RAM-SI, METODOLOGÍA PARA LA IDENTIFICACIÓN, MEDICIÓN Y EVALUACIÓN DEL RIESGO OPERATIVO ASOCIADO A LA PÉRDIDA O FUGA DE INFORMACIÓN EMPRESARIAL

Oscar Humberto Niño Ramírez[1]

Universidad Pontificia Bolivariana
Bucaramanga, Colombia
oscarhumberto16@gmail.com

Resumen

El diseño de una herramienta que permita la identificación y evaluación del riesgo operativo, es de vital importancia para la mitigación de las consecuencias y repercusiones generadas por la pérdida o fuga de información empresarial. Cumpliendo las demandas de seguridad que surgen hoy en día en términos de protección de la información, se desarrolló una metodología que basada en la herramienta Matriz para la gestión de riesgos (R.A.M), permite definir el nivel de riego asociado a cada tipo de información, la cual identifica y evalúa las probabilidades y las consecuencias derivadas de la fuga de información empresarial. Para desarrollar la Metodología, en primera instancia se diseñó un diagrama de flujo en el cual se correlacionaron los conceptos de riesgo, amenaza, consecuencia y probabilidad en la gestión segura del ciclo de la información empresarial. Como segundo elemento de consolidación de la herramienta se definió el conjunto de activos y procesos afectados en un posible caso de fuga de información, teniendo en cuenta las categorías consignadas en el Enfoque Stope de la Norma 27001.Con base en lo anterior, se procede a describir el procedimiento para la identificación, medición y evaluación del riesgo operativo asociado a las consecuencias generadas en caso de fuga de información, mediante la aplicación de la herramienta Risk Assessment Matrix Segurity Information (RAM-SI), con el fin de establecer un conjunto de controles y estrategias que posibiliten la gestión segura de la información empresarial. La aplicación de este procedimiento en conjunto con otras políticas de la organización contribuiría a la sinergia de reforzar el eslabón más débil de la cadena de la información: el usuario final.

Palabras claves

Fuga de Información, Amenaza, Riesgo, Consecuencia, Probabilidad, Matriz R.A.M-SI, Ciclo seguro de la Información.

[1] Ingeniero de Sistemas, Universitaria de Investigación y Desarrollo. Facultad de Ingeniería de Sistemas

Abstract

The design of a tool that allows the identification and evaluation of the operative risk, performs vital importance for the mitigation of the consequences and repercussions generated by the loss or escape of managerial information. Fulfilling the safety demands that arise nowadays in protection terms of the information, there developed a methodology that based on the tool Risk Assessment Matrix (R.A.M), allows to define the level of irrigation associated with every type of information, which identifies and to evaluate the probabilities and the consequences derived from the escape of managerial information. To develop the Methodology, in the first instance there was designed a flow chart in which there were correlated the concepts of risk, threat, consequence and probability in the sure management of the cycle of the managerial information. Since the second element of consolidation of the tool defined the set of assets and processes affected in a possible case of escape of information, having in it counts the categories recorded in the Approach Stope of the Norm 27001. With base in the previous thing, one proceeds to describe the procedure for the identification, measurement and evaluation of the operative risk associated with the consequences generated in case of escape of information, by means of the application of the Risk Assessment Matrix Segurity Information (RAM-SI), in order to establish a set of controls and strategies that make possible the sure management of the managerial information. The application of this procedure as a whole with other policies of the organization would contribute to the synergy of reinforcing the weakest link of the chain of the information: the final user..

Keywords:
It Escapes of Information, Threat, Risk, Consequence, Probability, Counterfoil R.A.M - SI, sure Cycle of the Information.

1. Introducción

La información es un activo empresarial que requiere ser manejada, clasificada y protegida adecuadamente de todas aquellas amenazas y vulnerabilidades que afecten su confidencialidad, integridad y disponibilidad

Una amenaza explícita, es la fuga o pérdida de información, la cual ha desencadenado y sigue desencadenando consecuencias negativas e irreversibles para cualquier organización. Tal y como se indica en el reporte elaborado por Roberto Cabrera y Rommel Garcia, directores de la práctica de Asesoría en IT en KPMG México[2] , el cual argumenta que desde el año 2007 hasta junio de 2010 alrededor de 514 millones de empresas en todo el mundo sufrieron este tipo de amenaza.

Teniendo en cuenta tal necesidad, se requiere de una herramienta que permita la identificación y evaluación del riesgo operativo, la cual contribuya a la mitigación de las consecuencias asociadas a la fuga de información empresarial

[2] CABRERA, R. y GARCIA R. KPMG International Data Loss Barometerhttp [en línea]. 2010 [citado enero 27 de 2012]. Disponible en internet: <URL:http://www.bsecure.com.mx/ultimosarticulos/crecen-fugas-de-informacion-por-hackeo-y-perdida-de-dispositivos-po>

Con respecto a lo anterior, es importante conocer que el proceso de administración de cualquier tipo de riesgo comienza una vez la organización ha sido consciente del conjunto de factores de riesgo al cual está expuesta. Este proceso está compuesto por el conjunto de todas las actividades y decisiones que una empresa realiza orientadas a controlar la exposición a los factores de riesgo que la afectan y que, según Smithson[3], consta de las siguientes etapas.

1. Formulación de objetivos y metas que debe cumplir la administración del riesgo.
2. Identificación y cuantificación de las exposiciones.
3. Definición de una filosofía de manejo y cubrimiento de riesgo.
4. Evaluación y control.

En la actualidad las metodologías utilizadas para el tratamiento de la fuga de información están basadas en complejos programas de software, los cuales implican altas inversiones en términos de recursos tecnológicos, humanos y financieros.

La Metodología Risk Assessment Matrix Segurity Information (RAM-SI), es un procedimiento que brinda a los usuarios un considerable ahorro de tiempo y dinero, ya que es de fácil entendimiento y aplicación. Esta herramienta se desarrolló mediante una adaptación de la Risk Assessment Matrix (R.A.M), con el fin de aplicarla a procesos de seguridad informática, adaptación que permite la identificación de activos, amenazas, probabilidades y consecuencias asociadas a la fuga de información empresarial, lo cual representa un avance significativo para la seguridad de la información.

Mediante la metodología RAM-SI se puede definir el nivel de riego asociado a cada tipo de información, permitiendo clasificarla según su valoración en: Secreta, Confidencial, Restringida y/o Pública, lo cual servirá de soporte para definir estrategias y controles que fortalecerán la gestión documental y el ciclo de la información en las organizaciones.

2. METODOLOGÍA GENERAL

La metodología general se soporta en la obtención de información teórica acerca de procedimientos y metodologías de identificación y medición del riesgo operativo en las empresas. Para tal efecto en la industria petrolera es muy difundido el uso de la herramienta R.A.M, la cual se utiliza, específicamente para la estimación del riesgo asociado a trabajos en áreas operativas, pero no se tiene precedente alguno de su aplicación para establecer los riesgos asociados con eventos de fuga de información.

La metodología RAM-SI, documentada en este artículo se desarrolló teniendo en cuenta las siguientes 4 etapas, las cuales facilitaron el cumplimiento a los objetivos propuestos:

2.1 Revisión detallada de la información relevante.

Para el diseño de la presente metodología se analizaron los conceptos relacionados con la gestión del riesgo operativo y su incidencia en la seguridad informática. Con base en esto, se desarrolló un diagrama de flujo que representa relación de los conceptos de riesgo, amenaza, consecuencia y probabilidad en la gestión segura del ciclo de la información empresarial.

