

Ingeniería en Sistemas de Información

Ciberseguridad

Docente: Ing. Gabriela Nicolao

Ayudantes: Ing. Luciano Sebastianelli, Matías
Baghdassarian



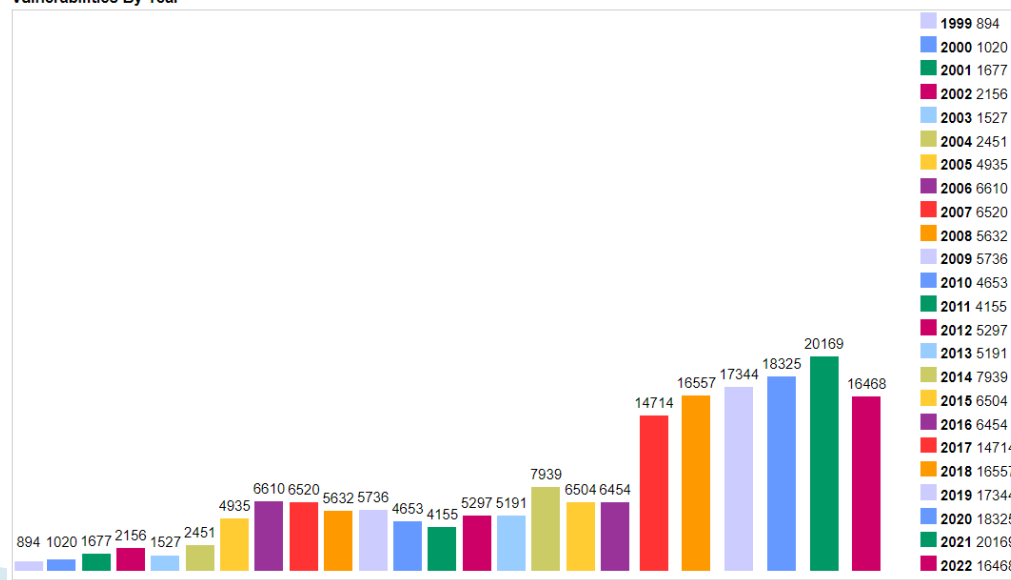
Seguridad en Desarrollo de Sistemas



Introducción a la Seguridad en Desarrollo

- ▶ Las organizaciones suelen poner mucho esfuerzo en resolver los problemas de seguridad con la implementación de firewalls, IDS, Antivirus, escáner de vulnerabilidades, etc.
 - Dichos controles permiten crear un perímetro entre el exterior y el interior de la organización.
- ▶ Sin embargo, la mayor cantidad de vulnerabilidades ocurre en los sistemas.

Vulnerabilities By Year



¿Por qué los sistemas son inseguros?

- ▶ En el pasado no se pensaba en seguridad y muchos sistemas fueron heredados.
 - Ejemplos:
 - El sistema de Oracle JD Edwards fue creado en 1977.
 - SAP fue fundada en 1972.
- ▶ Los sistemas mantienen actualizaciones y mejoras en las interfaces.
- ▶ Mantienen su diseño y no modifican las estructuras de sus sistemas.

¿Por qué los sistemas son inseguros?

Conocimientos de Seguridad

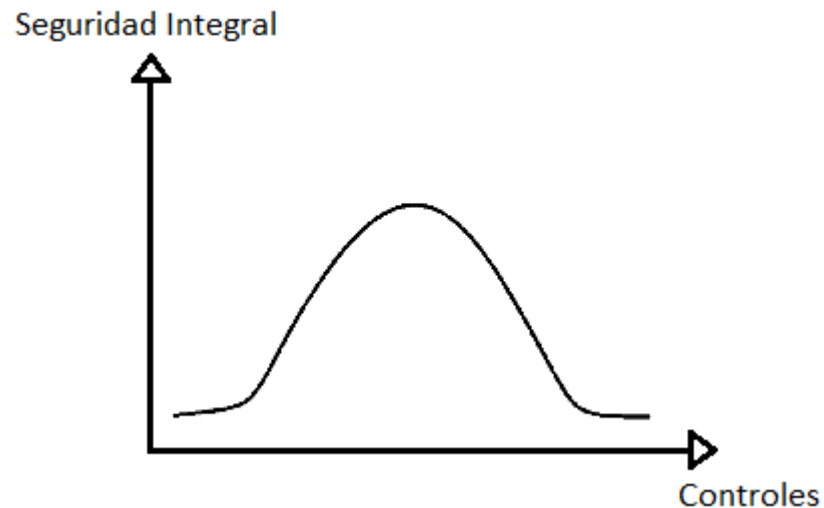
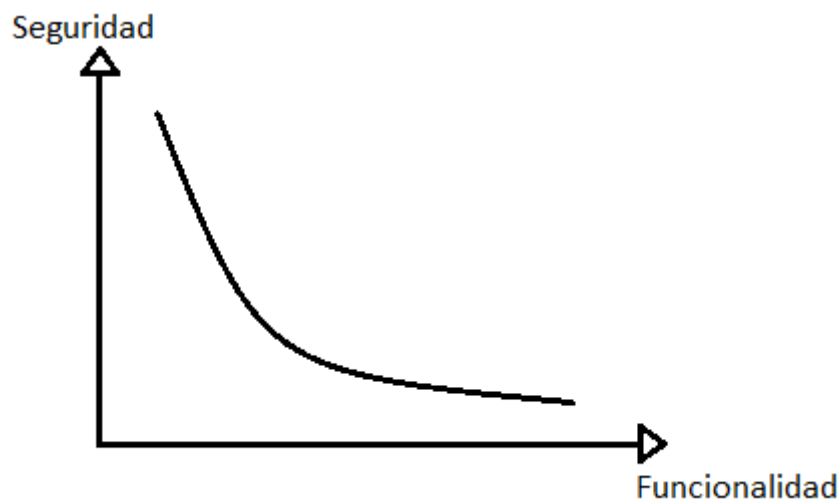


Conocimientos en Programación



¿Por qué los sistemas son inseguros?

- ▶ Los proveedores de sistemas tratan de lanzar sus productos al mercado poniendo el foco en la funcionalidad y no en la seguridad.



¿Por qué los sistemas son inseguros?

- ▶ La comunidad esta acostumbrada a recibir sistemas con vulnerabilidades y luego aplicar parches.



¿Por qué los sistemas son inseguros?

