Risk Management

Bernens (1997):" la grieta pequeña más grande en la armadura corporativa es la dirección de riesgos".

Entiendo que generalmente los usuarios actuales de lugares undergrond en internet, suelen confundirse el concepto "**seguridad de la información**" con el concepto "seguridad informática".
En los tiempos que estamos viviendo ya no se puede hablar de algo tan pequeño como lo es la seguridad informática, sino que se debe adoptar el concepto de seguridad de la información para poder suprimir las frases que ya no sirven.

Ustedes se preguntaran, quien ha de escribir esta guía. Mi nick es Cygog, soy un profesional de la seguridad de la información certificado por varias instituciones internacionales, me gusta enseñar a los **newbites** que empiezan en este mundillo, para atraparles y despertarle la curiosidad, que es lo que seguramente a muchas de las personas que en este momento estén leyendo lo que escribo quieran saciar un poco la sed de su sabiduría. Ya me deberán conocer muchos de ustedes, ya que entiendo que la mayoría siempre somos los mismos leyendo este tipo de guías.

Esta vez no voy a escribir sobre puro hacking, sino que voy a escribir sobre **introducción** a la gestión de los riesgos de la seguridad de la información en empresas IT (tecnologías de la información). También quiero dejar en claro, que esta guía está reflejada para personas sin conceptos previos, por lo cual, cualquier persona podrá entender lo escrito ya que he tratado reducir el lenguaje profesional y solo tocar aspectos básicos.

¿Que entendemos por gestión de riesgo?

La gestión de riesgo son acciones o metodologías coordinadas por la alta gerencia de una empresa o un siendo un servicio de un tercero confiable, intentando, evaluar todos los activos que puedan producir un problema para esta, siendo un circuito cerrado o abierto. Ahora entendemos que los riesgos son dinámicos. Algunos ejemplos evaluativos son: Monitoreo de red, revisiones de logs, cámaras de seguridad, backups protegidos por encriptaciones.
Los riesgos generalmente se los clasifica por:

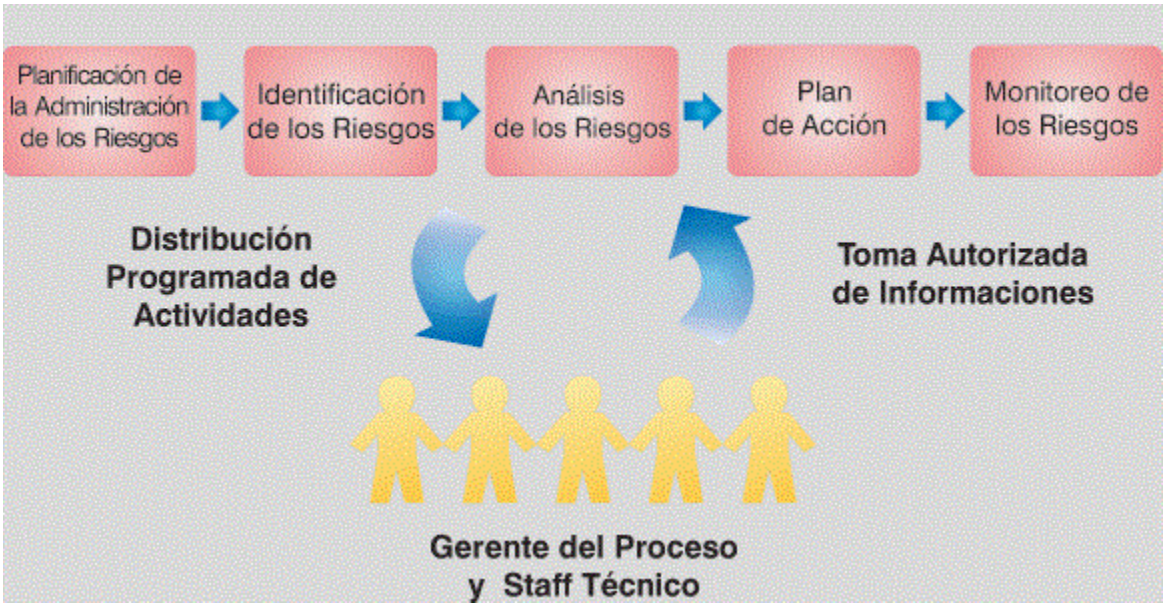

IMAGEN POR teostek

Riesgo Personal

Ejemplos: Secuestro, muerte prematura, enfermedad e incapacidades a una persona poseedora de contraseñas únicas

Riesgos de las posesiones

Ejemplos: Ruptura de servidores, perdida de dinero.

Riesgos de Responsabilidades

Ejemplos: Persona encargada de backups no los realiza diariamente como lo establecido previamente.

Riesgos físicos

Ejemplos: Instalaciones eléctricas inadecuadas

Riesgos químicos

Ejemplos: Gases tóxicos

Riesgos biológicos

Ejemplos: Hongos y bacterias.