[3] SMITHSON, Charles W. Managing Financial Risk. 3ª ed. McGraw-Hill. pp. 550-573

2.2 Diseño de la Metodología para la identificación, medición y evaluación del riesgo operativo asociado a la pérdida o fuga de información empresarial.

Con base en la bibliografía consultada, se diseña el procedimiento para la identificación, medición y evaluación del riesgo operativo asociado a los eventos de pérdida o fuga de información empresarial, mediante la aplicación de la Metodología R.A.M-SI. En esta etapa se identificaron, los activos y procesos afectados en un posible caso de fuga o perdida de información empresarial, teniendo en cuenta las categorías consignadas en el Enfoque Stope de la Norma 27001. Teniendo en cuenta este enfoque, en primera instancia, se definen las consecuencias potenciales y reales a la vez que se le asigna su nivel de afectación, posteriormente se establecen las probabilidades teniendo en cuenta la frecuencia de ocurrencia de un evento de fuga de información y por último se clasifican los riesgos.

Los anteriores parámetros permiten construir paso a paso la Metodología R.A.M-SI.

2.3 Clasificación de la Información según la evaluación del Riesgo RAM-SI.

En esta etapa se realiza una compilación de los diferentes tipos de información empresarial que está expuesta a diferentes amenazas y vulnerabilidades internas y externas. Esta clasificación se realiza teniendo en cuenta el nivel de riesgo derivado de la evaluación en la herramienta RAM-SI

2.4 Formulación de estrategias de Mejora para la Gestión Segura de la Información empresarial.

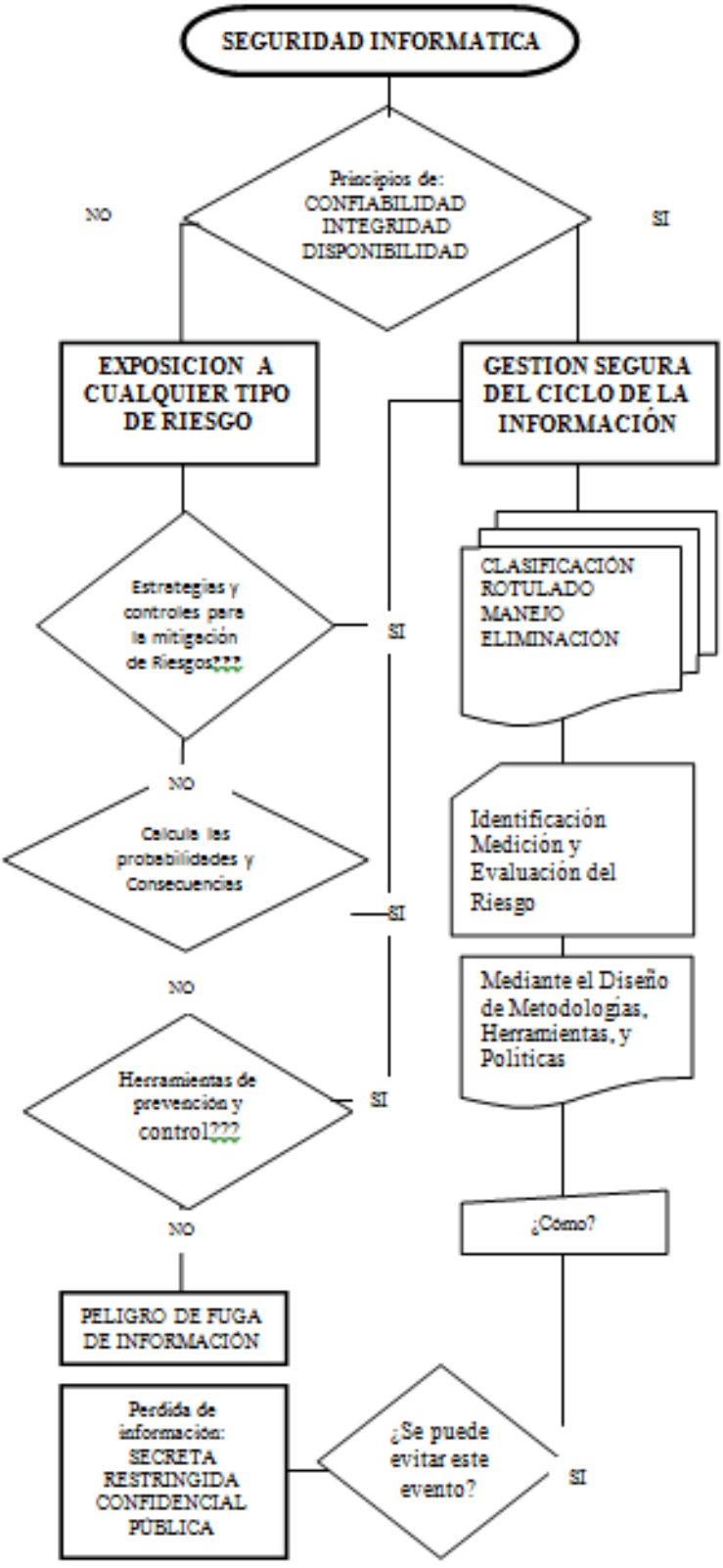
En esta etapa se establece un conjunto de controles y estrategias que posibilitan la gestión segura de la información empresarial.

3. DESARROLLO DE LAS FASES

3.1 Revisión detallada de la información relevante.

Esta etapa para efectos del presente artículo, se sintetizó en el siguiente objetivo específico: *Diseñar un diagrama de flujo que representa la incidencia que tienen los conceptos de riesgo, amenaza, consecuencia y probabilidad en la gestión segura del ciclo de la información empresarial*, en el cual tuvieron en cuenta las siguientes definiciones planteadas en el marco teórico de la propuesta.:

- Seguridad Informática.
- Confiabilidad.
- Integridad.
- Disponibilidad.
- Ciclo de la Información.
- Riesgo.
- Probabilidad.
- Consecuencia.
- Amenaza.
- Fuga de Información.
- Información Secreta.
- Información Confidencial.
- Información Restringida.
- Información Pública.
- Clasificación.
- Rotulado.
- Manejo.
- Eliminación.


SEGURIDAD INFORMATICA
Principios de:
CONFIABILIDAD
INTEGRIDAD
DISPONIBILIDAD
NO
SI
EXPOSICION A CUALQUIER TIPO DE RIESGO
GESTION SEGURA DEL CICLO DE LA INFORMACIÓN
Estrategias y controles para la mitigación de Riesgos???
SI
CLASIFICACIÓN
ROTULADO
MANEJO
ELIMINACIÓN
NO
Calcula las probabilidades y Consecuencias
SI
Identificación Medición y Evaluación del Riesgo
NO
Herramientas de prevención y control???
SI
Mediante el Diseño de Metodologías, Herramientas, y Políticas
NO
¿Como?
PELIGRO DE FUGA DE INFORMACIÓN
Perdida de información:
SECRETA
RESTRINGIDA
CONFIDENCIAL
PUBLICA
¿Se puede evitar este evento?
SI

3.2. Diseño de la Metodología para la identificación, medición y evaluación del riesgo operativo asociado a la pérdida o fuga de información empresarial.

Generalidades. La metodología desarrollada está conformada por un conjunto de pasos lógicos y secuenciales que permiten establecer cualitativamente el nivel de riesgo asociado a eventos de fuga de información empresarial convirtiéndose en un instrumento de apoyo a los programas, políticas y protocolos de aplicados en seguridad informática lo cual contribuye a fortalecer la gestión segura del ciclo de información m al interior de las empresas.

