ANÁLISIS DE RIESGOS

ING. FREDY BUSTAMANTE

ANÁLISIS DE RIESGOS

- El análisis de riesgos se debe realizar para poder tomar en cuenta la forma única en que su empresa manejará las posibles amenazas y su riesgo asociado tomando en cuenta factores como localización, tipo de industria, cultura organizacional, estructura organizacional, objetivos estratégicos, entre otros.
- El análisis de riesgos en TI puede respaldar una variedad de actividades de gestión de riesgos en toda la empresa que incluyen:
  - Desarrollo de una arquitectura de infraestructura de TI
  - Desarrollo de una arquitectura de seguridad de TI
  - Definición de requisitos de interfaz para funciones de TI
  - Implementación y mantenimiento de soluciones de seguridad
- No podemos crear un plan de BC/DR hasta que sepamos las amenazas específicas que enfrenta la empresa.

ANÁLISIS DE RIESGOS

- Una de las objeciones comunes hacia la planificación de BC/DR es que hay **demasiadas cosas que pueden salir mal** que no se puede planificar para todas ellas.
- Esto es parcialmente correcto pues es cierto que hay demasiadas cosas que pueden salir mal pero un número reducido de ellas tienen una **opción real de suceder.**
- Se debe crear el plan para lo que tiene una opción real de suceder.
- Esto sin dejar de revisar aquello que no parece tener una opción real de suceder pero que el **impacto** puede ser muy grande.

ANÁLISIS DE RIESGOS

- Por ejemplo, todos los días salimos a la calle en nuestro vehículo, lo que significa tener riesgo de un accidente de tránsito, la única forma de bajar a 0 la posibilidad de que nos ocurra es no salir, pero esto no es viable por lo que tomamos acciones para mitigarlo como tomar clases de manejo y obedecer las leyes de tránsito, además, podemos adquirir un seguro de automóvil para transferir el riesgo de costos altos por reparaciones u hospitalizaciones.
- Aun así, seguimos estando en riesgo de sufrir un accidente y tener costos asociados a ello, pero estamos dispuestos a correr dicho riesgo.
- Esto es un ejemplo de **evitar, reducir, aceptar y transferir el riesgo.**

GESTIÓN DEL RIESGO

- La gestión de riesgos debe ajustarse a las limitaciones financieras de la empresa para que sea viable, en otras palabras, debe ser **razonable**.
- Es un tema **general** que analiza cómo se gestionan todos los riesgos en **toda la empresa**.
- Tres aspectos clave en el proceso de gestión de riesgos:
  - Análisis de riesgos: ¿cómo se realizará la evaluación?
  - Enfoque de evaluación: ¿optará por un enfoque cuantitativo, cualitativo o semicualitativo?
  - Enfoque de análisis: ¿Quiere analizar su riesgo desde una orientación de amenaza, una orientación activo-impacto o una orientación de vulnerabilidad? Puede utilizar cualquiera, pero mantener un método consistente es importante para realizar un buen plan.

GESTIÓN DEL RIESGO

- Cuatro pasos básicos en la gestión de riesgos:
  - Evaluación de amenazas
  - Evaluación de vulnerabilidades
  - Evaluación de impacto
  - Desarrollo de estrategias de mitigación de riesgos

- Nos centraremos en las primeras dos, pero no podemos dejar de mencionar la gestión del riesgo cuando hablamos del análisis de riesgos.

GESTIÓN DEL RIESGO

- Certificaciones: si es de su interés personal o para su empresa existen diferentes certificaciones para la gestión del riesgo como:
- **Certified in Risk and Information Systems Control from ISACA (ISACA CRISC).**

- Además, puede encontrar otras certificaciones no enfocadas en IT.

GESTIÓN DEL RIESGO

- Proceso de gestión del riesgo: Incluye evaluar el potencial y también analizar las compensaciones (trade-offs) o el costo de oportunidad.
  - Trade-offs: se refiere a que gastar en la mitigación de riesgos significa quitar presupuesto de otras actividades.
- Dos conceptos útiles son **magnitud y frecuencia**:
  - Por ejemplo, el impacto de un terremoto tendría una alta magnitud, sin embargo, en muchos lugares incluso algunos que son propensos a estos, la frecuencia es relativamente baja.

