Guía de cómo calcular el riesgo antes de iniciar un Programa de Métricas.

Herbert Calderon CPP, PCI, PSP, CSMP@ISMI, CFE.

Introducción.

Todo programa de seguridad debe contar con métricas e indicadores necesarios para observar su desempeño. Erroneamente se asumen indicadores de costos, presupuestos, proyectos, de horas, de capacitaciones, etc. Sin antes considerar el estado real de los riesgos asociados, medir sus tendencias, observar el progreso del programa o simplemente evidenciar que no tenemos datos del daño en proceso contra la operación.

Debemos en primer término considerar que cualquier programa de seguridad debe ir orientado al nivel de los problemas que afecten y puedan afectar a la operación productiva. Este procedimiento se denomina la cuantificación del riesgo que es la expresión matemática del estado real de la amenaza en su aproximación al daño.

Los elementos que desarrollaremos serán a partir de la probabilidad y la consecuencia del daño al proceso en términos monetarios.

Con respecto a la probabilidad, proviene, como comentamos de la frecuencia de eventos relacionados con la pérdida. Esta frecuencia esta dividida en dos aspectos la información que identifica a la intencionalidad de la amenaza, esto obedece a todos los aspectos que establecen la amenaza, relativos a información sobre intenciones del evento de pérdida, entre los cuales hay información por ejemplo no confirmada que proviene de fuente interna, policiales así como llamadas a línea anónima, el considerarlos como información no confirmada, pero que si corresponden a una intención de un hecho. Adicionalmente se deben considerar los eventos realizados como robos efectuados, así como los incidentes de robos que vendrían a ser robos frustrados o que no se han logrado concretar.

En los alcances de la frecuencia de los fracasos del sistema son todos los robos concretados, simulacros de robo fracasados o eventos de daño. Denominados incidentes de robos.

La ecuación del riesgo compuesta de los elementos de amenaza y el fracaso del sistema, conjugado con el valor el activo.

La amenaza obliga a desarrollar la prevención necesaria para disminuir el fracaso del sistema, de forma que disminuyan los fracasos por haberse tomado en cuenta dicha información. Sin embargo al no tomar en cuenta o utilizar convenientemente la información las amenazas incrementarán.

En consecuencia, la medición de estado del riesgo periódicamente es considerar la tendencia, que es observar la mejora en la disminución del riesgo mes a mes, luego de ello se puede construir o implementar cualquier sistema o métrica.

Procedimiento.

I.-La Ecuación general del riesgo, es la ecuación utilizada en seguridad física que utilizaremos justamente para cuantificar los resultados reales de los éxitos o fracasos del sistema de gestión así como la tendencia de los informes recibidos por diferentes canales auque no sean confirmados sino en proceso.

Se consideran tres variables: la intencionalidad de la amenaza que son todos los informes sin confirmar o por trabajar que pueden dar inicio a una investigación como reportes de: vigilancia, líneas anónimas, personas sospechosas, hechos sospechozos, intentos de robos, informes verbales, etc.

La segunda variable se refiere a los fracazos del sistema, dados por fallas, errores, robos, simulacros, etc.

La tercera variable es refierida al valores del activo, calculado de acuerdo a tabla anexa.

ECUACION GENERAL RIESGO:
RIESGO=(INTENCIONALIDAD DE LA AMENAZA)(FALLAS DEL SISTEMA)(VALOR DEL ACTIVO).

INTENCIONALIDAD DE LA AMENAZA(POR CONFIRMAR O NO):
¿TENGO COMO ENTERARME DE LA AMENAZA?.
SE REFIERE A LA INFORMACION PREVIA QUE INDICA UNA POSIBILIDAD DE UN HECHO: REPORTES, INTELIGENCIA, INFORMACION PREVIA.

FALLAS DEL SISTEMA: ¿QUE HA PEMITIDO LA FALLA DEL SISTEMA?
SE REFIERE A LOS ERRORES O ACCIONES QUE EL SISTEMA PERMITIRA Y HA PERMITIDO UN HECHO NEGATIVO.

II.-La información se obtiene del Estudio de Seguridad, en el cual se establecen las preguntas relacionadas la identificación de hechos y la existencia o no de los recursos de información.

Observaciones del Estudio de Seguridad.

1. No existen reportes de vigilancia de robos. F-V-I
2. No hay informes de trabajadores sobre robos. F-I-V
3. Si hay revisión de CCTV, sobre personal sospechoso. E-I
4. No hay códigos de sanciones a la deshonestidad. F-V
5. No hay revisión de paquetes a trabajadores. F-V
6. No hay revisión de vehículos. F-V
7. No hay centro de control. F-I
8. Los agentes de vigilancia no tienen orden de puesto. F-V
9. Empresa de vigilancia, se le han encontrado durmiendo 4 veces a la semana. F-V
10. Reportes de decomisos. F-I-V
11. No hay información policial de robos. F-I-V
12. No hay Información interna de robos. F-I-V
13. Hay informes de otros incidentes no relacionados. E
14. Si hay Tips de empleados/ línea ética. I
15. Si hay recuperación objetos olvidados. E
16. Sistema no detecta robos: internos, externos. F-V
17. Existen huellas, pisadas, ventanas abiertas sospechosas. V-I
18. No hay simulacros de robos. F.
19. 4 robos de material informático, en oficinas en 1 mes, no hay back up.. F-V.