Los modelos estadísticos ascendentes[4], estan basados en información histórica sobre la frecuencia y la cantidad de los eventos de pérdida de información mediante las cuales se estima una medida del nivel de riesgo al que está expuesta la empresa u organización, en base a este modelo se diseña la Metodología R.A.M-SI. Un modelo estadístico similar es la herramienta utilizados para la medición del Riesgo (R.A.M), herramienta que mediante la clasificación de amenazas, consecuencias y probabilidades facilita la evaluación cualitativa de los riesgos en actividades propias de la industria petrolera.

Para efectos del diseño sistemático de la metodología se tuvieron en cuenta las siguientes fases:

Fase 1. Definir las categorías de las consecuencias.

Fase 2. Evaluación de las consecuencias.

Fase 3. Evaluación de las probabilidades.

Fase 4. Evaluación del Nivel de Riesgo.

Fase 5. Descripción del procedimiento para la aplicación metodología

Fase Nª 1. Definición de las categorías de las consecuencias según los estándares consignados en las normas ISO 17799 e ISO 27001

Los estándares ISO 27001 e ISO 17799 le brindan a una organización las bases para desarrollar un marco de gestión de la seguridad de la información efectivo, que le permita proteger sus activos de información importantes, minimizando sus riesgos y optimizando las inversiones y esfuerzos necesarios para su protección.

Una de las formas de protección consiste en la aplicación de controles, que en la práctica pueden ser políticas, procesos, procedimientos, organización (definición de una estructura organizacional de seguridad), elementos de software y hardware, mecanismos de protección de la infraestructura física y de seguridad, así como la adecuada selección y entrenamiento del personal que opera y utiliza los recursos de información o informáticos. La norma ISO 27001 presenta una serie de áreas para ser gestionadas, mediante la aplicación de controles o mecanismos de protección, las cuales van desde la seguridad en los sistemas, pasando por los aspectos de seguridad física, recursos humanos y aspectos generales de la organización

[4] Comité de Basilea (2.002), Hiwatashi (2.002) y Roehr (2.002)

interna en las organizaciones. Esta Norma Integra las diez áreas donde trabaja la IEC 17799 con base en el enfoque Stope, el cual se agrupa en las categorías de estrategia, tecnología, organización, personal y entorno, las áreas de acción del estándar.

Figura 2. Activos del Enfoque Stope de la IEC17799.

Fuente: Autor

La Metodología R.A.M-SI, se apoya en el esquema Stope de la Norma 27001 para darle más sustentabilidad y aplicabilidad a nivel práctico y poder definir las fronteras de acción de cada una de las áreas de la empresa. El enfoque Stope[5], pretende, a partir de las categorías, generar puntos de control para cada una de los activos. Esto llevará, a generar un procedimiento que pueda certificar que se cumplieron las metas de la implantación del estándar. Para esto debe apoyarse en una herramienta conceptual, que en este caso es la Matriz R.A.M-SI, la cual básicamente consiste en seguir un proceso lógico para la implantación de la norma desde el punto de vista práctico.

Fase Nª 2. Evaluación de las consecuencias.

En esta fase se realizó una clasificación de las consecuencias con base en lo que podrá o podría haber ocurrido bajo condiciones levemente diferentes (consecuencias potenciales estimadas) o en lo que realmente ocurrió, dependiendo del activo que se esté evaluando o clasificando, a saber. En esta fase, se realizan cuadros comparativos y explicativos en donde se clasifican las consecuencias potenciales y reales que podían ocurrir en caso de un evento de pérdida de información.

[5] Using ISO 17799-2005 Information security management a Stope view with six sigma approach. International Journal of Network Management, p. 93.

Tabla 1. Ejemplo de situaciones Hipotéticas con resultados, reales y potenciales.

SITUACIÓN HIPOTETICA	SITUACIÓN REAL	SITUACIÓN POTENCIAL
Empleado vendiendo información confidencial a la competencia (base de datos de clientes.)	Conocimento de los clientes potenciales y objetivos de parte de la competencia	Perdida de Clientes - Quiebra de la Empresa
Una empleado que pierde un documento memoria USB, una laptop, o un *pen drive* en la empresa o en un lugar público.	Manejo de la informacion por entes externos	Infiltracion en la empresa - Copia de estrategias organizacionales- Quiebra de la empresa
Ente externo que tiene acceso a una base de datos en la organización.	Infiltracion de entes externos y/o destruccion de la informacion	Conocimento de datos exclusivos y perdida de competencia.
Equipo infectado con un Spyware que envie información a un delincuente.	Infiltracion de entes externos y/o destruccion de la informacion	Extorsiones o chantajes empresariales
Mantener equipos corporativos desbloqueados o encendidos.	Copia y/o plagio de información	Usurpación de Identidad, transaciones indebidas

SITUACIÓN HIPOTETICA	SITUACIÓN REAL	SITUACIÓN POTENCIAL
Navegar por Internet desde casa mientras se está conectado a redes empresariales.	Recopilancion de información por programas espias.	Infeccion de las redes empresariales con Spyware.
Interceptación de una señal de radio desde otra empresa de algún delincuente para saber datos personales o corporativos.	Puesta en conocimiento de información personal y/o empresarial	Extorsiones, chantajes, secuestros personales y/o empresariales
Grabar información empresarial en un CD, DVD, memoria USB, Memory Card, Ipod.	Copia y/o plagio de información	Venta de informacion a delincuentes o a la competencia
Enviar datos confidenciales por correo corporativo, correo público, por mensajeria instantánea, o subirlo a alguna página de almacenamiento, transmitirlo por FTP, publicarlo en alguna de las redes sociales (hi5, Facebook, Myspace, etc.) y/o imprimirlo.	Puesta en conocimiento de información personal y/o empresarial	Extorsiones, chantajes, secuestros personales y/o empresariales. Perdida de Clientes - Quiebra de la Empresa.Venta de informacion a delincuentes o a la competencia

Fuente: El Autor

Definición y evaluación del Nivel de las de las consecuencias. La definición de las categorías de las consecuencias derivadas de un caso de fuga de información se realiza teniendo en cuenta las categorías relacionadas en el enfoque Stope de la norma ISO 27001, las cuales para efectos de medición se denominaran "categorías de consecuencia", las cuales se clasifican en: consecuencias al Recurso Humano, consecuencias económicas derivadas de un suceso de fuga de información, afectación a los clientes, impacto en la imagen de la empresa y daños Tecnológicos y Organizacionales. Para determinar el nivel de las consecuencias en la RAM-SI, estas se encuentran ordenadas en filas y se utiliza una escala de "0" a "5" para evaluar su impacto. En las siguientes tablas se describen y se define el nivel de las consecuencias según las categorías seleccionadas.

Tabla 4. Consecuencias al Recurso Humano por fuga de información.

NIVEL	DEFINICIÒN
0	**Ninguna Afectación** directa al personal o al rendimiento laboral de la empresa por motivos de la fuga de información
1	**Afectación leve :** Llamados de atención verbal al personal pero no afecta el rendimiento laboral.
2	**Afectacion menor:** Llamados de atención a un grupo de trabajo pero no afecta el rendimiento laboral.(Caso de Suplantacion de identidad p.ej.)
3	**Afectacion media:** Llamados de atención con copia a la Hoja de Vida. Apertura de Investigaciones. Perdida de tiempo por Afectación en el rendimiento laboral, cambio de contaseñas y permisos de acceso, (Caso de Perdida de propiedad intelectual p.ej.)
4	**Afectacion Mayor:** Investigaciones con perjucio de sanciones legales y/o penales. Suspención de contratos.Afectación en el rendimiento laboral por largo tiempo. Afectan el desempeño laboral por largo tiempo. Chantajes u extorsiones a la empresa o a funcionarios en especifico.
5	**Afectacion Grave.** Secuestros individuales o Masivos. . Extorsiones y Chantajes con afectacion de la integridad fisica de funcionarios directos o de su nucleo familiar.la empresa .Atentados terroristas contra la empresa.