GESTIÓN DEL RIESGO

- Cada amenaza y posible estrategia de mitigación tienen un costo y un beneficio
  - Analizaremos los costos en cifras en alguna moneda, en vidas humanas y operaciones comerciales.
  - También existe el beneficio de la mitigación, que idealmente debería compensar con creces el costo del evento.
- Por ejemplo, supongamos que el costo de instalar un sistema de extinción de incendios en un edificio pueda ser de $15,000. Comparando este costo contra (1) daños al edificio, (2) daños a los equipos y mobiliario, (3) daños a los equipos de TI y (4) lesiones y vidas humanas, dichos $15,000 parecen una inversión excelente pues supondrá evitar un costo mucho mayor en caso de un incendio.

EVALUACIÓN DE AMENAZAS

- Hemos utilizado las palabras **riesgo y amenaza** en varias ocasiones, casi indistintamente. Esto, en un contexto general, es correcto, pero no del todo en un contexto de administración del riesgo.
- **Riesgo del negocio**: Proceso de **identificar, controlar** y **eliminar** o **minimizar** eventos inciertos que puedan afectar al negocio. Incluye análisis de riesgos, análisis de costos y beneficios, selección, implementación y prueba de estrategias seleccionadas y mantenimiento de estas a largo plazo.

EVALUACIÓN DE VULNERABILIDADES

- La evaluación de vulnerabilidades **analiza que tan vulnerable, susceptible y expuesto está un negocio o sistema a una amenaza particular.**
  - Debe incluir una evaluación de **qué tan vulnerable** es un sistema en particular a una amenaza, así como la **probabilidad de que esa amenaza ocurra**.
  - La parte de la probabilidad de ocurrencia puede ser una evaluación aparte, considero que es mejor realizarse en conjunto dado que están muy relacionadas pues no es lo mismo evaluar una vulnerabilidad a una amenaza con mucha probabilidad de ocurrencia que una vulnerabilidad a una amenaza con muy poca probabilidad.

EVALUACIÓN DEL IMPACTO

- La evaluación del impacto analiza **que tan grande o pequeño será el impacto de la ocurrencia de una amenaza** en el negocio o sistema.
- Por ejemplo, un terremoto tiene un enorme impacto sobre empresas que estén localizadas cerca del epicentro, tendrá menor impacto sobre aquellas que están más lejos del mismo sin olvidar la evaluación del impacto indirecto como proveedores clave que se encuentren cerca del epicentro o el colapso de infraestructura de comunicación, transporte y otros servicios.

DESARROLLO DE ESTRATEGIAS DE MITIGACIÓN DE RIESGOS

- Es el **proceso de decidir cuáles riesgos deberíamos abordar y de qué manera**.
- Los insumos para este proceso son el análisis de evaluación de riesgos o los informes que delinean qué amenazas existen, qué tan vulnerables son sus sistemas y qué probabilidad hay de que ocurra la amenaza, así como el impacto de estos en el negocio.
- Recordemos que podemos reducir, evitar, aceptar o transferir riesgos. En muchos casos, es mucho más costoso evitar completamente un riesgo que reducir su impacto.
- Por ejemplo, para evitar en su totalidad un incendio, podemos construir un edificio con material no inflamable, así como comprar todo el mobiliario, cableado, etcétera, con esta misma característica. Pero tendríamos costos muy altos, para ciertas empresas en ciertas ubicaciones esto puede ser necesario, pero no para la mayoría.
- No existe una solución perfecta, **su trabajo en esta fase es tomar decisiones inteligentes y hacer concesiones** (trade-offs) a la luz de los datos recopilados.