III.-Los informes obtenidos son debidamente clasificados en base a lo requerido para las variables de intencionalidad, fallas del sistema.

Estudio de Seguridad: robo.	Vulnerabilidades-intencionalidad.	Peso
	1. ¿Existen reportes de vigilancia de robos?	
	2. ¿Existen informes de trabajadores sobre robos?	
	3. ¿Existen centro de control?	
	4. ¿Existen reportes de decomisos?	
	5. ¿Existen informes policiales de robos?	
	6. ¿Existen información interna de robos?	
	7. ¿Existen supervisión de condiciones inseguras internas?	
	8. ¿Existen reportes de CCTV, sobre condiciones inseguras?	
	9. ¿Existen informes de otros incidentes no relacionados?	
	10. ¿Existen Tips de empleados/ línea ética?	
	Vulnerabilidades-fallas del sistema.	
	1. ¿Existen inspecciones para recuperación objetos olvidados?	
	2. ¿El sistema detecta robos, esta en buenas condiciones?	
	3. ¿Existen simulacros de robos del sistema?	
	4. ¿Existen códigos de sanciones a la deshonestidad?	
	5. ¿Existen procedimientos de revisión de paquetes a trabajadores ?	
	6. ¿Existen procedimientos de revisión de vehículos?	
	7. ¿El personal de vigilancia tienen orden de puesto?.	
	8. ¿El personal de vigilancia tiene un buen desempeño?	
	9. ¿Han habido incidentes de robos de material informático, en oficinas?	

IV.- Asignación de valores a las preguntas, de acuerdo al cuadro siguiente:

Estado de la observación	Clasificación	Recomendación
No existe la medida/desconoce y ha habido daño.	5	Implementarla
Existe pero desactualizada o no se cumple ha habido daño parcial.	3	Actualizarla
Existe pero no es suficiente y ha habido daño.	1	Evaluarla.
Existe y cumple y el daño es el mínimo	0	Mantenerla

Para luego posteriormente asignar peso a cada pregunta y reorganizar en las clasificaciones de intencionalidad, fallas del sistema o vulnerabilidades.

Intencionalidad

Observación	Puntuación
1. Si hay reportes de vigilancia de robos	0
2. No hay informes de trabajadores sobre robos	5
3. No hay centro de control	5
4. Hay reportes de decomisos no bien implementados.	3
5. No hay información policial de robos	5
6. No hay Información interna de robos	5
7. Existen huellas, pisadas, ventanas abiertas sospechosas	3
8. Si hay revisión de CCTV, sobre personal sospechoso	0
9. Hay informes de otros incidentes no relacionados	0
10. Si hay Tips de empleados/ línea ética	0
10 NOVEDADES POR PESO 5=50	26/50=0.52

Fallas del Sistema

Observación	Puntuación.
1. Si hay recuperación objetos olvidados	0
2. Sistema no detecta robos obsoleto: internos, externos	3
3. No hay simulacros de robos	5
4. No hay códigos de sanciones a la deshonestidad	5
5. No se cumplen los procedimientos de revisión de paquetes a trabajadores	3
6. No se cumplen los procedimientos de revisión de vehículos	3
7. Los agentes de vigilancia no tienen orden de puesto.	5
8. Ha la empresa de vigilancia, se le han encontrado durmiendo 4 veces a la semana.	3
9. Ha habido 4 robos de material informático, en oficinas en 1 mes por descuido.	3
9X5=45	30/45=0.666

VI.- Cálculo de la consecuencia.

Consecuencias

Activo critico	Lap top	Material sensible	Herramientas.	Repuestos	Explosivos o sustancia.	Servidor
Proceso critico.						
No tiene back up.	5 Valor	10 Valor	5 Valor	5 Valor	5 Valor	20 Valor
No tiene reemplazo	10 Valor	20 Valor	15 Valor	10 Valor	5 Valor	15 Valor
Es altamente tóxico.					10 Valor	
No hay plan de contingencia	15 Valor	30 Valor	20 Valor	10 Valor	10 Valor	15 Valor
Proceso Secundario	2 Valor	3 Valor	3 Valor	2 Valor		

VII.- Cálculo final del riesgo.

2015	Intencionalidad	Fallas del sistema	Consecuencia	Riesgo
Enero	0.52	0.66	10 valor	0.34
Febrero	0.45	0.63	10 valor	0.284
Marzo	0.4	0.6	10 valor	0.240
Abril	0.35	0.5	10 valor	0.175
Mayo	0.35	0.45	10 valor	0.158
Junio	0.25	0.44	10 valor	0.110