Las personas constituyen uno de los problemas más importantes de seguridad para cualquier organización porque a diferencia de los componentes tecnológicos, son el único elemento, con la capacidad de decidir "romper" las reglas establecidas en las políticas de seguridad de la información[6].

Tabla 4. Consecuencias económicas[7], derivadas de un suceso de fuga de información.

NIVEL	DEFINICIÒN
0	Perdida Despreciable: de 0 al 1% del Capital Productivo de la empresa.
1	Perdida Marginal: Del 1 al 5% del Capital Productivo de la empresa.
2	Pérdida Importante: Del 5 al 10% del Capital Productivo de la empresa.
3	Perdida Severa: Del 10 al 25% del Capital Productivo de la empresa.
4	Pérdida Crítica: Del 25 al 50% del Capital Productivo de la empresa.
5	Perdida Catastrófica > 50% del Capital Productivo de la empresa.

[6] MIERES, Jorge. Debilidades de seguridad comúnmente explotadas. Ingeniería Social. Evil Fingers. Pag 8. Enero de 2009.

[7] PONEMON INSTITUTE LLC. The Cost of a Lost Laptop, Sponsored by Intel Corporation. [En línea]. :<URL:http://communities.intel.com/docs/DOC-3076>

Tabla 5. Consecuencias generadas en los clientes de la organización

NIVEL	DEFINICIÒN
0	Ningún impacto a los clientes
1	**Riesgo de incumplir cualquiera de las especificaciones acordadas con el cliente:** Fuga de información que afecta los procesos, los productos y/o los servicios que pueden impactar los compromisos establecidos con los clientes, pero con posibilidades de solución antes de que el cliente perciba tal circunstancia
2	**Implica quejas y/o reclamos:** Cuando la Fuga de información afecta los procesos o productos y/o servicios pactado con los clientes, situacion que genera quejas y/o reclamos , cuyo trámite de solución está definido dentro de la información perdida.
3	**Pérdida de clientes y/o desabastecimiento:** Fuga de información que pueden afectar la relación comercial y/o el índice de lealtad, al punto de llevar al cliente a que tome la decisión de no volver a comprarle a la empresa, o cuando efectivamente debido a tal perdida no se pueda asegurar el suministro confiable para algún mercado objetivo.
4	**Pérdida de participación en el mercado (para mercado internacional pérdida en la participación en el presupuesto del cliente destinado a la compra de productos ofertados por la empresa):** Fuga de información de una magnitud tal, que implique pérdida efectiva de participación en el mercado para productos y/o servicios de comercialización nacional, y en el mercado internacional la pérdida de participación en el presupuesto de compra del cliente.
5	**Veto a la empresa como proveedora de productos y/o servicios :** Fuga de información que genera un impacto comercial a gran escala, la cual implica el bloqueo por parte de segmentos de clientes que a su vez conforman mercados objetivo.

Tabla 5. Consecuencias generadas en la imagen de la organización.

NIVEL	DEFINICIÒN
0	**Ningún impacto:** No es de interés
1	**Interna:** La Fuga de información es de conocimiento interno de la empresa pero no de interés público.
2	**Local - interés público local relativo:** La Fuga de información despierta la atención de algunos medios de prensa locales que potencialmente pueden afectar a la empresa
3	**Regional - interés público regional:** La Fuga de información genera controversias y oposición de los medios Regionales de prensa. Relativa atención de los medios nacionales de prensa y/o partidos políticos locales/regionales.
4	**Nacional - interés público nacional:** La Fuga de información genera se eleva como noticia en los medios de prensa nacionales. Se generan políticas nacionales/regionales con medidas potencialmente restrictivas y/o impacto en el otorgamiento de licencias. Perdida de confiabilidad. Posible afectación del valor de las Acciones.
5	**Internacional – interés público internacional: La Fuga de información genera la atención de** los medios de prensa internacionales.Impacto potencialmente grave en las relaciones internacionales de la Empresa, Perdida de confiabilidad. Afectación del valor de las Acciones.

Tabla 7. Consecuencias generadas por el sabotaje y/o infiltraciones en los recursos tecnológicos de la empresa[8].

NIVEL	DEFINICIÒN
0	Sin afectación Tecnologica
1	**Ataques Personales:** Informacion personal y no empesarial
2	**Ataques de Phreakers:** son intrusos especializados en sabotear las redes telefónicas de la organización para poder realizar llamadas gratuitas. **Ataques de suplantación de la identidad**
3	**Ataques de Sniffers:**Son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.2.8. Lamers ("wannabes"): "Scriptkiddies" o "Click-kiddies" **Ataques de "lamers":** también conocidos por "script kiddies" o "click kiddies" ,obtiene determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan. **Ataques DoS– Denial of Service:** Denegación del Servicio
4	**Ataques de Crackers ("blackhats"):** individuos que atacan sistema informático para obtener beneficios o provocar daño a la organización. **Ataques de Spammers** son los responsables del envio masivo de miles de mensajes de correo electrónico no solicitados a través de redes como, provocando el colapso de los servidores **Ataques de Piratas informáticos** **Ataques Insiders:**empleados desde dentro de la Institución u Organización.
5	* **Creadores de virus y programas dañinos** * **Códigos maliciosos, o malware.** * **Fraudes, engaños y extorsiones** * **Ataques contra los sistemas criptográficos** * **Ataques de Inyección de Código SQL**

[8] Elaboración propia. Tomado de GÓMEZ V. Alvaro. Tipos de ataques e intrusos en las Redes informáticas[EnLínea]:http://www.mundointernet.es/IMG/pdf/ponencia95.pdf.

Tabla 6. Consecuencias al nivel Organizacional.

NIVEL	DESCRIPCIÓN
0	Sin afectación Organizacional
1	**Afectación a nivel Individual:** Datos no comprometen la integridad del funcioanrio o de las operacions de la empresa.
2	**Afectación a nivel Grupal:** La Fuga de información se genera por la perdida de datos de un grupo de trabajo en especifico. ocurre un ataque a los equipos infomaticos o se genera cambi de contraseñas grupales. Pero la informacion fugada, no incide en los porcesos de la empresa.
3	**Afectación a nivel de Departamento o Area:** La Fuga de información genera daño en los equipos de todo un departamento,
4	**Afectación a nivel Gerencial :** La Fuga de información se presenta a nivel gerencial
5	**Afectación a nivel Organizacional:** la fuga de informacion afecta a toda la Organización causando multiples consecuencias al interior de la misma.

Fase N° 3. Evaluación de las probabilidades.

En la metodología RAM-SI, se evalúa la probabilidad mediante la utilización de una escala de literal que va desde la “A” hasta la “E”, la cual se estipula en la siguiente tabla.

Tabla 2. Niveles de probabilidad.

A	B	C	D	E
Extremadamente Improbable	Improbable	Algo Probable	Probable	Muy Probable

El eje horizontal de la RAM-SI representa la medición de probabilidad de la ocurrencia del evento, con la consecuencia identificada. La escala del eje horizontal se define como:

A – Extremadamente Improbable.
B – Improbable.
C – Algo probable
D – Probable.
E – Muy Probable

Relación entre consecuencias y probabilidades.