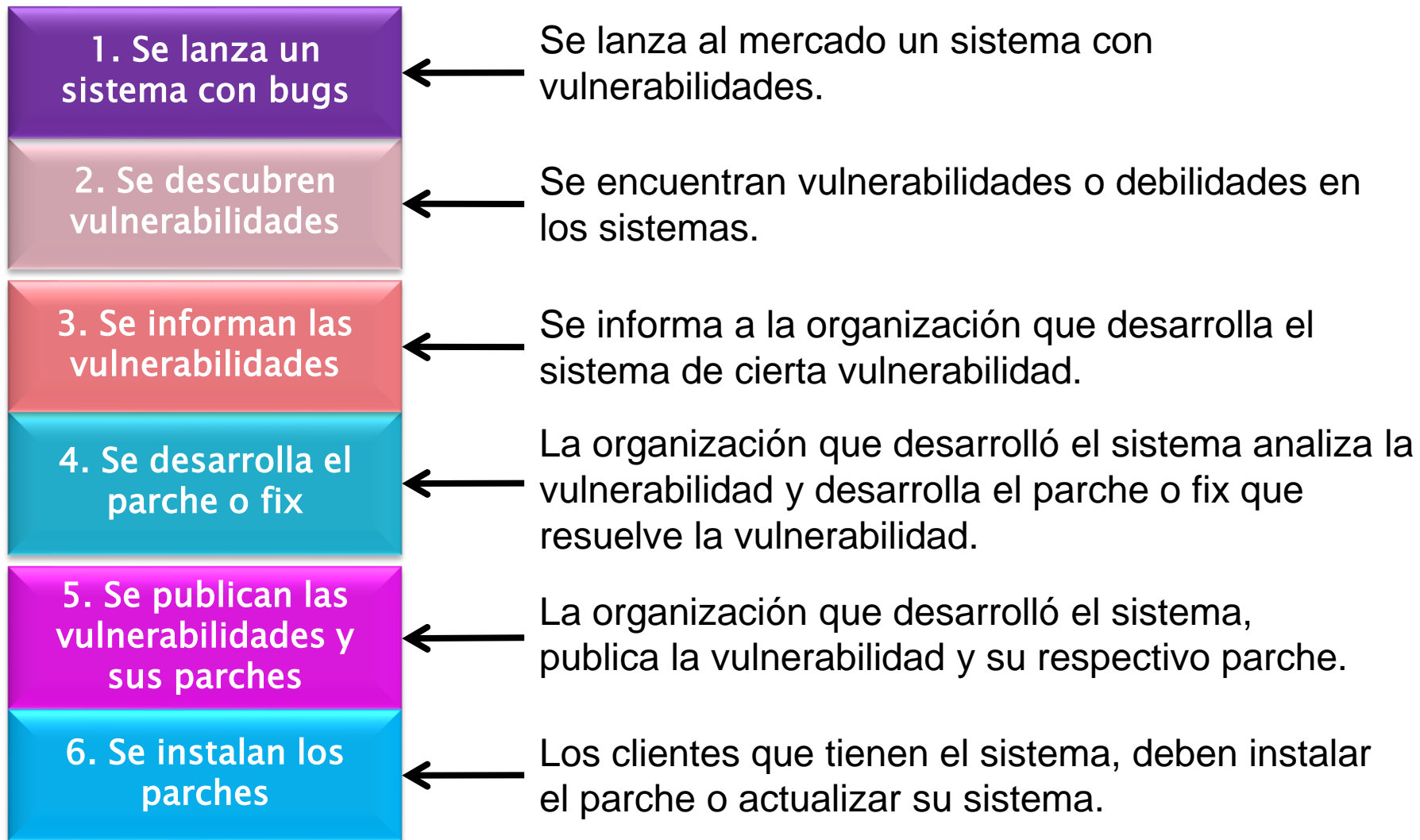
- ▶ Los clientes no pueden controlar las vulnerabilidades en los sistemas, por lo tanto tienen que confiar en ellos.



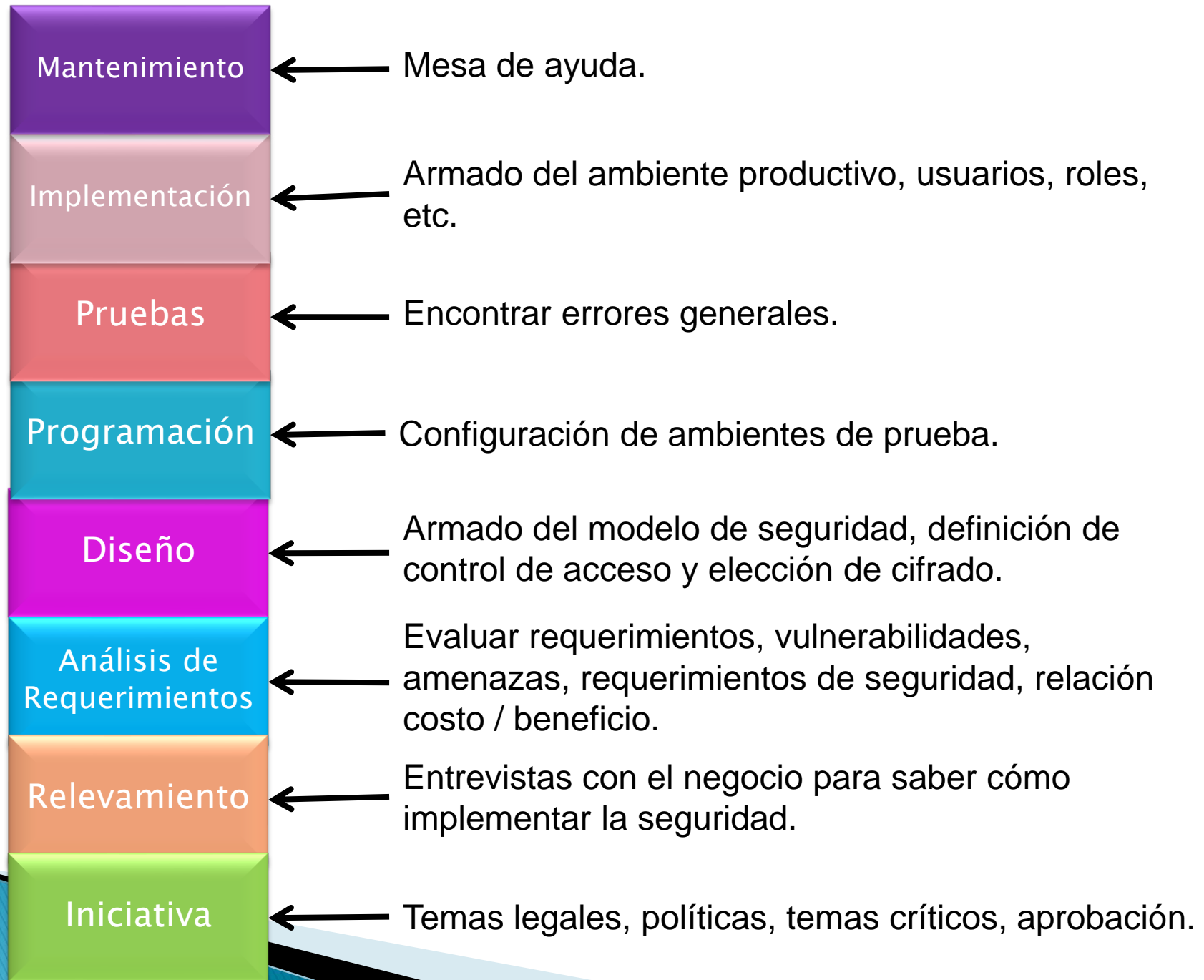
La confianza, como el arte, nunca proviene de tener todas sus respuestas, sino de estar abierto a todas las preguntas.