PERSONAS, PROCESOS, TECNOLOGÍA E INFRAESTRUCTURA EN LA GESTIÓN DE RIESGOS

- Ya habíamos hablado sobre personas, procesos y tecnología, en el ámbito de la planificación de BC/DR debemos agregar una cuarta categoría: **infraestructura**
- Claro que infraestructura está incluida en tecnología, pero no debemos olvidar los edificios, sus instalaciones, servicios públicos, transporte público, calles, etcétera. Toda vez sean relevantes para el negocio (de forma directa o indirecta por medio de clientes y proveedores)
- Por esta razón se recomienda separar infraestructura como una categoría adicional y no dejarla en tecnología.

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- En TI tenemos **riesgos únicos** que no existen en ninguna otra parte de la empresa
- Estos incluyen el desarrollo de estándares y procesos técnicos, físicos, administrativos y de gestión para proteger la **confidencialidad, integridad y disponibilidad (CIA) de la información** de toda la empresa.
- Se debe **balancear** las necesidades tecnológicas de la empresa (especialmente la disponibilidad) con las capacidades y costos tecnológicos actuales.
- Todo riesgo se puede mitigar con grandes gastos, **el objetivo de la gestión de riesgos es reducirlos de la manera más rentable posible.**

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- Parte de su trabajo como líder de TI es asegurarse que la empresa entienda el riesgo específico de TI y le respalde en los esfuerzos por mitigarlos.
- Por ejemplo, el departamento de finanzas puede entender ciertos riesgos relacionados con aceptar tarjeta de crédito en un punto de venta, pero no entenderá el riesgo relacionado a utilizar algún nivel o tipo de encripción, no tener actualizadas licencias para su firewall o SO del servidor, etc.
- Información adicional:
  - National Institute of Standards and Technology Resources (NIST)
  - http://csrc.nist.gov/publications/index.html

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- El mayor riesgo al que nos enfrentamos está relacionado con la seguridad de la información.
- El objetivo de la gestión del riesgo de TI es mantener los siguientes 3 elementos relacionados con CIA:
  - Asegurar completamente los sistemas de TI
  - Permitir a la gerencia tomar decisiones bien informadas con respecto a la compra e implementación de sistemas de TI
  - Permitir a la gerencia autorizar los sistemas de TI sobre la base de la documentación de respaldo que resulte de las actividades de gestión de riesgos de TI

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

Fases del desarrollo o adquisición de software	Descripción	Apoyo de las actividades de gestión del riesgo
1. Iniciación	Se expresa la necesidad de un sistema, se documenta el propósito y alcance de este.	Los riesgos identificados se utilizan para respaldar el desarrollo de los requisitos del sistema.
2. Desarrollo o adquisición	El sistema se diseña, compra, desarrolla o de alguna forma se construye.	Los riesgos identificados durante esta fase pueden ser utilizados para soportar el análisis de seguridad del software lo que puede llevarnos a concesiones en la arquitectura o diseño de este.
3. Implementación	Las características de seguridad del sistema deben configurarse, habilitarse, probarse y verificarse	El proceso de gestión de riesgos respalda la evaluación de la implementación del sistema frente a sus requisitos y dentro de su entorno operativo. Las decisiones sobre los riesgos identificados deben tomarse antes de la operación del sistema.

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

Fases del desarrollo o adquisición de software	Descripción	Apoyo de las actividades de gestión del riesgo
4. Operación / mantenimiento	El sistema está funcionando. Por lo general, el sistema será modificado de forma continua mediante la adquisición de nuevo hardware y software y debido a cambios en los procesos, políticas y procedimientos de la empresa	Las actividades de gestión del riesgo se reautorizan o reacreditan periódicamente o cuando existe un cambio importante en un sistema (como agregar nuevas interfaces)
5. Desecho	Esta fase puede implicar la disposición de información, hardware y software. Puede incluir mover, archivar, descartar o destruir la información y el hardware.	Se realizan actividades de gestión del riesgo para los componentes del sistema que se eliminarán o reemplazarán para garantizar que el hardware y software se eliminen adecuadamente, que los datos residuales se manejen adecuadamente y que la migración del sistema se realice de manera segura y sistemática.