Basándose en la experiencia, frecuencia y/o evidencia histórica en que las consecuencias derivadas de un evento de fuga de información se presenten dentro de la empresa permite relacionar la probabilidad de que se desencadenen consecuencias potenciales o reales, según el tipo de información.

Para efectos de la presente metodología, la estimación de la probabilidad y las consecuencias no es un criterio exacto, ya que el mismo depende de factores históricos y conceptos subjetivos de los responsables de realizar el análisis.

La estimación de la consecuencia depende entonces de respuestas al “qué ocurrió” o “qué pudo o podrá ocurrir; mientras que la estimación de la probabilidad se basa en información histórica respecto de casos ocurridos anteriormente en similares condiciones, sabiendo que las circunstancias nunca son exactamente las mismas.

El cruce entre las escalas de consecuencia y probabilidad se determina la evaluación y clasificación cualitativa del riesgo.

Fase Nª 4. Evaluación y Clasificación cualitativa del riesgo

La evaluación y clasificación de los riesgos debe hacerse teniendo en cuenta las consecuencias y las probabilidades, ya que por definición el concepto de riesgo corresponde a la siguiente expresión:

Riesgo = Probabilidad X Consecuencias

Para efectos de la Metodología RAM-SI, se han establecido 5 Niveles de riesgo los cuales son:

MA: Muy Alto
A: Alto
M: Medio
B: Bajo
N: Ninguno

Los 5 Niveles de riesgos definidos son consecuentes con la escala de "0" a "5" utilizada para la estimación de las consecuencias. Con del fin de facilitar la comprensión y aplicación de la metodología, los niveles de riesgo se han denotado cada uno con un color especifico. MA: Rojo; A: Naranja; M: Amarillo; B: Bajo; N: Verde.

En la tabla 4, se especifican los diferentes niveles de riesgo al igual que su descripción al momento de tomar decisiones al respecto de un caso de fuga de información empresarial.

Tabla 4. Niveles de riesgo y su descripción.

COLOR	RIESGO	DESCRIPCION
MA	Muy Alto	Intolerable. Se deben implementar medidas radicales al respecto.
A	Alto	Si se presenta un caso de fuga de infomacion catalogado como Alto, deben generarse estrategias que mitigen el riesgo. De lo contrario se debe demostrar cómo se controlará esta amenaza y los cargos de niveles iguales o superiores a Gerente, deben participar y aprobar tal decisión.

M	**Medio**	Los sistemas de control establecidos no son suficientes; se deben tomar medidas que controlen mejor el riesgo.
B	**Bajo**	Se deben gestionar mejoras a los sistemas de control establecidos (politicas, procedimientos, Herramientas, listas de chequeo, responsabilidades, protocolos).
N	**Ninguno**	Riesgo muy bajo, usar los sistemas de control y calidad establecidos (politicas, procedimientos, Herramientas, listas de chequeo, responsabilidades, protocolos).

Fuente: Autor.

Fase Nª 5. Descripción del procedimiento para la aplicación metodología.

Todas las organizaciones están sujetas a eventos de pérdida o fuga de información. Según un reciente estudio publicado por AvanteGarde[9], La falla principal que permite que los usuarios sean atacados y sean víctimas de la gran cantidad de amenazas que nos acechan, radica en que en muchos casos se está gestionando la tecnología dentro de un marco incompleto de protección de la información, y en la falta de concientización a las personas en los riesgos relacionados con el uso de tecnología y de herramientas organizacionales.

El procedimiento desarrollado y consolidado en la Metodología RAM-SI, se enmarca en un "Sistema Integral de Gestión de Seguridad de la Información", ya que está diseñado y direccionado para concientizar a los usuarios acerca de las consecuencias personales y empresariales generadas en caso de fuga o pérdida específicamente con la información que ellos manejan. Solo mediante la sensibilización en el uso adecuado de los recursos informáticos y en los riesgos propios de su utilización se pueden preservar las características básicas de la información. Esta metodología deja en claro a los funcionarios de la organización que las consecuencias de este tipo de ataques y amenazas, van desde el despido irrevocable con las sanciones legales y penales del caso, hasta la quiebra de la empresa.

[9] SECURITY ABSURDITY: The complete, unquestionable and total failure of information security. Noam Eppel, Vivica Information Security Inc.

Herramienta Metodológica.

La Metodología R.A.M-SI, está soportada en una herramienta de medición que unifica los conceptos y parámetros detallados en las fases 1, 2, 3 y 4, referentes al diseño de la metodología. Esta herramienta consolida en una matriz los elementos necesarios para la identificación, medición y evaluación del riesgo.

Componentes de la RAM-SI.

La Matriz para la Gestión de Riesgos de Seguridad Informática está conformada por 8 filas y 12 columnas en donde se consolidan los conceptos de probabilidad, consecuencia y riesgo. El cruce entre filas y columnas constituye la determinación del nivel de riesgo asociado según el caso a evaluar.

A continuación se describen los principales componentes de la matriz:

1. Filas de Categorías. Este componente está conformado por 6 filas enumeradas, en las cuales se consignas las categorías organizacionales consignadas en la norma ISO 27001.

Tabla X. Categorías Organizacionales

CATEGORIAS ORGANIZACIONALES					
I	II	III	IV	V	VI
RECURSO HUMANO	ECONOMICA	IMAGEN CORPORATIVA	CLIENTES Y ACREEDORES	TECNOLOGIA	ORGANIZACIÓN

2. **Columnas de descripción de las consecuencias de cada una de las Categorías.** Este componente contiene la definición de cada una de las consecuencias derivadas en un caso de fuga de información que impactan las categorías consignadas en el enfoque Stope de la Norma ISO 27001. Está conformado por 7 filas y 7 columnas. A medida de que ascendemos en una columna en específico, las consecuencias son de mayor impacto. En la última columna se utiliza una escala de "0" a "5". Para determinar el nivel de las consecuencias (Ver Anexo A)

3. Componente de probabilidades de Ocurrencia. En esta parte de la Matriz, se encuentran consignados los parámetros de ocurrencia y el nivel de riesgo asociado a cada una de las consecuencias evaluadas.

PROBABILIDAD DE OCURRENCIA				
A	B	C	D	E
Extremadamente improbable	Improbable	Algo Probable	Probable	Muy Probable
M	M	A	A	MA
B	M	M	H	A
N	B	M	M	A
N	N	B	B	M
N	N	N	B	B
N	N	N	N	N

Fuente: Matriz para la gestión de riesgos (R.A.M), Modificado por el Autor.

Procedimiento para la evaluación de riesgos asociados a un evento de pérdida o fuga de información.

Para evaluar el riesgo de un caso en particular se debe seguir la siguiente secuencia:

1. Identificar la información que maneja cada funcionario.

2. Evaluar las consecuencias que traería para la organización en un caso de fuga o pérdida de información, teniendo en cuenta cada una de las categorías organizacionales consignadas en la matriz.

3. Para cada categoría se debe evaluar la probabilidad de que ese suceso ocurra. Esto se hace desplazándose hacia la derecha (Identificar el numero con el que se encuentra (0-5) y evaluando si es probable, improbable etc., (A-E) según sea el caso.

4. La intersección entre la celda de la consecuencia fijada y la columna de la probabilidad estimada corresponde al nivel de riesgo asociado a la fuga o pérdida de información. Esto representa el producto de la fila y la columna. (1A, 5C, 2B, 3D, 4E etc.)

