La seguridad informática una política que funciona o no funciona gracias al activo "humano"

Arévalo Pinzón Edwin Fernando
Efap1024@yahoo.es
Universidad Piloto de Colombia

Abstract - Observation given to more general policies of companies not raises awareness of the importance of information security within their organizations devoted not only provide technology services.

Resumen - Observación dada a las políticas más genéricas de las empresas que no se concientizan en la importancia de la seguridad informática dentro de sus organizaciones tan solo por no dedicarse ofrecer servicios tecnológicos.

Índice de Términos — Riesgo, Administración de riesgo, Matriz de riesgo, Política, Activo, Información.

I. INTRODUCCIÓN

En la actualidad, existen dos elementos importantes a tener en cuenta que incrementan la relevancia de brindar una adecuada seguridad a la protección de la información de las empresas por parte de las organizaciones: las categorías crecientes de la información en las compañías y el aumento de los riesgos a la que las mismas se ven expuestas.

Las organizaciones logran llegar al éxito o al fracaso solamente por la manipulación de la información que contienen, lo que ha llevado a que ésta sea considerada un activo cada vez más representativo, aun cuando no es posible llegar a cuantificarlo exactamente. Y es lo dicho anteriormente que impide que la información se vea reflejada en una línea de balance, ya que cumple todas las condiciones restantes de un activo.

Descrito lo anterior, se requiere establecer controles eficientes a la hora de resguardar los activos – al igual que se hace para los bienes tangibles – para los datos.

Hoy en día la interacción entre usuarios, clientes, y proveedores entre otros es generalizado en un procesamiento descentralizado, ambientes cliente-servidor e ingresos al sistema de usuarios que no pertenecen a la empresa (usuarios, clientes, proveedores, etc.).

La dinámica actual de los servicios ofrecidos por las organizaciones hacia sus clientes trae inmersas nuevas oportunidades de negocios, mayor eficiencia a las operaciones y/o menores costos de transacción, lo que implica nuevos y más confusos riesgos que se deben tratar y mitigar, o por lo menos considerar.

Al establecer la matriz de riesgo y el plan de tratamientos del mismo, el valor creciente de la información y las nuevas tecnologías dinámicas, se impacta directamente en la ecuación costo-beneficio, volviéndola más amplia y robusta.

Para incrementar el nivel de evaluación de riesgos, si las organizaciones adicional a sus procesos propios, manejan información de terceros, no sólo debe lograr procesar la misma de una manera segura, sino también la información de ese tercero bien sea proveedor o cliente, para impedir pérdida reputacional de imagen o acciones legales en su contra, ya que la falta de seguridad o la apariencia de falta de seguridad pueden actuar como un impedimento para concretar negocios.

A continuación se quiere brindar un desarrollo sobre el concepto básico, implicaciones y técnicas de seguridad en el marco previsto de acuerdo a los objetivos de la especialización

A. Concepto de seguridad

La seguridad tiene tres objetivos principales:

Confidencialidad: Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. [1]

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. [2]

Disponibilidad: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. [3]

Y como complementos a la triada conceptual de la seguridad informática se presentan las siguientes propiedades:

Autenticación**:** Es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.
Esta propiedad se puede considerar como un aspecto de la integridad -si está firmado por alguien, está realmente enviado por el mismo- [4]

No repudio:

- ✓ No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.
- ✓ Prueba que el mensaje fue enviado por la parte específica.
- ✓ No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.
- ✓ Prueba que el mensaje fue recibido por la parte específica. [5]

Para que la organización cumpla con estos objetivos esta requiere tener establecidos procedimientos de seguridad de información convenientes con su core de negocio, formalmente definidos y ampliamente publicados.

Para poder cumplir con estos procedimientos se requieren actividades que aporten significativamente a fortalecer controles para reducir representativamente el impacto causado por alguna amenaza que ha sido explotada por medio de una vulnerabilidad existente, para ilustrar esto se muestra la figura 1 [6]