(Wallace Stevens)

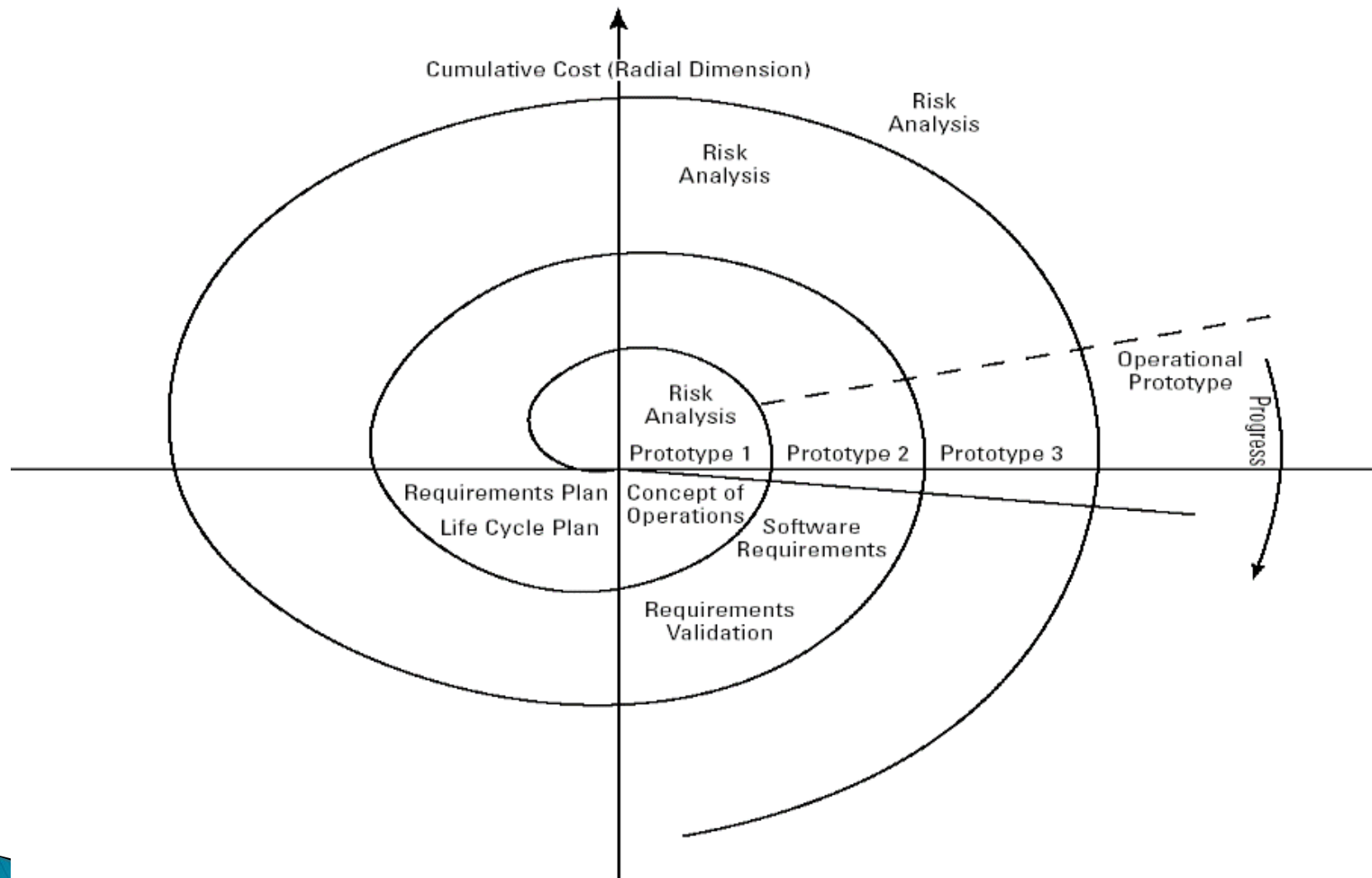
La tendencia de la Seguridad en los sistemas