5. El nivel de riesgo en cada una de las categorías, por lo general es diferente. Para establecer el nivel de riesgo total para la empresa, se debe tener en cuenta la categoría de consecuencia que tenga la mayor clasificación, por ejemplo: Un funcionario es el encargado de consolidar los costos derivados de la producción de un bien es específico. En dicho archivo, se establecen los elementos que fijan el precio final del producto. Si esta información se perdiese y llegará a manos de la competencia, ¿Qué consecuencias traería para el empleado y para la empresa? En este caso comenzamos a evaluar la categoría: Recurso Humano y cruzando las filas y las columnas este sea de 4D, con consecuencias en la categoría Económica de 2D, Imagen corporativa 1D Clientes y Acreedores 3D, y Tecnológico de 2B, Organizacionales de 5D. De esta manera el riesgo total de que un evento como este ocurra será de 5D. Para efectos de la aplicación de la metodología en otros casos consultar el Anexo B.

La evaluación de las consecuencias asociadas en un evento de fuga de información, permitirá que el funcionario sea consciente de la responsabilidad que tiene al ser el custodio directo de dicha información, lo cual permitirá definir según el nivel asociado a la información manejada, definir controles específicos para cada funcionario y definir el tipo de información según sea el caso en: Secreta, Confidencial, Restringida y/o Publica.

Clasificación de la Información según la evaluación del Riesgo RAM-SI.

La clasificación de la información, es una actividad y a la vez una competencia que cada organización debe desarrollar. Esta práctica define el nivel de importancia y protección que un funcionario debe darle a la misma, lo que en sí mismo, delinea aquello que no deberá circular, lo que deber fluir de manera restringida y lo que puede circular libremente.

Frente a esta práctica y competencia el reciente informe elaborado por Forrester por encargo de RSA y Microsoft, liberado en marzo de 2011, denominado *The value of corporate data*, advierte que el 57% de las fugas de información de las empresas están asociados con accidentes de la indebida clasificación de la información de parte de los empleados, tal como divulgación de información sensible de la empresa y/o envío de información confidencial de la empresa a través de medios masivos de información o vía correo electrónico[10].

Con base en esto, se puede inferir que cuando no se cuenta con una adecuada clasificación de la información, las fallas o accidentes que se presenten generarán mayores impactos negativos, tales como, multas, sanciones legales, quejas de los clientes, que generan pérdida de valor de la empresa y daños importantes en la imagen y competitividad en su entorno de negocio.

Considerando lo anterior, la clasificación de los activos de información, se convierte en una práctica indispensable para adelantar las actividades de negocio de cualquier organización. No asegurar esta práctica, expone a la organización a una pérdida de posicionamiento global e importantes impactos económicos, que debilitan, no solo los informes de pérdidas y ganancias, sino también la moral interna de cada persona perteneciente a la misma ya que se incumple con la misión de: generar valor con la información. La Metodología RAM-SI, permite clasificar la información según el nivel de riesgo asociado a la misma. De esta manera si después de realizada dicha evaluación, si el nivel de riesgos es MA, la información queda clasificada como Secreta, si el análisis de riesgos arroja un resultado A o M, la información se debe tratar como Confidencial y/o Restringida pero si dicha identificación es B y/o N, la información se considera General o Publica. A continuación se relaciona la clasificación según el nivel de riesgo asociado.

Tabla N° X. Clasificación de la información según el nivel de riesgo.

CLASIFICACIÓN	DESCRIPCIÓN	NIVEL DE RIESGO RAM-SI
SECRETA	La fuga o pérdida genera desventajas competitivas o pérdidas económicas significativas a la empresa	MA
	Puede comprometer la seguridad de los funcionarios de la empresa	
	Constituye un secreto comercial, industrial, fiscal o de otro tipo.	
	Puede poner en riesgo la vida, la seguridad o la salud de las personas.	
	Este tipo de información NO circula.	

[10] FORRESTER (2011). The value of Corporate Secrets. How Compliance And Collaboration Affect Enterprise Perceptions Of Risk. March. Disponible en: http://www.rsa.com/document.aspx?id=10844 (Consultado: 05-06-2012)

CONFIDENCIAL Y/O RESTRINGIDA	La fuga o pérdida puede crear cierto grado de expectativas o conllevar a pérdidas económicas bajas.	A
	Puede lesionar levemente la integridad del personal.	
	La mayoría de la información del día a día es de este tipo y sólo debe estar al alcance del personal autorizado.	M
	Circula en un proceso, departamento o area.	
GENERAL Y/O PUBLICA	Puede estar al alcance de todos los funcionarios.	B
	Puede ser conpartida con entes externos	
	Puede ser publicada en los medios internos de la Empresa.	N
	Circula libremente al interior dela Empresa.	

Fuente: Autor

2.4. Formulación de estrategias de Mejora para la Gestión Segura de la Información empresarial.

Para minimizar las consecuencias derivadas de un caso de pérdida o fuga de información, es necesario incorporar políticas, protocolos y procedimientos especiales en el diseño, implementación e implantación de los Sistemas de Información.

Los controles son todos aquellos métodos, estrategias, políticas y procedimientos que logran los activos de una organización, la precisión y la confiabilidad de sus registros.

El control debe ser parte integral del diseño, por tal motivo, se deben implementar controles que mitiguen el nivel de riesgo de las amenazas a la cual está expuesta la organización.

Según, el material pedagógico, *Seguridad y control de sistemas de información*, diseñado Mendoza[11], existen 2 tipos de controles: Generales y de Aplicaciones.

Controles Generales. Son aplicables a todos los sistemas de la organización y consisten en una combinación de software y procedimientos. Los cuales son:

- **De implantación.** Son puntos formales de revisión de las diferentes etapas del desarrollo del Software.

- **Del software**. Evitan el acceso al Software. Están diseñados para evitar cambios no autorizados de los programas y de los datos.

- **De hardware**. Deben asegurarse físicamente de forma tal que sólo tengan acceso a ellos las personas autorizadas. También contemplan aquellas aplicaciones que verifican posibles fallas de Hardware.

- **De operaciones de cómputo.** También conocidas como auditorías. Aseguran que los procedimientos programados sean consistentes y estén siendo aplicados correctamente en su procesamiento y almacenamiento.

- **En los datos.** Que los datos que están en cintas o discos no estén al alcance de personas no autorizadas.

- **Administrativos.** Son normas, reglas, procedimientos y disciplinas formales para garantizar que los controles de la organización se ejecuten.

Controles Aplicaciones. Son específicos para cada aplicación de computador (p.e., nómina, cuentas por cobrar). Consisten en controles aplicados a los tipos de usuarios particulares de un sistema y a la programación de los procedimientos. Los cuales son:

- **De entradas**. Procedimientos para chequear la exactitud y completitud de los datos cuando son introducidos en el sistema.

- **De procesamiento**. Rutinas para garantizar que los datos se mantienen completos y exactos durante una actualización.

- **De salidas.** Medidas que aseguren que los resultados de los procesamientos hechos por el computador sean exactos, completos y distribuidos apropiadamente.

Formulación de Controles. Para efectos del presente artículo se tuvieron en cuenta cada uno de los tipos de controles establecidos en la literatura. Los cuales se proponen como puntos de partida para evitar la consolidación de fugas o pérdidas de información empresarial.

[11] MENDOZA Luis E. MSc. en ingeniería de Sistemas. Departamento de Seguridad y sistemas. Universidad Simón Bolívar. Caracas, Venezuela 2009

Con respecto a los tipos de información.

1. Adquirir un sello de tinta indeleble para clasificar la información Secreta o Restringida y estamparlo en una parte que no afecte la visibilidad del documento.

