Que es la seguridad de la información

Para comprender la seguridad de software

IDTS 2020

Que no es seguridad de la información

Proteger los servicios o software ante atacantes **encapuchados**, para evitar el hacking.

Existe la creencia que la seguridad es a nivel nube únicamente y las activdades que hace otro **encapuchado** para evitar ataques de externos.

Por que es importante la SI

- ¿Que sucede si me secuestran mi base de datos?.. Se compromete mi información
- ¿Que sucede si logran insertar scripts maliciosas a mi software?.. Es muy probable que modifiquen mi información
- ¿Que sucede si mi servicio no se encuentra disponible?... Clientes molestos, pérdida monetaria y pérdida de información por el tiempo en el que mi servicio se encuentra en un estado de “No disponible”.
- ¿Que sucede si un atacante vive en mi sistema sin conocerlo? .. Tendrá disponibilidad de mi información.

¿Cual es el factor común?

La información, por lo tanto debemos de garantizar que la misma cumpla con:
Disponibilidad, Integridad y Confidencialidad

¿Y como lograrlo?

Mediante la implementación de un SGSI

¿Que es un SGSI?

SGSI (Sistema de Gestión de la Seguridad de la Información) es un conjunto de políticas, procedimientos, guías, recursos y actividades asociadas, que son gestionadas de manera colectiva en una organización.

Para lograrlo, debemos basarlo en una apreciación del riesgo y determinar los niveles de aceptación del mismo para diseñar, implementar, monitorear y mejorar la eficacia de los riesgos.

En resumen minimizar el riesgo de la falla de un activo tecnológico

Seguridad de la información = Ingeniería de software = Calidad de Software = Calidad de servicio

¿Que es el riesgo?

El riesgo operativo es la posibilidad de ocurrencia de pérdidas financieras, originadas por fallas o insuficiencias de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos.

¿Como lo calculamos?

		CLASIFICACIÓN DE RIESGOS		
IMPACTO	***ALTO***	MEDIO	ALTO	CRÍTICO
	MEDIO	BAJO	MEDIO	ALTO
	BAJO	BAJO	BAJO	MEDIO
		BAJA	***MEDIA***	***ALTA***
		PROBABILIDAD		

Se recomienda de 5 niveles

VALORACIÓN RIESGO ABSOLUTO INSTITUCIONAL							
Probabilidad	Muy Alta	5	Moderado 10	Alto 20	Alto 30	Crítico 40	Crítico 50
	Alta	4	Bajo 8	Moderado 16	Alto 24	Crítico 32	Crítico 40
	Media	3	Bajo 6	Moderado 12	Alto 18	Alto 24	Alto 30
	Baja	2	Bajo 4	Bajo 8	Moderado 12	Moderado 16	Alto 20
	Muy Baja	1	Bajo 2	Bajo 4	Bajo 6	Bajo 8	Moderado 10
				4	6	8	10
			Mínimas	Leves	Moderadas	Graves	Catastróficas
			Consecuencia o Impacto				

¿Y por donde comienzo?

Recomendaciones

- Usar framework’s.
- Establecer branches y una correcta nomenclatura de versiones
- Realizar pruebas en alpha, beta.
- Realizar pruebas de penetración en R.C.
- Uso de contendores.
- Establecer procesos para el mantenimiento y actualizaciones en la nube.
- Tener ambientes de desarrollo, pruebas y producción separados.
- En resumen un proceso SDLC.

Que seguir

- Owasp 10 top- https://owasp.org/www-project-top-ten/
- NIST - https://www.nist.gov/cybersecurity
- CIS - https://www.cisecurity.org/
- ISO - https://iso27001security.com/

SIEM

Security information and event management (SIEM), es un conjunto de herramientas y servicios que combinan la gestión de eventos de seguridad y las capacidades de gestión de la información de seguridad para permitir a los analistas revisar los datos de registros de eventos para comprender y prepararse para las amenazas.

El objetivo es detectar los **Eventos de Seguridad**, para impedir que se materialicen en **Incidentes de Seguridad**.