Riesgos psicosociales

Ejemplos: Motivación de parte de los empleados de una empresa

Riesgos ergonómicos

Ejemplos: Trabajo insalubre, incomodo.

Riesgos de choque de eléctrico

Ejemplos: Niveles altos de voltaje.

Riesgos de incendio

Ejemplos: Inflamabilidad de materiales.

Riesgos de radiaciones
Ejemplos: Ondas de ruido, de láser y ultrasónicas.

Riesgos mecánicos
Ejemplos: Inestabilidad de las piezas eléctricas.

Podría seguir con la lista de riesgos para una empresa largo tiempo, es por eso que para dejarles una participación a ustedes, he pensado preguntarles como clasificarían:
-El robo de un servidor
-Incendio de planta de desarrollo de software

Las respuestas envíenmela a cygog@live.com.ar

Identificación De Riesgos

Antes de enfrentar los riesgos, alguien debe identificarlos. Esta tarea es de nunca acabar, pues nuevas amenazas están surgiendo constantemente.

La identificación de riesgos es dinámica y depende de las metodologías o acciones que ejercerá la organización encargada de la misma, generando constantemente un relevamiento de información acerca de las actividades de la organización.

Los eventos indeseables que pueden ocurrir o los eventos deseables que pueden fallar	El hardware o software que puede causar la falla	Las razones humanas o fallas que en el mecanismo puede ocurrir.	El resultado funcional inmediato de un riesgo	El impacto de mal funcionamiento de los objetivos del sistema	La primera indicación o exhibición observable de un mecanismo del sistema	Una estimación del mal funcionamiento	Posibles medidas de eliminación de mecanismos de riesgo	Acción implementada para eliminar o controlar el riesgo	Valor de todos los recursos requeridos para implementar acciones preventivas.
MODO DE RIESGO	MECANISMO DE RIESGO	CAUSA DEL RIESGO	EFECTO DEL RIESGO	SEVERIDAD DEL RIESGO	DETECCION DEL RIESGO	PROBABILIDAD DEL RIESGO	MEDIDAS TOMADAS CON EL RIESGO	ACCION PREVENTIVA	RECURSOS DE CONTROL

IMAGEN SACADA DE monografías

Usualmente se hablan de 4 niveles o aspectos a someter por parte de la organización encargada de la gestión de riesgos, aunque existen más, pero aquí solo describiré la más usual.
Estas técnicas se utilizan eventualmente para prevenir la ocurrencia de pérdidas y minimizar los costos o pérdidas ante un incidente:

EVITAR RIESGOS: La organización no acepta el riesgo como tal.

REDUCCION DE RIESGOS: Una vez canalizados los riegos se prosigue a reducirlos. Un ejemplo es poner matafuegos.

CONSERVACION DE RIESGOS: La organización acepta convivir con determinados riesgos.

COMPARTIR RIESGOS: Los riesgos son participes de empleados de la empresa

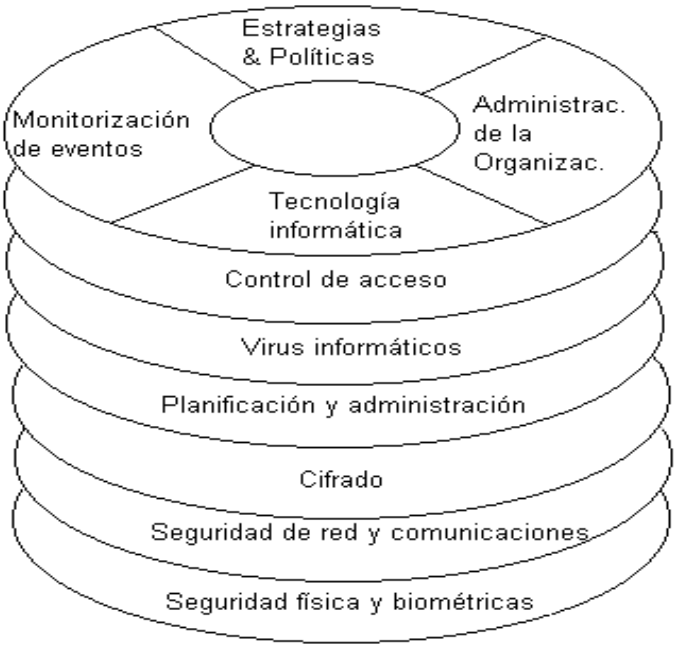

IMAGEN SACADA DE monografías

Adquisición con una gestión de riesgos satisfactoria:

Garantiza un mejor manejo de recursos

Minimizar el costo del negocio causado por los riesgos

Proteger a los empleados de perjuicios

Conocer las obligaciones contractuales y legales

Eliminar preocupaciones posteriores

Espero les haya gustado, esta es mi primer edición de este tema, teniendo en cuenta tiempos, un manual no introductorio, es decir el manual completa sobre gestión de riesgos lo estaré publicando dentro de aproximadamente 3 meses. Saludos. Atte.: Cygog