Modelo Cascada

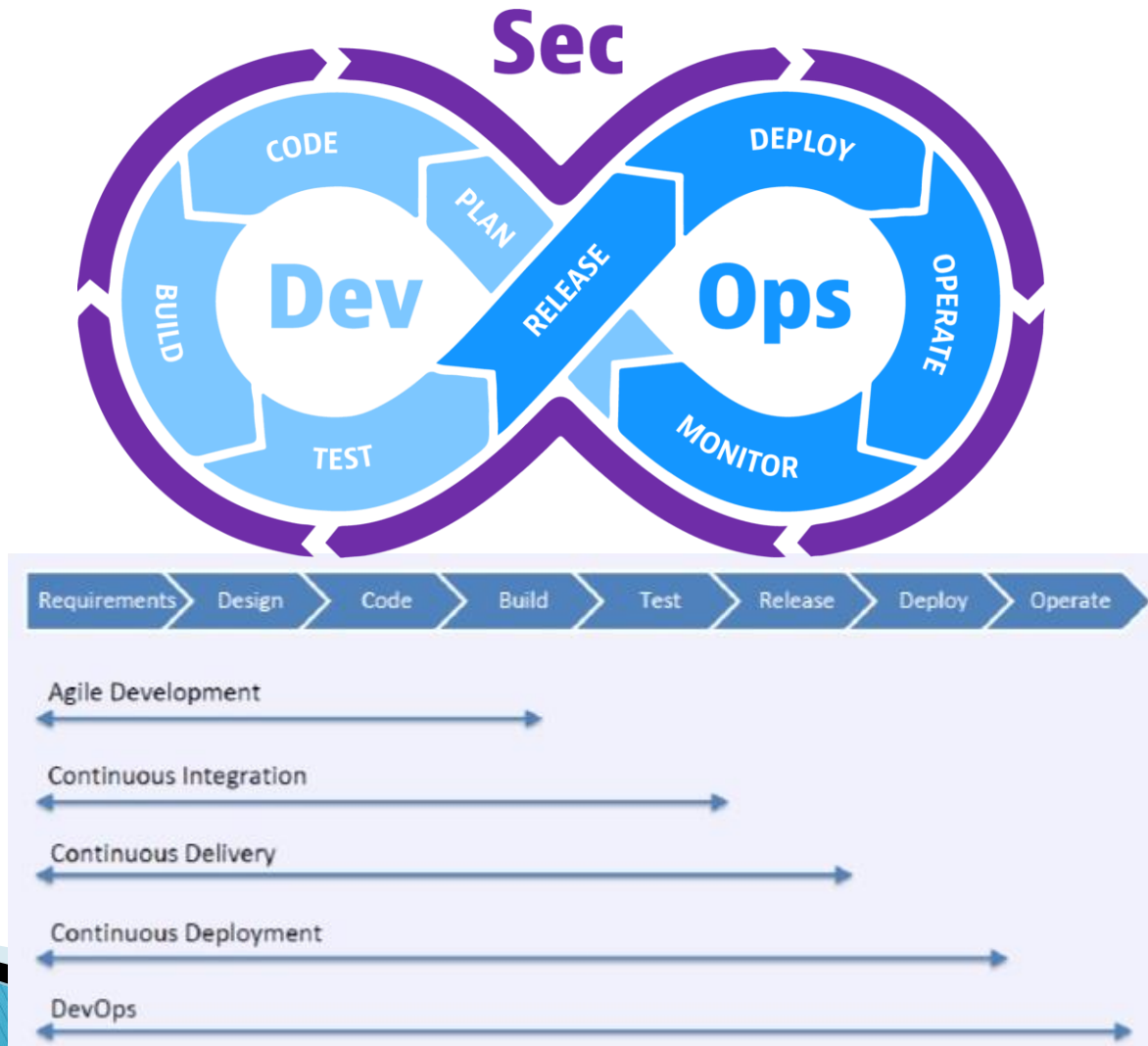


Modelo Espiral



DevSecOps

- ▶ Continuous Integration (CI) / Continuous Delivery (CD)



Variedad de entornos / ambientes

Desarrollo

Producción

Desarrollo

Pruebas

Producción

Desarrollo

Pruebas

Pre-
Producción

Producción

Desarrollo













Pruebas

Pre-
Producción

Capacitación

Producción

Accesos a los entornos

| Rol / Entorno | Desarrollo | Pruebas | Pre-Producción | Producción |
|------------------|--|--|--|---|
| Usuarios finales | | | |  |
| Usuarios claves | | |  |  |
| Desarrolladores |  | | | |
| Funcionales | |  |  | |
| Seguridad |  |  |  | |
| Tecnología |  |  |  | |

Control de cambios

- ▶ Quien lo debe hacer?
 - ¿Desarrolladores?
 - ¿Usuarios Finales?
 - ¿Administradores?
 - ¿Comité de control de cambios?
 - ¿Responsables de la aplicación?
- ▶ **Comité de control de cambios**
- ▶ El cambio debe estar analizado, probado, autorizado y documentado.
- ▶ Los cambios no deben afectar negativamente a la seguridad.



Segregación de Funciones

- Fase I: Armado de la matriz de segregación de funciones incompatibles.

| | | | Compras (B) | | | | | | | | | | | Activo Fijo (JAF) | | | | | | |
|-------------------|-------|---|------------------------------|-----------------------|---|-------------------------------------|-----------------------|-------------------------------|---------------|---------------|------------------|----------------------------------|--|--------------------------------------|--|--------------------------------------|---|--------------------|-----------------------------------|-----------------------|
| | | | B01 | B02 | B03 | B04 | B05 | B07 | B08 | B09 | B10 | B11 | | JAF01 | JAF02 | JAF03 | JAF04 | JAF05 | JAF06 | JAF07 |
| | | | ABM de Precios por proveedor | Ajustes de Inventario | Aprobación de Documentos de Compras (Requerim, Orden de Compra) | Aprobación de Precios por proveedor | Generación de Compras | Recepción de Bienes/Servicios | Generación OS | Generación OD | Aprobación OS/OD | Generación Compras Fuera Compras | | Alta de Bienes de Uso, Obra en Curso | Baja, División, Prestamos, Transferencia de Bienes | Configuraciones generales de activos | Contabilización de L/M en activos fijos | Informes generales | Proceso de Amortización y Ajustes | Proceso de fin de año |
| Compras (B) | B01 | ABM de Precios por proveedor | X | | | | | | | | | | | | | | | | | |
| | B02 | Ajustes de Inventario | N | X | | | | | | | | | | | | | | | | |
| | B03 | Aprobación de Documentos de Compras (Requerim, Orden de Compra) | N | N | X | | | | | | | | | | | | | | | |
| | B04 | Aprobación de Precios por proveedor | 1 | N | N | X | | | | | | | | | | | | | | |
| | B05 | Gen. Compras area Compras | N | N | 2 | 3 | X | | | | | | | | | | | | | |
| | B07 | Recepcion de Bienes/Servicios | 4 | N | N | 5 | 6 | X | | | | | | | | | | | | |
| | B08 | Generación OS | N | N | N | N | N | N | X | | | | | | | | | | | |
| | B09 | Generación OD | N | N | N | N | N | N | N | X | | | | | | | | | | |
| | B10 | Aprobación OS/OD | N | N | N | N | N | N | 7 | 8 | X | | | | | | | | | |
| | B11 | Generación Compras Fuera Compras | 9 | N | 10 | N | N | N | N | N | N | X | | | | | | | | |
| Activo Fijo (JAF) | JAF01 | Alta de Bienes de Uso, Obra en Curso | N | N | N | N | 11 | N | N | N | N | 12 | | X | | | | | | |
| | JAF02 | Baja, División, Prestamos, Transferencia de Bienes de Uso | N | N | N | N | 13 | N | N | N | N | 14 | | N | X | | | | | |
| | JAF03 | Configuraciones generales de activos | N | N | N | N | N | N | N | N | N | N | | N | N | X | | | | |
| | JAF04 | Contabilización de L/M en activos fijos | N | N | N | N | 15 | N | N | N | N | 16 | | N | N | N | X | | | |
| | JAF05 | Informes generales | N | N | N | N | N | N | N | N | N | N | | N | N | N | N | X | | |
| | JAF06 | Proceso de Amortización y Ajustes | N | N | N | N | N | N | N | N | N | N | | N | N | N | N | N | X | |
| | JAF07 | Proceso de fin de año | N | N | N | N | N | N | N | N | N | N | | N | N | N | N | N | N | X |

