DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Actividad formativa: Análisis de riesgos cualitativo y modelamiento de amenazas

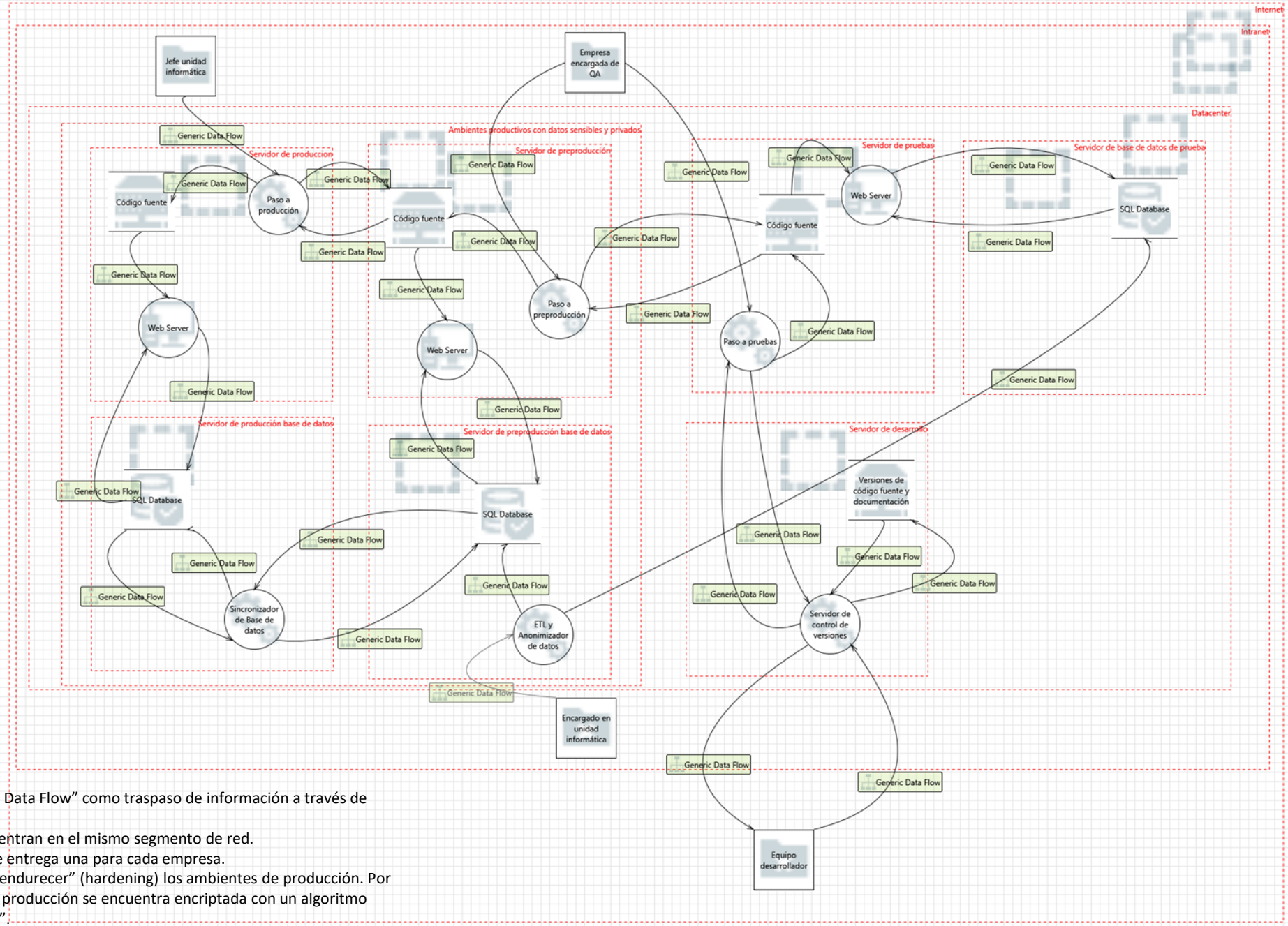
Fundamentos de ciberseguridad

Profesor

Juan Ignacio Iturbe A.

