ADMINISTRACIÓN DE RECURSOS
Unidad 2: Seguridad de la Información y Auditoría
Seguridad de la Información

Anexo II: FAIR – Factor Analisys Information Risk[1]

Factores para evaluar la magnitud de pérdida

FAIR establece cuatro componentes principales para evaluar la **magnitud de la pérdida**: activos y amenazas, que considera factores primarios de pérdida, y factores referidos a la organización y al ambiente externo que considera factores secundarios de pérdida.

Activos: Si bien las dimensiones establecidas anteriormente permiten establecer el nivel de criticidad, FAIR agrega algunos elementos que permiten mejorar esta valuación. Estos son:

- ✓ **Productividad**: característica de un activo que tiene que ver con el impacto en la productividad de una organización. Por ejemplo, el impacto que una base de datos dañada tendría en la capacidad de la organización para generar ingresos
- ✓ **Costo de reemplazo**: Los costos asociados con el reemplazo de un activo que ha sido robado o destruido. Por ejemplo, incluyen el costo de reemplazar una computadora portátil robada o reconstruir un edificio incendiado.
- ✓ **Sensibilidad**: el impacto resultante de la divulgación o uso indebido de información confidencial. En algunos casos representa un valor económico, en otros representa confiabilidad.
  - **Reputación:** La información divulgada proporciona evidencia de incompetencia, actuación criminal o poco ética. Refiere al daño de la reputación resultante de la naturaleza de la información divulgada a diferencia del daño de reputación que puede resultar cuando ocurre un evento de pérdida.
  - **Ventaja competitiva**: la información proporciona una ventaja competitiva (por ejemplo, estrategias clave, secretos, etc.).
  - **Legal / Regulatoria:** la organización está obligada por ley a proteger la información
  - **General**: información sensible que no se encuentra en ninguna de las categorías anteriores, pero daría como resultado alguna forma de pérdida si se revela
- ✓ **Volumen:** simplemente reconoce que más activos en riesgo equivalen a una mayor magnitud de pérdida si ocurre un evento - por ejemplo un registro de cliente sensible versus miles.

Amenazas son cualquier cosa (por ejemplo, objeto, sustancia, ser humano, plaga, etc.) que sea capaz de actuar contra un activo de manera que pueda resultar en daño. La consideración clave es que las amenazas aplican la fuerza contra un activo que puede causar que se produzca un evento de pérdida. Prácticamente cualquiera y cualquier cosa puede, en las circunstancias adecuadas, ser un agente de amenaza: el bien intencionado operador, pero inepto, que destruye un trabajo por lotes diario, un contador realizando una auditoría, un hacker que ejecuta un exploit tanto para lograr acceso

[1] Resumen y Traducción del original: An Introduction to Factor Analysis of Information Risk (FAIR) Disponible en: https://theartofservicelab.s3.amazonaws.com/All%20Toolkits/The%20Information%20risk%20management%20Toolkit/Act%20-%20Recommended%20Reading/Risk%20Management%20Insight.pdf

a un sistema como para tomar control del mismo, el agua en una inundación, el viento en un tornado o un roedor que mastica un cable de datos. De las amenazas es conveniente considerar:

- ✓ **Competencia:** son las capacidades que tiene el atacante de utilizar la información una vez conseguida. Por ejemplo: un hacker puede hacerse del código de un programa, sin embargo, puede tener las competencias necesarias para utilizarlo.
- ✓ **Internas/Externas:** se refiere a la identificación de las comunidades de amenaza. Esta es una herramienta para entender a quién y a qué nos enfrentamos cuando intentamos gestionar el riesgo. Internas pueden ser empleados, contratistas, socios, externas: ciberdelincuentes (hackers profesionales), espías de la competencia, hackers no profesionales.
- ✓ **Acción:**
  - **Acceso**: simplemente acceso no autorizado
  - **Uso indebido**: uso no autorizado de activos (por ejemplo, robo de identidad, configuración de un servicio de distribución de pornografía en un servidor comprometido, etc.)
  - **Divulgación**: el agente de amenaza revela ilícitamente información sensible
  - **Modificación**: cambios no autorizados en un activo
  - **Denegación de acceso**: incluye destrucción, robo de un activo que no es de datos, etc.

Organización: El riesgo existe dentro del contexto de una organización o entidad. Es la organización que pierde recursos o la capacidad de operar. Las características de la organización también pueden servir para atraer la atención de ciertas comunidades de amenazas, que pueden aumentar la frecuencia de los eventos.

