CMMI - Enabling

Equipo #4

José Ricardo De Anda Caballero
Brayan Uriel Sanchez Soto
Hector Jesus Solis Lazaro
Emanuel Vidal Gloria

Managing and Planning Security

Se centra en establecer y mantener procesos para gestionar y planificar eficazmente las medidas de seguridad durante todo el ciclo de vida del desarrollo de software.

Evaluación y gestión de riesgos: esto implica identificar posibles riesgos y amenazas de seguridad para el sistema o software que se está desarrollando, evaluar su impacto potencial y desarrollar estrategias para mitigar estos riesgos.

Planificación de seguridad: desarrollar planes y políticas de seguridad que describan los requisitos, objetivos y estrategias de seguridad para el proyecto. Esto puede incluir la definición de controles de seguridad, medidas de control de acceso, requisitos de cifrado y otras pautas relacionadas con la seguridad.

Arquitectura de seguridad: Diseño de la arquitectura de seguridad para el sistema o software, incluida la definición de zonas de seguridad, mecanismos de control de acceso, protocolos de autenticación y autorización.

Análisis de requisitos de seguridad: analizar los requisitos de seguridad y traducirlos en tareas específicas de diseño e implementación. Esto implica comprender las necesidades de seguridad del sistema o software y garantizar que se aborden adecuadamente en el proceso de desarrollo.

Developing secure solutions

Principios de diseño seguro: incorporar consideraciones de seguridad en la fase de diseño del desarrollo de software. Esto implica aplicar principios de diseño seguro, como privilegios mínimos, defensa en profundidad y valores predeterminados a prueba de fallos, para garantizar que la seguridad esté integrada en la arquitectura y el diseño de la solución desde el principio.

Prácticas de codificación segura: seguir prácticas de codificación segura para mitigar las vulnerabilidades de seguridad comunes, como ataques de inyección, secuencias de comandos entre sitios y referencias directas a objetos inseguras. Esto incluye el uso de estándares de codificación seguros, la realización de revisiones de código y el empleo de herramientas automatizadas de análisis de código para identificar y corregir fallas de seguridad.

Autenticación y autorización: implementar mecanismos sólidos de autenticación y autorización para controlar el acceso a recursos y funcionalidades confidenciales dentro del software. Esto puede implicar la implementación de métodos de autenticación sólidos, como la autenticación multifactor (MFA), y la implementación de políticas de control de acceso detalladas para imponer privilegios mínimos.

Protección de datos: Implementar mecanismos para proteger datos sensibles durante todo su ciclo de vida, incluido cifrado, enmascaramiento de datos y protocolos de transmisión segura. Esto garantiza que los datos estén adecuadamente protegidos tanto en reposo como en tránsito, lo que reduce el riesgo de filtraciones de datos y acceso no autorizado.

Pruebas y validación de seguridad: realización de actividades de pruebas de seguridad, como pruebas de penetración, escaneo de vulnerabilidades y revisiones de códigos de seguridad para identificar y remediar vulnerabilidades. Esto implica probar sistemáticamente los controles y mecanismos de seguridad implementados en el software para garantizar que mitiguen eficazmente las posibles amenazas.

Managing security threats and vulnerabilities

Implica establecer procesos y procedimientos para identificar, evaluar y mitigar amenazas y vulnerabilidades de seguridad a lo largo del ciclo de vida del desarrollo de software.

Identificación y evaluación de amenazas: identificación de posibles amenazas y vulnerabilidades de seguridad que podrían afectar el software que se está desarrollando. Esto puede implicar la realización de ejercicios de modelado de amenazas para analizar sistemáticamente posibles vectores de ataque y priorizar las amenazas en función de su probabilidad e impacto.

Gestión de vulnerabilidades: implementación de procesos para rastrear, priorizar y remediar vulnerabilidades de software. Esto incluye escanear periódicamente los componentes de software en busca de vulnerabilidades conocidas, evaluar su gravedad e impacto potencial y aplicar parches o implementar controles de mitigación para abordar las vulnerabilidades identificadas.