Verde:

No es conflicto (Marcado con "N")

Rojo:

Definido como conflicto (Marcado con "Y" o "3L#")

Segregación de Funciones

► Fase II: Carga y ejecución de la listas y reglas de incompatibilidades.

| Nombre Regla | Ref. | Lista A | Descripción Lista A | Lista B | Descripción Lista B | Riesgo |
|--------------|------|---------|-------------------------------------|---------|-------------------------------------|--|
| RB04B01 | 1 | B04 | Aprobación de Precios por proveedor | B01 | ABM de Precios por proveedor | Una misma persona puede alterar y aprobar los precios de compra, permitiendo fijar precios para operaciones puntuales y luego modificar ese precio para no dejar pistas. |
| RB03B05 | 2 | B03 | Aprob. documentos Compras | B05 | Gen. Compras area Compras | Una misma persona cierra un proceso de compras a precios indebidos al poder generar una orden de compra y aprobarla |
| RB05B04 | 3 | B05 | Gen. Compras area Compras | B04 | Aprobación de Precios por proveedor | Aprobación de precios de compra por personal que no tiene la jerarquía necesaria |
| RB07B01 | 4 | B07 | Recepcion de Bienes/Servicios | B01 | ABM de Precios por proveedor | Se podrían modificar ciertos precios en las ordenes de compra y realizar la recepción de los mismos. |
| RB07B04 | 5 | B07 | Recepcion de Bienes/Servicios | B04 | Aprobación de Precios por proveedor | Aprobación de precios de compra por personal que no tiene la jerarquía necesaria |
| RB07B05 | 6 | B07 | Recepcion de Bienes/Servicios | B05 | Gen. Compras area Compras | Posibilidad de registrar operaciones ficticias mediante la generación de órdenes de compra y su correspondiente recepción. |
| RB10B08 | 7 | B10 | Aprobación OS/OD | B08 | Generación OS | Una misma persona crea y aprueba una OS/OD para permitir el pago de servicios no prestados |
| RB10B09 | 8 | B10 | Aprobación OS/OD | B09 | Generación OD | Una misma persona crea y aprueba una OS/OD para permitir el pago de servicios no prestados |
| RB11B01 | 9 | B11 | Generación Compras Fuera Compras | B01 | ABM de Precios por proveedor | Personal ajeno al sector de compras puede alterar los precios de compra. |
| RB11B03 | 10 | B11 | Generación Compras Fuera Compras | B03 | Aprob. documentos Compras | Una persona fuera del área de compras puede aprobar una orden de compra en condiciones distintas a las pactadas por el área de compras. |

Segregación de Funciones

- Fase III: Identificar los usuarios con funciones incompatibles.

| Usuarios | Role | Role Description | Embedde | Embedded List Description | Programs | Programs Description | Versions | Versions Description |
|------------|------------|---------------------|---------|---------------------------|----------|---|----------|--|
| jperez | R501091670 | Analista Compras | B03 | Aprob. documentos Compras | P5943005 | Asignacion de Responsable de Aprobacion | ARC01019 | Aprobación OC Importada (6B, 6U, 6T, 6W, |
| | | | B05 | Gen. Compras area Compras | P43060 | Blanket Order Release | ARC01031 | Aprobación OC Nacional (6A, 6D, WN) |
| | | | | | | | ARC01004 | Generacion de P. C. Nac. (6A) desde req. |
| | | | | | | | ARC01005 | Generacion de P. C. Imp. (6B) desde req. |
| | | | | | | | ARC01009 | Generacion de P. C. Nac. (6A) desde req. |
| arodriguez | R501091730 | Jefe Sector Compras | B03 | Aprob. documentos Compras | P5943005 | Asignacion de Responsable de Aprobacion | ARC01010 | Generacion de P. C. Imp. (6B) desde req. |
| | | | B05 | Gen. Compras area Compras | P43060 | Blanket Order Release | ARC01703 | Generación de Pedido de Gestión (6T)desd |
| | | | | | | | ARC01704 | Generación Directa (6D) desde Req.(6Q) |
| | | | | | P43360 | Release Open Quotations | ARC01006 | Gen. P. Cpra. Imp.(6B) desde Cotiz. Punt |
| | | | | | | | ARC01010 | Gen. P. Cpra. Nac.(6A) desde Cotiz. Punt |
| | | | | | | | ARC01012 | Gen. P. Cpra. Nac.(6D) desde Cotiz. Punt |
| | | | | | | | ARC01019 | Aprobación OC Importada (6B, 6U, 6T, 6W, |
| | | | | | | | ARC01031 | Aprobación OC Nacional (6A, 6D, WN) |
| | | | | | | | ARC01004 | Generacion de P. C. Nac. (6A) desde req. |
| | | | | | | | ARC01005 | Generacion de P. C. Imp. (6B) desde req. |
| | | | | | | | ARC01009 | Generacion de P. C. Nac. (6A) desde req. |
| | | | | | | | ARC01010 | Generacion de P. C. Imp. (6B) desde req. |
| jdominguez | R501018780 | Jefe Compras | B03 | Aprob. documentos Compras | P5943005 | Asignacion de Responsable de Aprobacion | ARC01703 | Generación de Pedido de Gestión (6T)desd |
| | | | B05 | Gen. Compras area Compras | P43060 | Blanket Order Release | ARC01704 | Generación Directa (6D) desde Req.(6Q) |
| | | | | | | | ARC01006 | Gen. P. Cpra. Imp.(6B) desde Cotiz. Punt |
| | | | | | | | ARC01010 | Gen. P. Cpra. Nac.(6A) desde Cotiz. Punt |
| | | | | | | | ARC01012 | Gen. P. Cpra. Nac.(6D) desde Cotiz. Punt |
| | | | | | | | ARC01019 | Aprobación OC Importada (6B, 6U, 6T, 6W, |
| | | | | | | | ARC01031 | Aprobación OC Nacional (6A, 6D, WN) |
| | | | | | | | ARC01004 | Generacion de P. C. Nac. (6A) desde req. |
| | | | | | | | ARC01005 | Generacion de P. C. Imp. (6B) desde req. |
| | | | | | | | ARC01009 | Generacion de P. C. Nac. (6A) desde req. |
| | | | | | | | ARC01010 | Generacion de P. C. Imp. (6B) desde req. |
| | | | | | | | ARC01703 | Generación de Pedido de Gestión (6T)desd |

Segregación de Funciones

- ▶ Fase IV: Armado del Plan de Acción correctivo:
 - Modificación de accesos.
 - Justificación de los conflictos.