- ✓ **Momento**: el momento en que tiene lugar un evento puede tener un tremendo impacto en la pérdida. Por ejemplo, un evento que ocurre en medio de un gran la campaña publicitaria puede generar una pérdida significativamente mayor que un evento similar en algún otro momento.
- ✓ **Debido cuidado:** puede jugar un papel importante en el grado de responsabilidad que una organización enfrenta ante un evento. Si no se han tomado las medidas preventivas del caso (en función de la amenaza y el valor del activo) el daño puede ser mucho más severo. A menudo, los estándares de la industria o las "buenas prácticas" teóricas se consideran pautas para el debido cuidado y estas pautas generalmente no consideran el entorno de amenaza o la magnitud de la pérdida. En consecuencia, pueden ser insuficientes (es decir, no son verdaderamente representativas del debido cuidado) o excesivamente conservadoras (es decir, prohibitivamente caras dado el riesgo inherente).
- ✓ **Detección:** No se puede responder a algo que no ha detectado, es decir, la respuesta se basa en la detección. Claramente, ocurren incidentes que no aparecen en el radar. Sin embargo, también es razonable creer que tales eventos, si dan como resultado una pérdida material, casi siempre se detectarán con el tiempo. Por ejemplo, una información que ha sido robada y da ventaja a un competidor casi seguramente será reconocida. Si bien la detección puede no haber sido en el momento oportuno, una vez detectado el robo, la organización aún puede tener la oportunidad de responder y reducir sus pérdidas por ejemplo, con un acción legal. El punto es que casi

seguramente se detectará, y con la detección viene una oportunidad de responder y gestionar la magnitud de la pérdida

- ✓ **Respuesta:** Refiere a la eficiencia con que la organización responde a un evento. Tiene tres componentes cuya inexistencia puede tener un impacto significativo en la magnitud de pérdida. Tendemos a pensar en las capacidades de respuesta únicamente dentro del contexto de volver a brindar los servicios normalmente. Sin embargo, las capacidades de respuesta también se relacionan con la divulgación de información. Por ejemplo, una organización que experimenta la divulgación pública datos de sus clientes puede ser afectada en la reducción significativa de su cartera de clientes y probablemente deba compensar el perjuicio del cliente afectado.
  - **Contención**: tiene que ver con la capacidad de una organización de limitar la amplitud y la profundidad de un evento. Por ejemplo, la capacidad para contener la propagación de un gusano.
  - **Remediación**: refiere a la capacidad de eliminar el agente amenazante, por ejemplo, erradicar el gusano
  - **Recuperación**: refiere a la capacidad de devolver las cosas a la normalidad.

Factores externos: El entorno en el que opera una organización juega un papel importante en el riesgo. Los factores externos afectan la magnitud de pérdida cuando el evento es detectado por una entidad externa.

- ✓ **Detección**: La detección externa de un evento puede suceder como consecuencia de la gravedad del evento, debido a acciones intencionales del agente de amenaza, a través de divulgación por parte de alguien interno a la organización familiarizado con el evento, divulgación intencional por parte de la organización (ya sea por el sentido del deber, o porque es requerido por la ley), o por accidente. Los restantes factores estarán basados en el factor de detección.
- ✓ **Legal / Regulatorio**: se compone principalmente de tres partes: regulaciones (locales, provinciales, federales e internacionales), derecho contractual y jurisprudencia específica.
- ✓ **Competidores**: Las pérdidas asociadas con el panorama competitivo típicamente tienen que ver con la capacidad de la competencia para aprovechar la situación. Por ejemplo, si una organización experimenta un evento que hace que sus partes interesadas consideren abandonar la organización, la capacidad de un competidor para aprovechar esa debilidad afectará la cantidad de pérdidas que se produzcan.
- ✓ **Medios de comunicación**: La reacción de los medios puede tener un alto efecto sobre cómo las partes interesadas, los abogados e incluso los reguladores y los competidores ven el evento. Si los medios eligen difamar a la organización y mantenerla en los titulares durante un período prolongado, el resultado puede ser devastador. Por el contrario, si los medios pintan a la organización como una víctima bienintencionada que ejerció el debido cuidado pero aún sufrió el evento a manos de un criminal, entonces el daño legal y de reputación puede ser minimizado. Esta es la razón por las organizaciones deben tener procesos efectivos de comunicación de crisis.
- ✓ **Otros grupos de interés**: Otros grupos de interés que pueden haber detectado o que se consideren implicados en el riesgo (Ej. Organizaciones no gubernamentales)

ADMINISTRACIÓN DE RECURSOS
Unidad 2: Seguridad de la Información y Auditoría
Seguridad de la Información

Factores para evaluar la frecuencia de eventos de pérdida

FAIR establece como frecuencia de eventos de pérdida a la frecuencia probable, dentro de un rango de tiempo, que un agente de amenaza podrá causar daño sobre un activo.