Selecting & Managing Secure Suppliers

Se le conoce como el proceso de escoger con cual vendedor prospectivo se debería entablar una organización para una relación de negocios.

Uno de los principales objetivos de seleccionar a un proveedor es poder establecer una relación de negocio mutuamente beneficiosa que pueda proporcionar el mayor dinero posible.

Etapas para seleccionar un proveedor:

1. Identificar las necesidades del negocio
2. Listar posibles proveedores
3. Determina tus criterios de selección para el proveedor
4. Conocer a los proveedores
5. Realiza un borrador, negocia y firma un contrato.

Criterios para seleccionar un proveedor

1. Calidad y seguridad de los productos
2. Flexibilidad
3. Entrega
4. Fiabilidad
5. Costo
6. Calidad de servicio

Planning & Supporting Security in Work

La seguridad en el trabajo es un aspecto importante en la industria laboral. Existen diversos aspectos de una empresa que se debe de proteger como serian los empleados y los clientes. Así mismo los datos que guardan empresas como bancos son de extrema importancia para los clientes y la misma empresa. Es importante cuidar los datos y asegurar la triada de la seguridad que es confidencialidad, integridad y disponibilidad.

Pasos para crear un plan de seguridad

1. Analizar las necesidades de seguridad
2. Realizar un plan de seguridad
3. Meter gente abordo
4. Definir y discutir respuestas a accidentes
5. Implementar el plan de seguridad
6. No lo hagas solo

Respuesta a incidentes de seguridad: Establecer procedimientos y protocolos para responder a incidentes y violaciones de seguridad de manera oportuna y efectiva. Esto puede implicar definir roles y responsabilidades para los miembros del equipo de respuesta a incidentes, establecer canales de comunicación para informar incidentes y desarrollar guías de respuesta a incidentes con pasos predefinidos para contener y mitigar incidentes de seguridad.

Monitoreo y detección de seguridad: Implementación de mecanismos para monitorear y detectar amenazas a la seguridad y actividades sospechosas dentro del entorno de software. Esto puede incluir la implementación de sistemas de detección de intrusos, soluciones de gestión de eventos e información de seguridad y herramientas de monitoreo de registros para detectar intentos de acceso no autorizados, comportamientos inusuales o indicadores de compromiso.

Concientización y capacitación sobre seguridad: Proporcionar programas educativos y de capacitación en concientización sobre la seguridad para desarrolladores, evaluadores y otras partes interesadas para aumentar su conciencia sobre las amenazas y vulnerabilidades de seguridad comunes. Esto ayuda a garantizar que el personal esté equipado con los conocimientos y habilidades necesarios para identificar y responder a los riesgos de seguridad de manera efectiva.

Gestión de la seguridad

La gestión de la seguridad es un enfoque integral que busca proteger a las personas, la información y los activos físicos de una organización contra amenazas y riesgos. Este proceso incluye la evaluación de riesgos, la implementación de medidas de control y la monitorización continua para asegurar un entorno seguro.

Comunicación y coordinación

La comunicación y coordinación son vitales para la gestión eficaz de la seguridad, asegurando que toda la organización esté alineada y preparada para responder a incidentes de seguridad. Los componentes clave incluyen:

Protocolos de Comunicación:
Definición de canales de comunicación claros y efectivos.
Protocolos de reporte de incidentes.
Comunicación regular y clara de políticas de seguridad y actualizaciones.

Coordinación Interna:
Colaboración entre diferentes departamentos (TI, recursos humanos, operaciones).
Equipos de respuesta a incidentes y comités de seguridad.
Planificación conjunta y simulacros de respuesta a emergencias.

Coordinación Externa:
Colaboración con agencias de seguridad, proveedores y socios.
Participación en redes y foros de seguridad.
Cumplimiento de regulaciones y normativas externas.