Estimado/a,

El presente documento tiene por finalidad justificar las incompatibilidades de funciones identificadas. Las mismas fueron validadas en conjunto con los referentes funcionales del negocio y auditoría interna.

| | |
|--|---|
| Conflicto | Generación de Compras (RAB406 - Compras Nacionales (6A - 6D))) Vs Aprobación de Documentos de Compras (RAB406 - Aprobación de OC) |
| Usuarios Involucrados | R501079720 Jefe Sector Eventos/Promociones |
| Riesgo del Conflicto | Desvíos no autorizados pueden incurrir al generar y aprobar órdenes de compra por una misma persona. |
| Comentario Auditoría Interna | |
| Negocio | Compras |
| Base / Planta | Maipú |
| Referente Funcional | 50107421 - Jefe Compras: Edgardo S. De Gaetano |
| Responsable del Negocio | 50106704 - Gte. Corp. Suministros 50107421 - Jefe Compras |
| ¿Aprueba el conflicto identificado? (Sí/No) | Si |

Comentario del Responsable del Negocio (Mandatorio):

Se aprueba el conflicto por falta de personal para dividir las funciones en el área en cuestión.

¿Qué loguear y dónde?

► ¿Qué es necesario loguear?

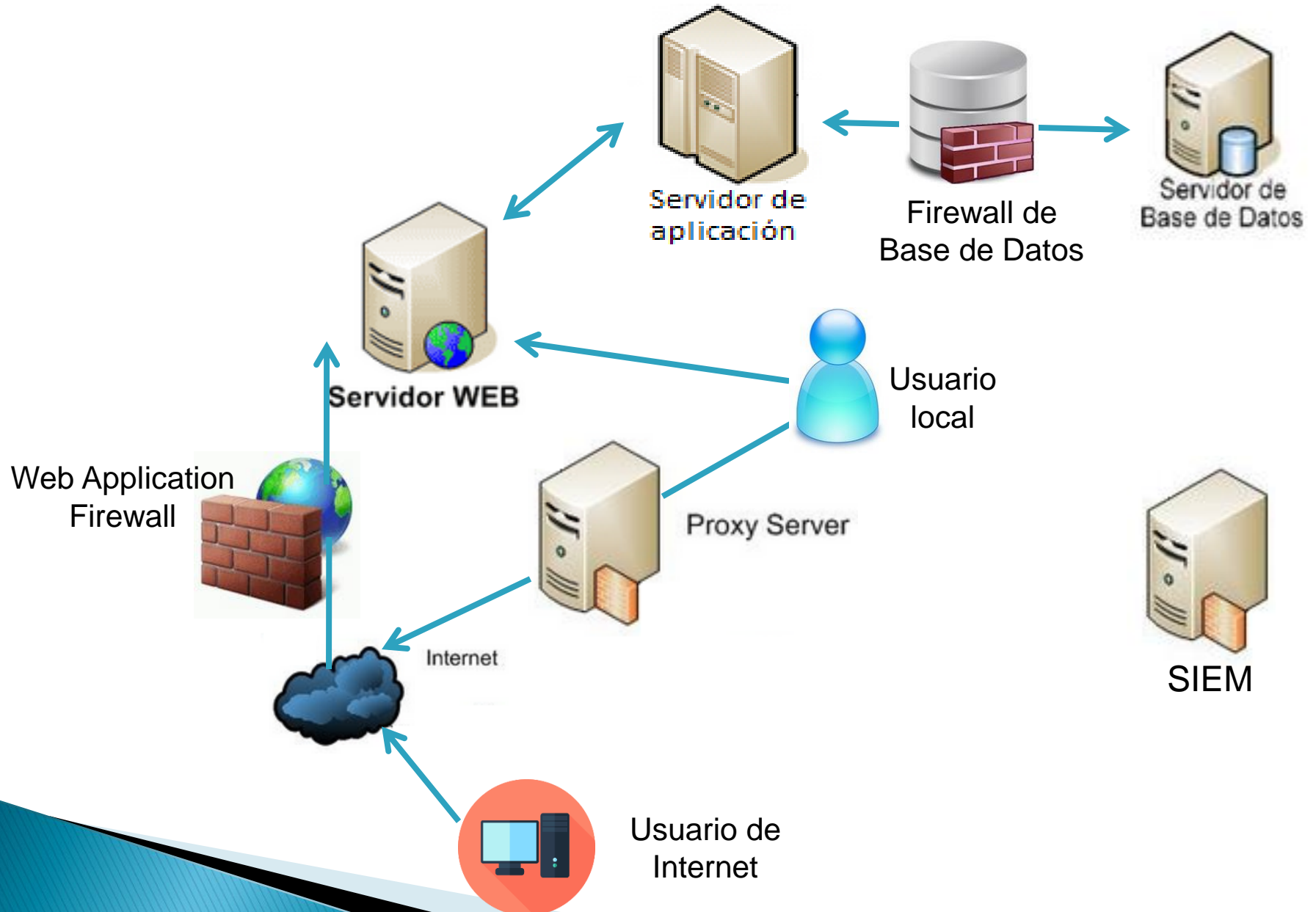
- Definir que eventos registrar.
 - Monitoreo usos indebidos, cambios de contraseña, ABM de usuarios.
- Definir distintos niveles.
- Contar con evidencia de los casos de incidentes de seguridad.

► ¿Dónde loguear?