COMPONENTES DE LA EVALUACIÓN DEL RIESGO

- **Amenazas** y **fuentes de amenazas** son términos que podemos utilizar sin distinguir alguna diferencia, pero en la evaluación del riesgo es importante realizar la distinción entre la amenaza y su fuente.
- Por ejemplo, un corte de energía es una amenaza que nos afecta a todos, la causa del corte de energía (fuente de la amenaza) podría ser un accidente en una subestación, falta de agua en una represa o un accidente en un poste cercano, tomar en cuenta las posibles causas nos ayuda a evaluar de mejor forma el riesgo determinando de mejor forma su probabilidad e impacto.

COMPONENTES DE LA EVALUACIÓN DEL RIESGO

- En lugar de realizar un análisis exhaustivo para cada amenaza que encontremos, se debe primero realizar la evaluación integral de amenazas para luego decidir en dónde enfocaremos nuestros esfuerzos en la evaluación de vulnerabilidades, en lugar de esforzarnos desde el inicio y desperdiciar recursos en una amenaza en específico.

MÉTODOS DE RECOPILACIÓN DE INFORMACIÓN

- Métodos más utilizados:
  - Cuestionarios: Permiten obtener datos específicos y estandarizados.
  - Entrevistas: Permiten descubrir información necesaria por medio de un diálogo.
  - Revisión de documentos: Revisión de la documentación de la empresa (manuales, procesos, etc.) nos puede ayudar en identificar amenazas, sus fuentes y vulnerabilidades.
  - Investigación: Investigar sobre diferentes amenazas, estadísticas asociadas a estas, procesos y recomendaciones durante un desastre, datos públicos de policía, bomberos, hospitales u otras organizaciones.
- Aunque se verá tentado a buscar la mayor cantidad de datos, recuerde que debe establecer un límite para no verse inmerso en una gran cantidad de datos que después no pueda analizar de forma correcta.

LISTA DE VERIFICACIÓN DE AMENAZAS

- Amenazas naturales/ambientales
  - Inundación
  - Tormenta invernal severa
  - Tormenta eléctrica
  - Sequía
  - Terremoto
  - Tornado
  - Huracán
  - Tsunami
  - Volcán
  - Pandemias
- Amenazas causadas por humanos
  - Incendio, incendio provocado
  - Robo, sabotaje, vandalismo
  - Disputas laborales
  - Violencia en el trabajo
  - Terrorismo
  - Peligros químicos y biológicos
  - Guerra, guerra civil
- Amenazas a la infraestructura
  - Fallas en edificios
  - Equipos no informáticos / sistemas
  - Calefacción / refrigeración, energía
  - Interrupción de transporte público
  - Falta de combustible
  - Contaminación de comida o agua
  - Cambios legales
- Amenazas específicas de TI
  - Amenazas cibernéticas (amenazas a CIA)
  - Fallos en sistemas y hardware
  - Fallos en equipos de línea de producción
  - Pérdida de datos

EVALUACIÓN DEL RIESGO

- De esta fase se obtiene un documento listando todas las amenazas potenciales y sus fuentes que se han analizado para la empresa.
- Solo se deberían eliminar aquellas amenazas que claramente no aplican para su empresa, el resto se utilizará como entrada para la fase de evaluación de vulnerabilidades.
- Ejemplo: esta matriz es solo una guía y puede ser modificada según las necesidades específicas:

No.	Amenaza	Fuente	Vulnerabilidad	Probabilidad	Controles existentes	Impacto	Calificación
1	Fuego	Interna	%	%	Extintores, …	%	%
2	Fuego	Externa	%	%	Extintores, …	%	%
3	Inundación	Interna	%	%	Sensores de humedad	%	%

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Revisaremos algunas metodologías de evaluación de amenazas que nos pueden servir para esta fase.
- Existen dos enfoques esenciales:
  - Cuantitativo
  - Cualitativo