Situación actual

- Escenario:
  - La unidad informática de la empresa farmacéutica “NoEtix” debe desarrollar varios proyectos relacionados a la clasificación de sus clientes en sus hábitos de consumo, para así hacer campañas para ofrecer productos personalizados.
  - Se decide la utilización de los datos recogidos por el programa de puntos de las farmacias y supermercados del holding con más de 15 años en registros de personas identificadas por su rut.
  - Se observa que al interior de la empresa no existe personal con las capacidades para desarrollar dichos proyectos y tampoco para probarlos a fondo (QA). Por lo que se requiere subcontratar estos servicios a varias empresas especializadas.
  - La problemática radica en que se manejan varios datos personales y sensibles de los clientes, por lo que se siente temor por parte de la gerencia de que estos se filtren.
  - Dado lo anterior, el jefe de la unidad informática de la farmacéutica propone una arquitectura como la que se aprecia en la siguiente Figura para el desarrollo de los nuevos proyectos.
  - En esta se aprecia una separación de ambientes de desarrollo, pruebas, preproducción y producción.
  - Además se observan varios controles. Por ejemplo, el sistema de control de versiones, la réplica de la base de datos, personal encargado de QA, etc.
  - Después de una reunión con la Gerencia, se llegó a la conclusión de aceptar dicha propuesta. Sin embargo, para estar seguros de la arquitectura, se solicita un análisis de sus riesgos. Con este fin, se establecen tablas de impactos y probabilidad para el desarrollo de un análisis cualitativo (diapositiva 6, 7 y 8).



Notas:

- Considere los flujos “Generic Data Flow” como traspaso de información a través de protocolo HTTP.
- Todos los servidores se encuentran en el mismo segmento de red.
- Las credenciales de acceso se entrega una para cada empresa.
- Hay gran preocupación por “endurecer” (hardening) los ambientes de producción. Por ejemplo, la base de datos de producción se encuentra encriptada con un algoritmo propio por lo es “mas segura”.

Desarrollo de la actividad

- Identifique los activos propuestos, valorícelos y priorice.
- Identifiquen vulnerabilidades y amenazas sobre los 3 activos de mayor valor. Apoyarse en las diapositivas 9 y 10.
- Enfóquese en el activo de mayor valor.
- Calcule el riesgo inherente (Probabilidad x Impacto)
- Identifique controles mitigantes en el enunciado (deben ser controles implementados actualmente).
- Calcule el riesgo residual (Probabilidad x Impacto considerando los controles mitigantes)
- Priorice el listado de acuerdo al riesgo residual.
- Proponga controles adicionales para alcanzar el apetito de riesgo para la amenaza con mayor prioridad (Utilice CIS Controls). Puede también modificar o eliminar controles actuales.
- Suponga un apetito de riesgo igual o mayor a “Alto” (Se deben analizar al menos 3 riesgos).
- Desarrolle nuevamente el análisis de riesgos incluyendo los nuevos controles.

Se requiere…

- Completar la planilla compartida (utilizar la hoja correspondiente a su grupo).
- Explicite los supuestos que se requieran.

CATEGORÍAS DE PROBABILIDAD		
Categoría	**Valor**	
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente en el año en curso. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente en el año en curso.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente en el año en curso.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente en el año en curso.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente en el año en curso.

CATEGORÍAS DE IMPACTO		
Categoría	**Valor**	**Descripción**
Catastróficas	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren en el año en curso.
Mayores	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal en el año en curso.
Moderadas	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal en el año en curso.
Menores	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos en el año en curso.
Insignificantes	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos en el año en curso.