2. Foliar y/o rotular los documentos para identificar y corregir a tiempo perdidas de información. Exceptuar los documentos generales y/o públicos.

3. Si se debe enviar información secreta o restringida al interior de la red de la empresa, escribir en el asunto: ***información restringida*** o ***información secreta*** con el texto del asunto.

4. No dejar visible la información Secreta o Restringida, guardarla en cajones bajo llave, y asegurar las mismas en un lugar confidencial.

Controles a la Información Impresa

La información secreta, debe tener un responsable, solo el podrá autorizar la copia de las mismas.

La impresora debe estar adecuada con facilidades de captura y liberación controladas.

Asignar una clave para la impresión.

La impresión no se debe enviar desde equipos remotos, se debe recoger inmediatamente.

Si se debe enviar información al interior de la empresa, seguir las siguientes recomendaciones:

Si la información es restringida enviar los documentos en un sobre sellado marcado como información restringida.

Si la información es secreta enviar los documentos en doble sobre sellado:

El sobre interior debe ir cerrado y marcado con información secreta más los datos del destinatario.

El sobre exterior debe ser de mayor tamaño. Debe contener el sobre interior y la carta remisoria. Debe ir cerrado y marcado con los datos de correspondencia.

Para eliminar información secreta o restringida se debe tener autorización del custodio de la misma.

Utilizar las máquinas destructoras de papel.

No botar a la caneca documentos con información secreta o restringida, existe una práctica denominada “trashing” que consiste en buscar información en la basura.

Controles en la información de formato electrónico

Almacenar la información secreta o restringida en las carpetas del área en los servidores corporativos.

Establecer una nomenclatura en el área para nombrar las carpetas que contengan información secreta o restringida, pero que no lo digan de manera explícita.

Identificar los usuarios que pueden acceder a esas carpetas y los permisos que tienen (lectura, escritura y/o control total).

Revisar los usuarios y permisos cada 3 meses

Nunca se debe almacenar información secreta o restringida en USB, discos externos, CD, DVD y demás dispositivos portátiles. Tienen un alto riesgo de pérdida, daño o hurto.

Hacer copias de respaldo de la información del PC (de uso general) y de los Pst de su correo, al menos una vez al mes.

En caso de hurto o pérdida del pc, reportar inmediatamente a la empresa.

Cuando exista un cambio de máquina o equipo se debe informar a los encargados de los sistemas la necesidad de depuración o eliminación de la información, mediante un formato para oficializar la actividad de depuración y eliminación de medios).

Los encargados de los sistemas de cómputo que realiza la depuración de la información deben utilizan herramientas de borrado seguro. De esta forma no se puede restaurar la información.

Controles a la información recibida y enviada por Correos electrónicos internos

En caso de recibir información secreta o restringida en el correo corporativo, se recomienda:

Poner una etiqueta de color en el Outlook. Es una herramienta que le permite identificar los mensajes a simple vista.

Verificar los nombres de los destinatarios si debe renviarlos al interior, por error puede enviar el correo a un nombre similar.

Si es información secreta o restringida marcar el asunto para que los destinatarios lo tengan en cuenta.

Controles a los Correos electrónicos fuera de la red de la empresa.

Si se debe enviar información secreta o restringida al exterior de la red de la empresa:

Enviar los documentos adjuntos con clave de acceso. No enviar la clave en el mismo correo.

Indicar la clave por teléfono; o enviarla en otro correo y "modificarla". Por ejemplo, la clave que envía es *gentecorporativa*, la clave real es g3nt3*3c0rp0r@t1V@

No indicar en el asunto que se está enviando información secreta o restringida

No envíe información de la empresa por los correos personales.

Si la información a enviar excede el tamaño del correo de la empresa, enviar varios mensajes.

Controles para implementar en las contraseñas.

Se deben crear contraseñas fáciles de recordar y difíciles de adivinar

Construirlas con caracteres alfanuméricos y especiales (# - $ - % - *)

Deben tener mínimo 8 caracteres

Utilizar caracteres diferentes, no consecutivos ni idénticos.

Memorizar la contraseña y no divulgarla nunca

Cambie las contraseñas periódicamente

Controles para construir una contraseña segura:

1. Seleccionar una frase y tomar la primera o última letra de cada palabra y agregar caracteres especiales y alfanuméricos.

Frase: "La Gente corporativa es Gente Pila"
Clave: **Lge%Cgp%99**

Frase: "Oh gloria inmarcesible, oh júbilo inmortal"
Clave: **Ogioji18**

Seleccionar las consonantes de una palabra y establecer un orden, agregar caracteres especiales y alfanuméricos.
Palabra: crucigrama
Clave: ***crcgrm23***

Reemplazar las vocales por números. Clave Murciélago: a = 4; e = 3; i = 1; o = 0; u = otro número

Seleccionar dos palabras y unirlas por caracteres especiales y alfanuméricos.
Frase: Soy Feliz
Clave: **S0y%f3l1z57**

Utilizar la letra «ñ» y tildes, para hacer más difícil la captura de la clave.

No utilice combinaciones obvias de teclado. Ejemplo “1q2w3e4r”.

No utilice claves secuenciales. Ejemplo: asdfghjk – zxcvbnm

Controles para los Sitios Web no apropiados y correo no solicitado (SPAM)

Los funcionarios de la empresa no deben acceder a sitios Web que:

Contengan o distribuyan material que es objetable en el lugar de trabajo.

Sitios web para descargar música o videos.

Sitios web que contienen imágenes y material pornográfico explícito.

Sitios web que promuevan la actividad ilegal.

Sitios web que promuevan la intolerancia.

En el caso de recibir correo no solicitado (SPAM). No lo abra, cópielo en otro correo y repórtelo al departamento de sistemas de la empresa.

Para identificar si el sitio web está utilizando una conexión segura, se debe buscar el icono de un candado en el navegador web. Este indica que se está utilizando un cifrado SSL (Secure Sockets Layer).

Consulte la dirección en el navegador web. Si la dirección URL es "https:" en vez de sólo "http:", está utilizando la tecnología SSL.

Identificar el sello de seguridad del sitio web

Controles en la información publicada en redes sociales y chat:

Cuidar los datos personales. Nunca se debe publicar:

La dirección de la casa ni el teléfono
El número de cédula, fecha de nacimiento
El lugar de trabajo
El nombre del colegio de los hijos
Fotos de la casa, el carro, la placa.
Planes de vacaciones
Revisar la configuración de privacidad
Evitar comentarios personales o del sitio de trabajo.
En lo deseado no publicar fotografías
Aceptar como amigos a personas conocidas y de "confianza"

Controles para resguardar activos de información y tener un puesto de trabajo seguro.

Con el computador:

Interiorizar la cultura de bloquear la pantalla al dejar el puesto: presionar "Windows" y "L"

Usar la guaya para la seguridad del computador portátil. No dejarlo desasegurado «ni por un minuto».

Mantener los documentos corporativos en directorios de la red, especialmente la información Secreta y Restringida

Use contraseñas fuertes

Con las USB y discos extraíbles:

Se debe implementar en la empresa la política de no permitir almacenar ni transportar información Secreta o Restringida.

Establecer sanciones para los funcionarios que dejen conectados estos dispositivos al computador o sobre el escritorio.

Borrar el contenido después de usarlos.

Con el escritorio y en las conversaciones

Evitar dejar documentos impresos sobre el escritorio. Guardar con llave documentos Secretos o Restringidos.

