias y anuncio del próximo sprint.

RETROSPECTIVA

El equipo autoanaliza la forma de trabajo Identificación de fortalezas y debilidades. Refuerzo de las primeras, plan de mejora de las segundas.

core networks

1 Gestión de la seguridad y normativas

1.3 LOPD

core networks

LOPD

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), fue una ley orgánica española que tenía por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Fue aprobada por las Cortes Generales el 13 de diciembre de 1999 y derogada con la entrada en vigor, el 6 de diciembre de 2018, de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que adapta la legislación española al Reglamento General de Protección de Datos de la Unión Europea.

GDPR

El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones se fueron adaptando para su cumplimiento.

Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión, o aquellas empresas que tengan negocios en la Unión Europea, que manejen información personal de cualquier tipo, deberán acogerse a la misma. Las multas por el no cumplimiento del RGPD pueden llegar a los 20 millones de euros.

core networks

Consentimiento inequívoco y explícito

De esta manera, de forma general, según el RGPD el consentimiento tiene que ser inequívoco, no puede haber dudas de que el usuario no ha sido informado y explícito, se debe haber comunicado con qué causa se van a almacenar y tratar sus datos personales, lo que modifica la legislación anterior en la que el consentimiento tácito era válidos.

Datos sensibles (PID)

Solo pueden ser tratados (recopilados y archivados) con autorización expresa y justificación de su empleo. Son aquellos que:

- que revelen el origen étnico o racial,
- las opiniones políticas,
- las convicciones religiosas o filosóficas,
- la afiliación sindical,
- el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,
- datos relativos a la salud
- datos relativos a la vida sexual o las orientación sexuales de una persona física.

Derecho al olvido

Literalmente, el RGPD establece que el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales.

1 Gestión de la seguridad y normativas

1.4 Normativas utilizadas para la gestión de la seguridad física

core networks

Normativa de seguridad física

Además de las normativas comunes de la edificación e industrias, es recomendable cumplir las recomendaciones de la ISO 27002 que define dos tipos de medidas a implementar:

- Áreas seguras.
- Seguridad de los equipos.

Requisitos de los CPD

Recurso

http://wiki.intrusos.info/doku.php/cpd:requisitos