A partir de esto establece dos factores: frecuencia de amenazas y vulnerabilidades.

Frecuencia de amenazas: frecuencia probable, dentro de un rango de tiempo, que un evento de amenaza podrá actuar sobre un activo.

- ✓ **Contacto**: la frecuencia probable, dentro de un rango de tiempo, que el agente de amenaza entrará en contacto con el activo. El contacto puede ser físico o lógico.
  - **Aleatorio**: el agente entra en contacto accidentalmente con el activo en el curso de una actividad no controlada
  - **Regular**: el agente de amenaza entra en contacto con el activo durante el curso de una actividad regular.
  - **Intencional**: el agente de amenaza busca entrar en contacto con el activo con objetivos específicos.
- ✓ **Acción**: Una vez que se produce el contacto entre un agente de amenaza y un activo, es posible que se produzca o no una acción contra el activo. Por algunos tipos de agente de amenaza, la acción siempre tiene lugar. Por ejemplo, si un tornado entra en contacto con una casa, la acción es una conclusión inevitable. La acción solo se cuestiona cuando hablamos de agentes de amenaza como los humanos y otros animales, y agentes de amenaza artificialmente inteligentes como programas maliciosos.
  - **Beneficio**: valor del activo desde el punto de vista del agente de amenaza
  - **Nivel de esfuerzo**: la expectativa del agente de amenaza de cuánto esfuerzo se necesitará para comprometer el activo
  - **Riesgo de detección**: la probabilidad de consecuencias negativas para el agente de amenaza, es decir, la probabilidad de ser atrapado y sufrir consecuencias inaceptables.

Vulnerabilidades: Refiere a la probabilidad de que un activo no sea capaz de resistir las acciones de un agente de amenaza. La vulnerabilidad siempre es relativa al tipo de fuerza involucrada. En otras palabras, la resistencia a la tracción de una cuerda solo es pertinente si la fuerza del agente de amenaza es un peso aplicado a lo largo de la cuerda. La resistencia a la tracción generalmente no se aplica a un escenario donde el agente de amenaza es fuego, erosión química, etc. Asimismo, un producto antivirus no proporciona protección en el caso de que un empleado busque perpetrar un fraude. La clave, entonces, es evaluar la vulnerabilidad en el contexto de tipos específicos de amenazas y tipos de control. La vulnerabilidad puede existir de tal manera que el daño puede ocurrir a partir de más de un agente de amenaza a través de más de un vector de ataque, pero cada uno de ellos representa un evento de amenaza potencial diferente. Por ejemplo, si estoy caminando por la calle de noche en una parte particularmente peligrosa de la ciudad, soy vulnerable a múltiples amenazas potenciales, por ejemplo, ser atropellado por un automóvil, ser asaltado o ser víctima de

un tiroteo. Mi vulnerabilidad a cualquiera de estos eventos no puede exceder el 100%, sin embargo, mi riesgo agregado es obviamente mayor como resultado de los múltiples escenarios de amenaza.

- ✓ **Capacidad de las amenazas**: El nivel probable de fuerza que un agente de amenaza puede aplicar contra un activo. No todos los agentes de amenaza tienen las mismas habilidades ni los mismos recursos. De hecho, dependiendo de la comunidad de amenaza bajo análisis y otras condiciones dentro del escenario, la probabilidad de encontrar un agente de amenaza altamente capaz puede ser remota. Como profesionales de la seguridad de la información, a menudo tendemos a enfocarnos en los posibles peores casos y no en la probabilidad de que cualquier caso posible suceda. Se debe considerar que algunos agentes de amenaza pueden ser muy hábiles en la aplicación de un tipo de fuerza, e incompetentes en otros. Por ejemplo, es probable que un ingeniero de redes sea competente en la aplicación de formas tecnológicas de ataque, pero puede ser relativamente incapaz de ejecutar un fraude contable complejo.
- ✓ **Capacidad de resistencia**(CR): La fortaleza de un control en comparación con una medida de referencia. Un ejemplo simple puede ser la fortaleza de una contraseña. Se puede estimar que una contraseña de ocho caracteres, compuesta de una combinación de letras mayúsculas y minúsculas, números y caracteres especiales resistirán los intentos de craqueo de algún porcentaje general de la población de agentes de amenaza. La fuerza de control de contraseñas (CR) se puede representar con un porcentaje. La vulnerabilidad se puede determinar comparando CR con la capacidad de la comunidad específica de amenaza específica bajo estudio. Supongamos que el porcentaje de la capacidad de resistencia de una contraseña se puede estimar en un 80%, pero la comunidad de amenazas dentro de un escenario tiene capacidades mejores que el promedio, digamos en el rango del 90%. La diferencia representa la vulnerabilidad.