Guardar los documentos, USB, discos en cajones bajo llave., al igual que los objetos personales tales como cartera, celular, billetera, etc.

No hablar de asuntos confidenciales frente a extraños o en aeropuertos, restaurantes, ascensores, chats, por teléfono, etc.

Con la aplicación de los anteriores controles se espera lograr un avance en términos de seguridad informática al interior de las organizaciones, teniendo en cuenta que la capacitación y culturización del recurso humano es clave para fortalecer y perfeccionar la gestión segura del ciclo de la información.

Conclusiones.

Todas las organizaciones están expuestas a amenazas y vulnerabilidades a sus sistemas de información.

Una amenaza puede constituirse como cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan. La pérdida o fuga de información es una de ellas

Según las referencias consultadas y el concepto de múltiples autores, queda claro, que la fuga de información ocurre cuando un sistema diseñado para realizar tareas que no deben ser observadas por un atacante, revela parte de esa información debido a errores en procedimientos o controles establecidos por la organización.

La carencia y/o debilidad para la implantación de políticas, protocolos y procedimientos, constituye un riesgo para la organización y para las personas que la conforman.

En términos organizacionales, el riesgo a asociado a la fuga o perdida de información, se denomina Riesgo operativo, y consiste en básicamente en “la pérdida (de cualquier tipo) causada por falla o insuficiencia de procesos, personas y sistemas internos, o por eventos externos”.

Actualmente existe un sinnúmero de metodologías para la medición del riesgo operativo asociado a eventos de perdida. En los últimos años la mayoría de las organizaciones importantes están empezando a utilizar metodologías estructuradas y avanzadas para la

identificación y cuantificación del Riesgo basadas principalmente en cuestionarios, cuadros de Control internos y matrices de frecuencia y criticidad.

Las metodologías planteadas y aplicadas en actualmente, se clasifican en dos grandes categorías: los enfoques descendentes (Aproximación por Datos Externos, la aproximación CAPM, el Indicador Básico y la Aproximación Estandarizada) y los enfoques ascendentes (Modelos Estadísticos y Modelos Causales).

La Metodología RAM-SI, está basada en un modelo estadístico el cual hace parte del enfoque ascendente.

Los modelos estadísticos trabajan mediante información histórica sobre la frecuencia y la cantidad de los eventos de pérdida para estimar una medida del nivel de riesgo al que está expuesta la empresa u organización.

La metodología diseñada, integra la frecuencia (probabilidad) y la cantidad de los eventos de pérdida (consecuencias), para estimar el riesgo asociado a un evento de pérdida o fuga de información.

El procedimiento planteado en la metodología diseñada, se puede calcular el nivel de riesgo de una manera rápida, sencilla y de bajo costo para la organización, a diferencia de otras metodologías que requieren de altas inversiones en términos humanos y financieros, pero que desde la concepción de la cultura de la seguridad es muy poco lo que aportan.

La Metodología RAM-SI, se propone como un apoyo corporativo a las políticas y protocolos establecidos en la empresa en términos de seguridad informática, ya que su principal objetivo es asegurar la gestión segura del ciclo de la información.

Solo mediante la identificación, medición y evaluación del nivel de riesgo asociado a eventos de fuga de información se puede asegurar el ciclo de la información, ya que lo que no se mide no se puede gestionar, además teniendo en cuenta los resultados de

Con la aplicación del procedimiento propuesto en RAM-SI, se puede clasificar la información dependiendo del nivel de riesgo resultante de la evaluación según el caso en: Secreta, Restringida o General.

La clasificación de la Información, permite, formular controles direccionados a mitigar el nivel de riesgo asociados a eventos de fuga de información.

Los controles formulados en el presente artículos son de fácil entendimiento y aplicación por los funcionarios de las empresas. La implementación de los mismos debe ser una directriz corporativa, así mismo, los sucesos ocurridos por la carencia en la ejecución de los mismos debe conllevar a tomar acciones radicales al interior de la organización.

La Metodología diseñada, además de estimar el nivel de riesgo, clasificar la información y establecer controles para la mitigación de las amenazas, está abierta a ser fortalecida, mediante el desarrollo de otros proyectos asociados a la misma, tales como: Utilizar programas computarizados para modelar el riesgo operativo mediante la aplicación del procedimiento RAM.SI.

La norma ISO 17799 y ISO 27001 brindan un marco de referencia general para la identificación, tratamiento de riesgos en términos de amenazas a la seguridad informática, pero no especifican las herramientas a utilizar para una clasificación rápida y ágil de los riesgos asociados en específico a la fuga o perdida de información. La Metodología diseñada, es única en cuanto a poner en práctica los conceptos y las recomendaciones establecidas en estos estándares, lo que establece un gran aporte en términos de seguridad informática a nivel organizacional.

Agradecimientos

Este proyecto está Dedicado a Dios que me dio salud, y paciencia para poder lograr cumplir mis objetivos.

A mi madre María Consuelo, gracias por su amor, por su paciencia, por sus palabras de ánimo y sus expresiones de cariño, gracias… porque sin su apoyo no habría alcanzado mi objetivo.

A mis hermanas Ruby, Diana quienes siempre me brindaron una voz de aliento cuando decaía y pensaba que no lo lograría.

Y a Patricia... quien le da alegría a mis días.

Biografía

Oscar Humberto Niño Ramírez, Ingeniero de Sistemas por la Universitaria de Investigación y Desarrollo – UDI, Bucaramanga, promoción (2008), aspirante a Especialista en Seguridad Informática de la Universidad Pontificia Bolivariana.

Ha sido docente en programación del lenguaje PHP, desarrollo web, actualmente se desempeña como ingeniero en la Universidad Nacional Abierta y a Distancia –UNAD.

Referencias

CABRERA, R. y GARCIA R. (2010) KPMG International Data Loss Barometerhttp [Disponible en línea]. URL:http://www.bsecure.com.mx/ulti osarticulos/crecen-fugas-de-informacion por-hackeo-y-perdida-de-dispositivos po

Comité de Basilea (2002). Basel Committee on Banking Supervision (marzo, 2.003). The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected.

FORRESTER (2011). The value of Corporate Secrets. How Compliance And Collaboration Affect Enterprise Perceptions Of Risk. March. Disponible en: http://www.rsa.com/document.aspx?id=10844 (Consultado: 05-06-2012)

GÓMEZ V. Alvaro. Tipos de ataques e intrusos en las Redes informáticas[EnLínea]: http://www.mundointernet.es/IMG/pdf/ponencia95.pdf

HIWATASHI, Junji (septiembre, 2002). Solutions on Measuring Operational Risk. Capital Markets News.

ISO 17799-2005 Information security management a Stope view with six sigma approach. International Journal of Network Management, p. 93.

MENDOZA Luis E. MSc. en ingeniería de Sistemas. Departamento de Seguridad y sistemas. Universidad Simón Bolívar. Caracas, Venezuela 2009

MIERES, Jorge. Debilidades de seguridad comúnmente explotadas. Ingeniería Social. Evil Fingers. Pag 8. Enero de 2009.

PONEMON INSTITUTE LLC. The Cost of a Lost Laptop, Sponsored by Intel Corporation. [En línea]. :URL: http://communities.intel.com/docs/DOC-3076

ROEHR, Ancus (2002). Modelling Operational Losses. Research Quarterly, Vol. 5, No.2.

SECURITY ABSURDITY: The complete, unquestionable and total failure of information security. Noam Eppel, Vivica Information Security Inc.

SMITHSON, Charles W. Managing Financial Risk. 3 Ed. Mc Graw-Hill. 2006.