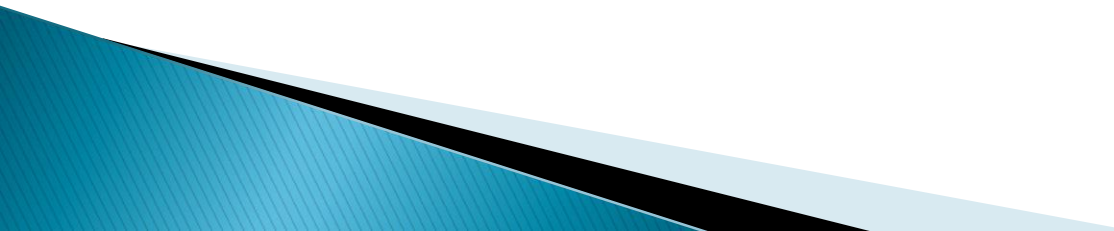
- Archivos propios de la aplicación:
 - Ingresos.
 - Cambios en el sistema.
 - Transacciones críticas de negocio.
- Logging local:
 - Windows – Visor de sucesos.
 - Unix – Syslog.
- Consola de administración de log centralizada.



Arquitectura de sistemas



Técnicas de ataque

- ▶ Búsqueda de revelación de información.
 - ▶ Búsqueda de vulnerabilidades conocidas.
 - ▶ Explotación de vulnerabilidades top 10 OWASP.
 - ▶ Fuzzing.
 - ▶ Ingeniería inversa/análisis de código.
 - ▶ Análisis de protocolos.
- 



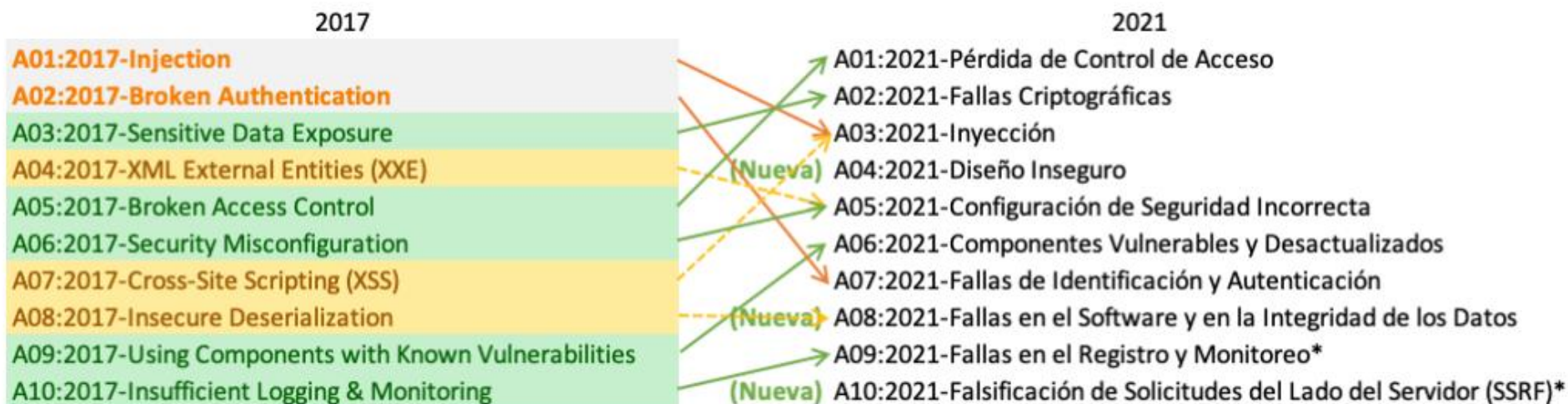
OWASP (Open Web Application Security Project)



Top 10 2021

- ▶ A1 – Pérdida de Control de Acceso.
- ▶ A2 – Fallas Criptográficas.
- ▶ A3 – Inyección.
- ▶ A4 – Diseño Inseguro.
- ▶ A5 – Configuración de Seguridad Incorrecta.
- ▶ A6 – Componentes Vulnerables y Desactualizados.
- ▶ A7 – Fallas de Identificación y Autenticación.
- ▶ A8 – Fallas en el Software y en la Integridad de los Datos.
- ▶ A9 – Fallas en el Registro y Monitoreo.
- ▶ A10– Falsificación de Solicitudes del Lado del Servidor (SSRF).

Comparación Top 10 2017-2021



* A partir de la encuesta

A1 – Pérdida de Control de Acceso

► Exploit

- La explotación del control de acceso es la habilidad principal de los atacantes. Puede darse por la falta del control o por una mala implementación.

► Vulnerabilidad

- Las debilidades de control de acceso son comunes debido a la falta de detección automática y a la falta de pruebas funcionales efectivas por parte de los desarrolladores de aplicaciones.

► Impacto

- Personas no autorizadas actúan como usuarios sin privilegios o administradores, o usuarios pueden utilizar funciones privilegiadas, o crear, acceder, actualizar o eliminar registros.

► ¿Cómo prevenirlo?

- El control de acceso solo es efectivo si se aplica código confiable del lado del servidor.
 - Ejemplos: “denegación por defecto”, capturando las excepciones, implementando control de acceso, deshabilitando el listado de directorio, implementando logs, etc.

A2 – Fallas Criptográficas



► Exploit

- A través de fallas en la implementación de sistemas criptográficos, la información sensible queda expuesta. Permite robar credenciales, realizar ataques “man-in-the-middle”, robar datos en texto claro/plano del servidor (mientras se encuentran en tránsito o desde el navegador del usuario).

► Vulnerabilidades

- La vulnerabilidad mas común es no cifrar datos sensibles.

► Impacto

- Las fallas potencialmente comprometen toda la información que debería estar protegida como tarjetas de créditos, registros médicos, datos personales, etc.

► ¿Cómo prevenirlo?

- Aplicar algoritmos de cifrado para los datos sensibles.
- No almacenar datos sensibles innecesariamente.
- Asegurarse que las claves se almacenen con un algoritmo especialmente diseñado para protegerlas.

A3 – Inyección

- ▶ **Exploit**
 - El atacante envía mensajes con cadenas de texto, las cuales explotan la sintaxis del interprete.
- ▶ **Vulnerabilidad**
 - Ocurre cuando una aplicación envía información no confiable a un interprete.
 - Ejemplos: SQL, NoSQL, LDAP, entre otros.
- ▶ **Impacto**
 - Puede causar denegación de servicio, pérdida o modificación de datos. En ciertos casos puede causar el compromiso total.
- ▶ **¿Cómo prevenirlo?**
 - Utilizar una API segura que provea una interfaz parametrizada.
 - Validar los valores de entrada usando listas de entrada o whitelist.
 - Realizar revisiones de código fuente.
 - Implementar SAST, DAST, IAST para detectar fallas antes de desplegar a producción.