  - Recuerde seleccionar uno de los dos enfoques y quedarse con este.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Enfoque Cuantitativo
  - Se busca utilizar números concretos para representar amenazas, vulnerabilidades e impactos ($, %).
  - Por ejemplo, “el servidor cuesta $1,500 más que una workstation” es una declaración cuantitativa, mientras “el servidor es más caro que una workstation” sería una declaración cualitativa “más” no es específico ni medible.
- Veamos el siguiente ejemplo

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Amenaza: Corte de energía
- Fuente: Rayo
- Probabilidad de ocurrencia: datos recabados indican que ocurre 1 vez cada 4 años por lo que la probabilidad será **0.25 anual**. No solo tomamos en cuenta rayos que caigan directamente sobre el edificio sino aquellos que caigan en el área y que puedan causar un corte de energía.
- Vulnerabilidad: Si cada vez que cae un rayo en el área tenemos un corte de energía la vulnerabilidad a esta amenaza será de 1 (100%) anual.
- Valor de riesgo: Probabilidad de ocurrencia x Vulnerabilidad = 0.25 x 1 = 0.25.
- Impacto: Asumamos que cada vez que esto ocurre la empresa eléctrica se tarda en llegar y reparar la falla por lo que el tiempo entre la ocurrencia y la reparación es de 2 días. ¿Cuánto nos cuesta estar sin energía 2 días?
  - Pérdidas en ventas: Q18,000 diarios, Q36,000 por ocurrencia.
  - Costos fijos: Q4,200 diarios, Q8,400 por ocurrencia.
  - Daño por mala reputación: arbitrariamente se asignó Q2,000 diarios, Q4,000 por ocurrencia. Este dato puede ser muy subjetivo (cualitativo por naturaleza), si su empresa puede realizar un cálculo objetivo utilícelo. Puede utilizar el mismo costo diario para cualquier amenaza para ser consistente, pero recuerde que no es lo mismo estar cerrado por 2 días que 1 mes.
  - Impacto total: Q36,000 + Q8,400 + Q4,000 = Q48,400
- **Valor total del Riesgo: Q48,400 * 0.25 = Q12,100 anual.**
- Si sabe que el costo del riesgo de un corte de energía eléctrica debido a un rayo es de Q12,100 al año, es más fácil evaluar las posibles inversiones para mitigarlo, como un generador de energía que cueste Q50,000, equipo de protección contra rayos por Q5,000, seguro que cubra parte de la pérdida asociada por Q3,000 anuales, etc.
  - Para evaluar inversiones recuerde que, por ejemplo, el generador de energía tiene una inversión inicial, costo de operación y tiempo de vida que puede ser mucho mayor a 1 año. Tampoco olvide que puede tener beneficios adicionales que le generen otros ahorros o ingresos.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Enfoque Cualitativo
  - Se busca definir las amenazas, vulnerabilidades e impactos relativos utilizando lenguaje, por ejemplo, “alto”, “medio” y “bajo”.
  - Se debe utilizar un sistema cualitativo con una escala que le permita ser consistente.
  - Por ejemplo:

Numérico	Frecuencia	Impacto
6	Constante	Extremadamente alto
5	Muy frecuente	Muy alto
4	Frecuente	Alto
3	Poco frecuente	Bajo
2	Muy poco frecuente	Muy bajo
1	Nunca	Extremadamente bajo

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Otro ejemplo:

Nivel de probabilidad	Descripción
Alto	La fuente de la amenaza está altamente motivada y es suficientemente capaz y los controles para evitar que se ejerza la vulnerabilidad son ineficaces
Medio	La fuente de la amenaza está motivada y es capaz, pero existen controles que pueden impedir el ejercicio exitoso de la vulnerabilidad
Bajo	La fuente de la amenaza carece de motivación o capacidad o existen controles para impedir, o al menos impedir significativamente que se ejerza la vulnerabilidad

