Mitigar riesgos de Ciberseguridad

by Miguel Solinas

Departamento de Computación

Julio XX22

Mitigar riesgos de ciberseguridad

De acuerdo a la RAE, **mitigar** del latín *mitigāre*.

1. tr. Moderar, aplacar, disminuir o suavizar algo riguroso o áspero.

Mitigar riesgos de ciberseguridad

De acuerdo a la RAE, **mitigar** del latín *mitigāre*.

1. tr. Moderar, aplacar, disminuir o suavizar algo riguroso o áspero.

Contexto

- **Seguridad absoluta** No existe...
- **Presupesto** Como en todas partes, limitado...
- **Negocio** No es la seguridad, salvo que seamos una AC.!!
- **Riesgos** Minimizarlos dentro del presupesto...

Mitigar riesgos de ciberseguridad

Propuestas

- **Auditorías de seguridad** Es fundamental tener un diagnóstico inicial para enforcarnos en el 20% de las causas que generan el 80 % de los problemas.

Mitigar riesgos de ciberseguridad

Propuestas

- **Auditorías de seguridad** Es fundamental tener un diagnóstico inicial para enforcarnos en el 20% de las causas que generan el 80 % de los problemas.
- **Políticas y buenas prácticas** Una buena forma de empezar a ordenar la complejidad e involucrar a todos.

Mitigar riesgos de ciberseguridad

Propuestas

- **Auditorías de seguridad** Es fundamental tener un diagnóstico inicial para enforcarnos en el 20% de las causas que generan el 80 % de los problemas.
- **Políticas y buenas prácticas** Una buena forma de empezar a ordenar la complejidad e involucrar a todos.
- **Personas** Una de las caras del cubo de destrezas. TODOS deben comprometerse con la seguridad. Recuerdan el asunto de "calidad"..?

Mitigar riesgos de ciberseguridad

Propuestas

- **Auditorías de seguridad** Es fundamental tener un diagnóstico inicial para enforcarnos en el 20% de las causas que generan el 80 % de los problemas.
- **Políticas y buenas prácticas** Una buena forma de empezar a ordenar la complejidad e involucrar a todos.
- **Personas** Una de las caras del cubo de destrezas. TODOS deben comprometerse con la seguridad. Recuerdan el asunto de "calidad"..?
- **Monitorear** Una vez que tengamos un SGSI/aproximación en marcha, debemos monitorear eventos en tiempo real.

Auditorías de seguridad

¿ De qué se trata ?

- Vulnerability assesment, Penetration test, Ethical hacking. ¿ Son todos la misma cosa ?

Auditorías de seguridad

¿ De qué se trata ?

- Vulnerability assesment, Penetration test, Ethical hacking. ¿ Son todos la misma cosa ?
- Todo en un marco de un estricto acuerdo de confidencialidad.
- No es lo mimo un banco que una organización gubernamental o una pyme.

Auditorías de seguridad

¿ De qué se trata ?

- Vulnerability assesment, Penetration test, Ethical hacking. ¿ Son todos la misma cosa ?
- Todo en un marco de un estricto acuerdo de confidencialidad.
- No es lo mimo un banco que una organización gubernamental o una pyme.
- Existen varias metodologías, una de ellas es la desarrollada por el *Institute for Security and Open Methodologies* **(ISECOM)** denominada *Open Source Security Test Methodology* **(OSSTM)**.

Oper Source Security Test Methodology

Una auditoria interna, tipo whitebox, realizada por un tercero con acceso físico a la empresa puede ser una buena opción.

Oper Source Security Test Methodology

Una auditoria interna, tipo whitebox, realizada por un tercero con acceso físico a la empresa puede ser una buena opción.

Conceptos

- **Posicionamiento** Interno o externo
- **Visibilidad** Blind/Blackbox, Double blind/Blackbox, Graybox, Double Graybox, Whitebox, Reversal
- **Perfil adoptado** Usuario sin privilegios, Usuario con privilegios, Tercero ajeno a la organización con acceso físico a la misma, sin acceso físico a la misma, Usuario con conocimiento técnico avanzado, intermedio o básico, otros...

Obtendremos un mismo informe con destino a tres públicos objetivos: Dirección, Gerencia y personal Técnico.