A3 – Inyección (Ejemplo)

► Escenario

- La aplicación usa datos no confiables en la construcción de la siguiente instrucción SQL vulnerable:
 - `String query = "SELECT * FROM accounts WHERE custID=" + request.getParameter("id") + "";`

► Ataque

- El atacante modificar el parámetro 'id' en su navegador para enviar:
 - `2' or '1'='1`
- Ejemplo:
 - `http://example.com/app/accountView?id=2'or'1'='1`
- La consulta quedaría:
 - `SELECT * FROM accounts WHERE custID='2' or '1'='1';`

A4 – Diseño Inseguro

► Exploit

- Los atacantes podrían ingresar de forma no autorizada a los sistemas, adquirir productos o descuentos desmesurados, o usar bots sin ningún tipo de restricciones, entre otros.

► Vulnerabilidad

- La falta, ineficiencia o inexistencia de controles en el diseño de los sistemas debido a la falta de consideración de los riesgos inherentes asociados al sistema no permite implementar controles claves.

► Impacto

- Accesos no autorizados, pérdida de dinero, imposibilidad de realizar transacciones.

► ¿Cómo prevenirlo?

- Diseño seguro (threat modeling, historias de usuario).
- Ciclo de desarrollo seguro (patrones de diseño, modelos de madurez).
- Test unitarios e integrales.
- Limitar consumo de recursos por un usuario o servicio.

A5 – Configuración de Seguridad Incorrecta



- ▶ **Exploit**
 - Un atacante accede a cuentas por defecto, páginas sin uso, fallas sin parchear, archivos y directorios sin protección, etc., con el fin de obtener acceso no autorizado o conocimiento del sistema.
- ▶ **Vulnerabilidades**
 - Las configuraciones de seguridad incorrectas pueden ocurrir a cualquier nivel de la aplicación.
- ▶ **Impacto**
 - Estas vulnerabilidades frecuentemente dan a los atacantes acceso no autorizado a algunas funciones o datos del sistema. Ocasionalmente provocan que el sistema se pueda comprometer completamente.
- ▶ **¿Cómo prevenirlo?**
 - Arquitectura fuerte de los sistemas y seguridad en capas.
 - Hardening.

A6 – Componentes Vulnerables y Desactualizados



- ▶ **Exploit**
 - El atacante identifica un componente débil a través de escaneos automáticos o análisis manuales. Ajusta el exploit como lo necesita y ejecuta el ataque.
- ▶ **Vulnerabilidades**
 - En general, los equipos de desarrollo no se preocupan que sus componentes o bibliotecas estén actualizados, exponiéndose a vulnerabilidades.
- ▶ **Impacto**
 - El impacto varia en función de la vulnerabilidad que se encuentra en el componente o biblioteca desactualizada.
- ▶ **¿Cómo prevenirlo?**
 - Identificar todos los componentes y versiones, revisar su seguridad, establecer políticas para el uso de componentes y agregar capas de Seguridad.

A7 – Fallas de Identificación y Autenticación



- ▶ **Exploit**
 - El atacante utiliza filtraciones o vulnerabilidades en las funciones de autenticación o gestión de sesiones para suplantar otros usuarios.
- ▶ **Vulnerabilidades**
 - Los desarrolladores a menudo crean esquemas propios de autenticación o gestión de sesiones. Pueden contener vulnerabilidades de cierre de sesión, gestión de contraseñas, tiempo de desconexión, preguntas secretas, entre otros.
- ▶ **Impacto**
 - Las vulnerabilidades pueden permitir que una o todas las cuentas sean atacadas. El atacante podría hacer cualquier acción que la víctima este autorizado a hacer.
- ▶ **Como prevenirlo?**
 - Autenticación fuerte o utilizar frameworks confiables.



A7 – Fallas de Identificación y Autenticación (Ejemplo)

► Escenario

- Aplicación de reserva de vuelos que soporta reescritura de URL poniendo los ID de sesión en la propia dirección:
- `http://example.com/sale/saleitems;jsessionid=2P0OC2JDPXM0OQSNDLPSKHCJUN2JV?dest=Hawaii`

► Ataque

- Un atacante podría utilizar cualquier técnica de man-in-the-middle para poder utilizar esa sesión y obtener los datos de tarjetas de crédito ingresadas.

A8 – Fallas en el Software y en la Integridad de los Datos



- ▶ **Exploit**
 - Un atacante se aprovecha de la falta de controles que tiene el código y lo modifica según sus necesidades.
- ▶ **Vulnerabilidad**
 - El código no está protegido contra alteraciones, afectando su integridad.
- ▶ **Impacto**
 - Acceso no autorizado, inclusión de código malicioso, compromiso del sistema.
- ▶ **¿Cómo prevenirlo?**
 - Verificar la integridad de cada descarga antes de su instalación.
 - Usar firmas digitales.
 - Asegurarse de que las bibliotecas y dependencias (npm, Maven) son usadas desde repositorios confiables.
 - Usar herramientas de análisis.
 - Revisión de código.

A9 – Fallas en el Registro y Monitoreo



- ▶ **Exploit**
 - Los atacantes dependen de la falta de monitoreo y de la respuesta oportuna para lograr sus objetivos sin ser detectados.
- ▶ **Vulnerabilidad**
 - La debilidad se encuentra en la falta de logs y monitoreo de los servidores críticos de la organización.
- ▶ **Impacto**
 - Este puede ser el inicio de las pruebas sobre otros ataques posibles haciendo investigación de las vulnerabilidades que tiene el o los servidores en cuestión.
- ▶ **¿Cómo prevenirlo?**
 - Asegúrese de que todos los inicios de sesión, las fallas de control de acceso y las fallas de validación de entrada del lado del servidor puedan registrarse con un contexto de usuario suficiente para identificar las cuentas sospechosas o maliciosas, y conservarlas durante el tiempo suficiente para permitir el análisis forense.

A10 – Falsificación de Solicitudes del Lado del Servidor (SSRF)



- ▶ **Exploit**
 - Envío de solicitudes falsificadas a un destino inesperado.
- ▶ **Vulnerabilidades**
 - El atacante tiene acceso parcial o total de las consultas enviadas por una aplicación.
- ▶ **Impacto**
 - Exposición de datos sensibles, acceso a almacenamiento de metadatos de los servicios en la nube, escaneo de servidores internos para generar un mapa de la red interna, entre otros.
- ▶ **¿Cómo prevenirlo?**
 - Defensa en profundidad (Defensa por capas).

PREGUNTAS?