Gestionar y planificar la seguridad

La gestión y planificación de la seguridad implica desarrollar estrategias y planes que permitan a la organización anticipar, prevenir y responder a amenazas de manera eficaz. Los pasos incluyen:

Planificación Estratégica:
Definición de la visión y objetivos de seguridad.
Desarrollo de un plan de seguridad a largo plazo.
Integración de la seguridad en la estrategia general de la organización.

Desarrollo de Políticas y Procedimientos:
Creación de políticas de seguridad claras y detalladas.
Procedimientos específicos para la prevención, detección y respuesta a incidentes.
Documentación y revisión regular de las políticas.

Implementación de Programas de Seguridad:
Programas de capacitación y concienciación.
Implementación de tecnologías y herramientas de seguridad.
Programas de auditoría y evaluación continua.

Garantizar la seguridad

Garantizar la seguridad implica asegurar que las medidas y controles implementados son efectivos y se mantienen en el tiempo. Esto se logra a través de:

Evaluación Continua:
Monitoreo regular de los sistemas de seguridad.
Realización de pruebas de penetración y evaluaciones de vulnerabilidades.
Auditorías internas y externas.

Mejora Continua:
Análisis de incidentes de seguridad y retroalimentación.
Ajustes y mejoras a las políticas y procedimientos de seguridad.
Adopción de nuevas tecnologías y mejores prácticas.

Cultura de Seguridad:
Fomentar una cultura organizacional que valore y priorice la seguridad.
Involucrar a todos los niveles de la organización en las prácticas de seguridad.
Reconocer y recompensar comportamientos que refuerzan la seguridad.

supporting implementation

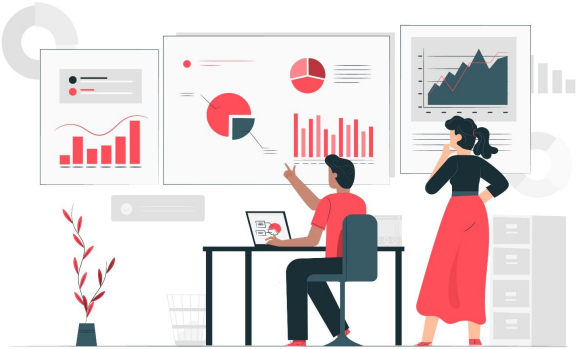
Análisis y Resolución Causal (CAR)

El Análisis y Resolución Causal (CAR) es un enfoque sistemático para identificar las causas fundamentales de los problemas o defectos e implementar soluciones para evitar su recurrencia. Se utiliza ampliamente en diversas industrias, especialmente en el desarrollo de software, control de calidad e iniciativas de mejora de procesos.

Pasos en el análisis y resolución causal

1- identificación del problema

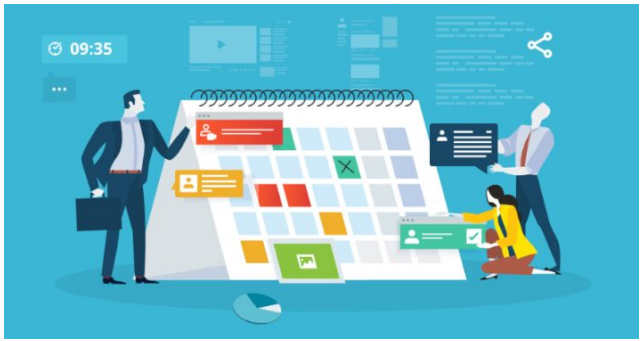
2-Recopilación de datos



Pasos en el análisis y resolución causal

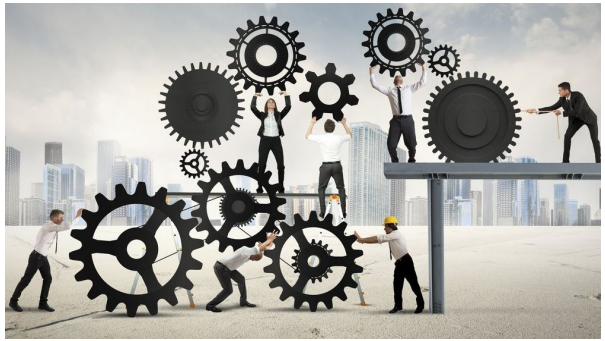
3-Análisis de causa raíz (RCA)