- Tabla realizada por NIST (National Institute of Standards and Technology) específicamente para vulnerabilidades asociadas a la seguridad informática.
- Trate de utilizar valores pares como en el primer ejemplo, para obligarse a realizar una elección y no tender a ir al medio.
- Al utilizar el enfoque cualitativo debe asegurarse que todas las personas involucradas tienen un claro entendimiento y están de acuerdo con las escalas; no todos le damos el mismo significado a las palabras.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Veamos el ejemplo anterior con un enfoque cualitativo:
- Amenaza: Corte de energía
- Fuente: Rayo
- Probabilidad de ocurrencia: Ocurre 1 vez cada 4 años, le asignaremos un valor de 3, es decir, “Poco frecuente”.
- Vulnerabilidad: Si cada vez que cae un rayo en el área tenemos un corte de energía le asignaremos un valor de 6, es decir, “extremadamente alta”.
- Impacto: Asumamos que cada vez que esto ocurre la empresa eléctrica se tarda en llegar y reparar la falla por lo que el tiempo entre la ocurrencia y la reparación es de 2 días. Supongamos que esto es un impacto “bajo” (3) pues no nos pone en mucha desventaja frente a nuestros competidores, clientes y proveedores por lo que son pérdidas que podemos soportar.
- **Valor total del riesgo: promedio del valor de Probabilidad de ocurrencia + Vulnerabilidad + Impacto = (3 + 6 + 3)/3 = 4, según nuestra tabla: Alto**

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Podemos buscar mayor detalle, por ejemplo, en Impacto podríamos determinar diferentes valores para diferentes problemas, no es lo mismo que una PC ya no funcione después de un apagón a que sea el servidor de base de datos, quedará en usted la decisión de qué tanto detallarlo y qué escala utilizar (6 elementos, calificación de 1 a 100, etcétera)
- Puede indagar más al respecto en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- En el apéndice G de este documento puede encontrar diferentes tablas para la probabilidad de ocurrencia, incluso utilizando diferentes escalas dependiendo si la amenaza es intencional o no.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

EVALUACIÓN DE VULNERABILIDADES

- Una vulnerabilidad se define como la debilidad, susceptibilidad o exposición a peligros o amenazas.
- Estas pueden ser explotadas intencionalmente o activarse involuntariamente.
- El resultado de la evaluación de amenazas se convierte en el insumo para la evaluación de vulnerabilidades.
- Esta evaluación se puede dividir en probabilidad de ocurrencia y vulnerabilidad basada en la probabilidad de ocurrencia.
  - La ventaja de separarlos es tener visibilidad de aquellas amenazas que son poco probables pero que la empresa es muy vulnerable a ellas, como a los terremotos, y hacer un análisis especial para estas.
- Para realizar esta evaluación se recomienda dividir las amenazas para que diferentes equipos puedan encargarse de esta evaluación, queda a su criterio la forma que pueda funcionar mejor según el caso específico. Por ejemplo,
  - Clasificar las amenazas utilizando la estructura de Personas, Procesos, Tecnología e Infraestructura.
  - Clasificarlas como Externas e Internas.
  - O por área de la empresa como IT, Instalaciones, Finanzas, RRHH, Operaciones, etc.
- La evaluación no será exclusiva del grupo encargado, por el contrario, tendrán que trabajar en conjunto con personal de toda la empresa.
- Asegúrese de establecer metas, fechas de entrega y hacer revisiones cruzadas entre equipos de forma que estén seguros de seguir un estándar.

EVALUACIÓN DE VULNERABILIDADES

- Revisemos nuevamente la estructura Personas, Procesos, Tecnología e Infraestructura desde el punto de vista de una evaluación de vulnerabilidades.
- Personas: debemos evaluar qué tan vulnerables son las personas a las fuentes de amenazas, por ejemplo, phishing o ingeniería social. No solo evaluar pensando en las personas que trabajan en la empresa sino la comunidad que nos rodea.
- Procesos: ¿Qué tan vulnerables son nuestros procesos (de negocio y de TI) a las fuentes de amenazas identificadas? Por ejemplo:
  - El proceso de toma de pedidos que se ejecuta en un área con 10 computadoras, 10 teléfonos y un sistema que lo facilita, ¿qué tan vulnerable es a una fuente de amenaza que no permita utilizar este espacio?
    - A la vez que estemos evaluando esta vulnerabilidad seguramente estemos pensando en formas de mitigar el riesgo.
  - Entre más estandarizados y documentados tengamos nuestros procesos, más fácil será el poder evaluarlos y crear estrategias de mitigación.