NIVEL DE RIESGO						
		Impacto				
		Catastrófico	Mayores	Moderado	Menor	Insignificante
Probabilidad	Casi certeza	Extremo	Extremo	Extremo	Alto	Alto
	Probable	Extremo	Extremo	Alto	Alto	Moderado
	Moderada	Extremo	Extremo	Alto	Moderado	Bajo
	Improbable	Extremo	Alto	Moderado	Bajo	Bajo
	Muy improbable	Alto	Alto	Moderado	Bajo	Bajo

Amenazas a la Privacidad

- Su sistema reutiliza los datos personales recopilados para un propósito específico para otro propósito no compatible.
- Su sistema está procesando datos personales de una manera que no se describe en el aviso de privacidad.
- Su sistema está procesando datos personales en países o con terceros que tienen estándares de privacidad débiles.
- Su sistema no implementa el borrado o la anonimización de los datos personales una vez que se ha retirado la base legal para el procesamiento.
- El equipo de su producto evita los controles necesarios para los datos personales, ya que los mueve fuera de los entornos regulados y endurecidos.
- Su sistema está recopilando datos personales sin poder nombrar el propósito específico, explícito y legítimo para el que se utiliza.
- Su sistema no está siguiendo la eliminación de datos personales en terceros integrados
- Su sistema recopila más datos personales que los estrictamente necesarios para cumplir con el propósito previsto.
- A los datos personales de su sistema les faltan punteros a los propietarios de los datos, por lo que los datos se olvidan (o quedan almacenados sin referencia) cuando el propietario se elimina o realiza una solicitud de acceso.
- Su sistema recopila el consentimiento pero no documenta aspectos sobre cómo, cuándo y qué consentimiento se proporcionó.
- Su sistema no puede manejar adecuadamente el retiro del consentimiento o la objeción al procesamiento
- Su sistema no se entrega de forma predeterminada con configuraciones optimizadas y amigables con la privacidad.

Amenazas sobre divulgación de información

- Un atacante puede realizar fuerza bruta sobre archivos cifrados porque no hay ninguna defensa en su lugar (por ejemplo: *password stretching*).
- Un atacante puede ver los mensajes de error con contenido sensible a la seguridad.
- Un atacante puede leer el contenido porque los mensajes (por ejemplo, un correo electrónico o una cookie HTTP) no están cifrados incluso si el canal está cifrado.
- Un atacante puede leer un documento o datos porque está cifrado con un algoritmo no estándar.
- Un atacante puede leer datos porque está oculto u ocluido (para deshacer o cambiar el seguimiento) y el usuario podría olvidar que está allí.
- Un atacante puede actuar como un "hombre en el medio" porque no se autentican los puntos finales de una conexión de red.
- Un atacante puede acceder a la información a través de un indexador de búsqueda, registrador u otro mecanismo similar.
- Un atacante puede leer información confidencial en un archivo con ACL incorrectas.
- Un atacante puede leer información en archivos sin ACL.
- Un atacante puede descubrir la clave fija que se utiliza para cifrar.
- Un atacante puede leer todo el canal porque el canal (por ejemplo, HTTP o SMTP) no está cifrado.
- Un atacante puede leer la información de la red porque no se usa criptografía.

Otras fuentes de amenazas

- STRIDE
- MAGERIT libro II – Catalogo de elementos
- ENISA Threat Taxonomy

- Investigar otras

Ejemplo

Nº Riesgo	Riesgo		Activo Involucrado	Riesgo inherente			Controles Mitigantes	Riesgo residual		
	Amenaza	Vulnerabilidad		I	P			I	P	
R1	Accesos no autorizados a la Red	Inexistencia procedimientos tareas de monitoreo de la Red	Red Productiva	5	5	Extremo	1- Posee un área de Gestión de Incidentes, la cual registra, comunica, clasifica y analiza todas las llamadas e incidentes reportados relacionados con la seguridad de la información 2- Se realizan tareas de monitoreo a los distintos aplicaciones críticas, bases de datos, alertas y vulnerabilidades para detectar incidentes de seguridad de la información 3- Se cuenta con herramientas que permiten, a través del uso de logs, visualizar eventos sospechosos, estos a nivel de sistema de resguardo de plataformas, de Red, a los Firewalls y a IDS IPS. La responsabilidad de realizar dicha información se encuentra definida e incorporada dentro de la descripción de cargo. 4- Posee responsabilidades y procedimientos de Gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información	2	1	Bajo

En este caso el riesgo residual, es menor al apetito de riesgo. En caso contrario se deberían considerar mas controles

Comentarios sobre la actividad

- ¿Qué incluiría en la actividad?
- ¿Qué sacaría de la actividad?
- ¿Algún otro comentario?