Políticas de seguridad

¿ Por qué hacerlo ?

- Mostrar el compromiso de una organización con la seguridad.
- Establecer reglas para el comportamiento esperado.
- Garantizar la coherencia en las operaciones del sistema, la adquisición y uso de software y hardware, y su mantenimiento.
- Definir las consecuencias legales de las violaciones.
- Brindar al personal de seguridad el respaldo de la máxima autoridad.

Políticas de seguridad continuación

La industria automotriz de Córdoba de los '90 exigió niveles de primera categoría para la calidad de producto, la productividad, la competitividad y la mejora continua. ¿ Quien no escuchó hablar de ISO 9001 ?

Algunas fuentes de información

- ISO/IEC 27000/1 2018/2013.
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC).
- National Security Agency (NSA) Cybersecurity Advisories and Guidance.
- En INCIBE recomiendo buscar en la playlist SGSI

Políticas de seguridad continuación

Es relevante lo que dice la European Union Agency for Cybersecurity (ENISA)

Políticas en materia de ciberseguridad

La ciberseguridad es la **piedra angular de la transformación digital** y su necesidad es transversal a todos los sectores, por lo que resulta necesario tenerla en consideración en una amplia serie de iniciativas y ámbitos políticos. La ciberseguridad no debe limitarse a una comunidad especializada de expertos técnicos en cibernética. La ciberseguridad debe estar integrada en todos los ámbitos de las políticas de la UE. Es por tanto esencial evitar la fragmentación y contar con un enfoque coherente teniendo en cuenta al mismo tiempo las características específicas de cada sector.

Políticas de seguridad y buenas prácticas

Navegemos el sitio de INCIBE, busquemos estos videos cortos de su playlist en youtube, los ecuchemos y compartamos preguntas.!!

Protege tu empresa

- ¿ Cómo identificar una fuga de información ?
- ¿ Qué vas a hacer con mis datos ?
- Kit de concienciación para empresas
- Políticas de seguridad para las pyme
- Incidente de seguriad en pymes
- Backup: la primera línea de defensa
- Proteger y usar de forma segura los dispositivos móviles

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos
- No existen carreras de grado específicas en universidades públicas ¿ algunas en el ámbito privado ?

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos
- No existen carreras de grado específicas en universidades públicas ¿ algunas en el ámbito privado ?
- Muy pocas carreras de grado abordan la temática

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos
- No existen carreras de grado específicas en universidades públicas ¿ algunas en el ámbito privado ?
- Muy pocas carreras de grado abordan la temática
- Las carreras de posgrado son actualizaciones ¿ o parches ?

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos
- No existen carreras de grado específicas en universidades públicas ¿ algunas en el ámbito privado ?
- Muy pocas carreras de grado abordan la temática
- Las carreras de posgrado son actualizaciones ¿ o parches ?
- Cerficiaciones de la industria.., muchos u$s !!

Personal

Hay un escenario similar al observado al principio de los '80 con la informática / sistemas.!!

¿ Cuál es el contexto ?

- Excases de profesionales y abundancia de idóneos
- No existen carreras de grado específicas en universidades públicas ¿ algunas en el ámbito privado ?
- Muy pocas carreras de grado abordan la temática
- Las carreras de posgrado son actualizaciones ¿ o parches ?
- Cerficiaciones de la industria.., muchos u$s !!
- Debemos empezar por capacitar a NUESTRO PERSONAL.!!

Monitorear eventos

Nuestra Unidad Académica cuenta con un Laboratorio de Redes y Ciberseguridad **(LARYC)** donde hemos desarrollado capacidades propias:

Proyectos integradores

- **Implementación de una solución para gestión de eventos de seguridad de una red de datos**; Figueroa S., Sepulveda F., Solinas M.; 2021.
- **Sistema de detección de intrusiones utilizando técnicas de machine learning**; Rébola C., Vázquez F., Solinas M.; 2021.
- **Detección y Evaluación de Alertas de Seguridad en Redes de Datos**; Sleiman M., Aagaard M., Solinas M.; 2022.
- **Detección de botnets en redes segmentadas**; Miranda R., Wortley A., Solinas M.; 2022.
- Otros...

Muchas gracias..!!