4-Planificación de acción



Pasos en el análisis y resolución causal

5-Implementación



6-Mejora Continua

Beneficios del análisis y resolución causal

Prevención de recurrencia: al abordar las causas fundamentales, CAR ayuda a prevenir la recurrencia de problemas, lo que conduce a una mejor calidad y confiabilidad.

Procesos mejorados: los conocimientos de CAR pueden conducir a mejoras en los procesos y operaciones más eficientes.

-Ahorro de costos: Reducir defectos y prevenir problemas puede generar importantes ahorros de costos a largo plazo.

-Satisfacción del cliente mejorada: Al mejorar la calidad del producto o servicio, CAR contribuye a una mayor satisfacción y lealtad del cliente.

-Aprendizaje Organizacional: CAR promueve una cultura de mejora continua y aprendizaje dentro de la organización.

El Análisis y Resolución de Decisiones (DAR)

El Análisis y Resolución de Decisiones (DAR) es un enfoque estructurado que se utiliza para evaluar y seleccionar la mejor opción entre múltiples alternativas. A menudo se emplea en negocios, ingeniería y gestión de proyectos para garantizar que las decisiones se basen en un análisis exhaustivo de todos los factores relevantes

Pasos en el análisis y resolución causal

1. Definición del problema
2. Identificar alternativas
3. Definir criterios de evaluación
4. Recopilar datos
5. Analizar alternativas
6. Seleccione la mejor alternativa
7. Planificación de implementación
8. Monitorear y revisar

Herramientas y técnicas

- Árboles de Decisión: Representaciones visuales de decisiones y sus posibles consecuencias.

- Análisis de decisiones multicriterio (MCDA): un método para evaluar múltiples criterios conflictivos en la toma de decisiones.

- Proceso de jerarquía analítica (AHP): una técnica estructurada para organizar y analizar decisiones complejas.

- Análisis Costo-Beneficio (CBA): Una herramienta de análisis financiero para comparar los costos y beneficios de diferentes alternativas.

- Análisis FODA: una herramienta de planificación estratégica para identificar fortalezas, debilidades, oportunidades y amenazas.

Líder: Equipo #4

Fecha: Abril 25, 2024

Avance Planeado 33%	Avance Real 33%

Name	Duration	Start
Planificación de la investigación	3 days	4/22/24 8:00 AM
Revisión de literatura	5 days	4/25/24 8:00 AM

Actividades Realizadas:

-Planificación de la investigación
-Revisión de literatura

Compromisos Pendientes:

-Recopilación de datos

Riesgos:

- Equipo Incompleto por Salida de Personal

Líder: Equipo #4

Fecha: Mayo 9, 2024

Avance Planeado 66%	Avance Real 66%

Recopilación de datos	5 days	5/2/24 8:00 AM
Análisis de los datos	3 days	5/9/24 8:00 AM

Actividades Realizadas:

-Recopilación de datos
-Análisis de los datos

Compromisos Pendientes:

-Preparación de la presentación

Riesgos:

- Fuentes difíciles de localizar

Líder: Equipo #4

Fecha: Mayo 24, 2024

Avance Planeado 100%	Avance Real 100%

Preparación de la presentación	8 days	5/14/24 8:00 AM
Revisión y finalización	1 day	5/24/24 8:00 AM

Actividades Realizadas:

-**Preparación de la presentación**
-**Revisión y finalización**

Compromisos Pendientes:

Riesgos:

- **Condiciones climaticas adversas**