EVALUACIÓN DE VULNERABILIDADES

- Tecnología: Claro está que la tecnología es vulnerable a muchas fuentes de amenazas, nosotros como Ing. En Sistemas podemos pensar rápidamente en los más comunes. ¿Qué tan vulnerables estamos a un ataque interno o externo? ¿Qué tan vulnerable es nuestro servidor web?
- No asuma que sus procesos estándares ya han abordado las vulnerabilidades, tampoco asuma que sus planes de emergencia actuales serán adecuados para todas las fuentes de amenazas.
- Por el contrario, asuma que no tiene nada al respecto o trate de verlo desde "fuera de la caja" para realizar una evaluación detallada.
  - Por ejemplo, pudo haber tomado en cuenta una inundación pensando en algún río cercano o por alcantarillado con problemas, pero no por una tubería defectuosa dentro del edificio y esta última fuente hace que se deba tratar por separado.
- Por último, recuerde incluir la tecnología que no esté a su cargo pero que puede de igual forma ser vulnerable como TV por cable, sistema de alarmas y cámaras, etc.

EVALUACIÓN DE VULNERABILIDADES

- Infraestructura: Por supuesto que la infraestructura es vulnerable a ciertas fuentes de amenazas y no a otras; una inundación solo si estamos a nivel de un río o lago, inundación interna, etc.
- Será el experto, como un Ing. Civil o Arquitecto, quien pueda apoyarnos con esta evaluación.
- No olvidemos evaluar la infraestructura externa a la empresa, como carreteras, instalaciones de las empresas que nos brindan servicios (telecomunicaciones, energía, etc.), etc.

EVALUACIÓN DE VULNERABILIDADES

- Una evaluación de vulnerabilidades puede ser cuantitativa, cualitativa o semicuantitativa.
- Muchas veces se utiliza la semicuantitativa con tablas como las que ya revisamos con anterioridad.
- Al igual que en la evaluación de amenazas y sus fuentes, debemos recabar información por medio de cuestionarios, entrevistas, etc.
- Por ejemplo, fuentes de amenaza de daño por agua a los sistemas informáticos:

Descripción	Alto	Medio	Bajo
1. Si la tubería del edificio se dañara y dejara escapar gran cantidad de agua, ¿qué tan vulnerables son nuestros sistemas informáticos?			
2. Si en el edificio hubiera un incendio, ¿qué tan vulnerables son nuestros sistemas informáticos al agua que el sistema de supresión de incendios utilizara para apagarlo?			
3. Si el edificio se viera afectado por ingreso de agua por fuertes lluvias, ¿Qué tan vulnerable son nuestros sistemas informáticos?			

EVALUACIÓN DE VULNERABILIDADES

- Con esta tabla evaluamos qué tan vulnerables están los sistemas informáticos a estas fuentes de amenaza, ahora se debe determinar la probabilidad de ocurrencia para obtener un valor de riesgo (subtotal pues aún falta el impacto) utilizando los datos cuantitativos, cualitativos o semicuantitativos.
- Finalmente se deberá analizar todos los datos recabados y ajustarlos de ser necesario para que sean consistentes.
- Al finalizar este proceso obtendremos un listado de:
    1. Todas las fuentes de amenazas potenciales.
    2. La probabilidad de ocurrencia de estas.
    3. Vulnerabilidad de su empresa y sistemas informáticos a estas.
    4. Valor de riesgo provisional.
- El documento puede ser un entregable que pueda dar una mejor idea a la alta gerencia sobre avances e importancia de este proyecto. Si fuera necesario, debería obtener una aprobación formal de este.