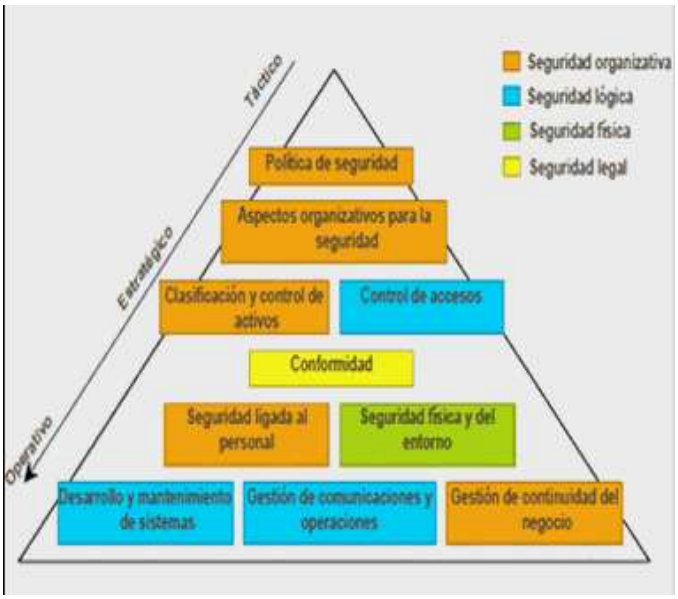

Fig. 1 Estructura piramidal (Dominos de control) [6].

A través de los tiempos se ha logrado establecer que la amenaza más relevante para la información de las organizaciones, está dentro de las mismas, como lo son los accesos no autorizados o indebidos llevados a cabo por funcionarios de la misma compañía, adicionando los ataques por malware informáticos accionados intencionalmente o por falta de conocimiento del personal interno.

A pesar de estas amenazas "*pasivas*" las organizaciones se enfocan más en prevenir los agentes externos dado el daño reputacional público ante los medios de comunicación que pueden sufrir por causa de ataques realizados por crackers o hackers, lo que conlleva una mayor sensibilización por este tipo de delitos a las personas involucradas en la protección de la información dentro de las compañías.

Lo conveniente dentro de las organizaciones debe ser, llevar a cabo un formal análisis de riesgos que arroje resultados concretos sobre los mismos con el fin de clasificarlos por su nivel de criticidad, lo cual establecerá sí el nivel máximo a exposición, se encuentra adentro o afuera de la compañía, o, se requiere tener en cuenta otro tipo de amenazas, que logrará centralizar mejor las acciones preventivas y de mitigación, desarrollando procedimientos de seguridad más puntuales.

Los procedimientos básicos de seguridad iniciales a tener en cuenta, sin importar el nivel de tecnología que tenga la empresa deben ser:

- ✓ Autenticación
- ✓ Autorización
- ✓ Gestión de los sistemas
- ✓ Auditoria y log´s
- ✓ Mantenimiento de datos

En todo caso, cualquiera de los procedimientos se administran con herramientas o técnicas propias de seguridad, las cuales van directamente relacionadas o dependientes de la tecnología utilizada por cada organización, a medida que el desarrollo tecnológico avanza se requieren metodologías de seguridad que permitan gestionar el control de nuestros datos y una de las mejores técnicas es establecer una política de seguridad.

B. Política de seguridad.

La política de seguridad informática es el canal de comunicación entre los gerentes y los usuarios finales, esta no es una descripción procedimental técnica respecto a mecanismos de seguridad ni tampoco una carta de navegación para efectos legales o sanciones disciplinarias hacia los funcionarios, debe ser sin lugar a dudas una descripción de lo que la alta gerencia desea proteger y porque de esto.

El objetivo específico al establecer una política de seguridad de información es explicar el alcance y posicionamiento de la compañía con relación a la misma, adicional es la base para el desarrollo de todos los controles y procedimientos de seguridad.

Se requiere contar con un documento formalmente elaborado al respecto, el cual debe ser difundido a todos los niveles de la empresa, esta política no puede ser solo una carta intencional, como tampoco es necesario un alto grado de detalle o profundidad, estas generalmente contienen las practicas que serán adoptadas al interior de la empresa, las cuales previamente serán revisadas y de ser necesario actualizadas con una periocidad conveniente para la organización.

A manera de ejemplo sin ser muy profundos en las recomendaciones, las políticas deben comprender:

- ✓ Definir claramente el concepto de seguridad de información, sus objetivos y su importancia al interior de la compañía.
- ✓ Mostrar el compromiso por parte de la junta directiva con la seguridad de la información y sus objetivos.
- ✓ Definir los procedimientos respecto al acceso a la información
- ✓ Clara asignación de roles y responsabilidades inherentes al tema

- ✓ Contar con instrucciones documentadas para diseñar normas y procedimientos al respecto que permitan:
  - Organización de la seguridad tanto para el hardware, el software, el ambiente físico, las personas y el ambiente.
- ✓ Clasificación de la información y su control
- ✓ Planes de contingencia
- ✓ Planes de continuidad de negocio
- ✓ Gestión de los sistemas del negocio, asignación de usuarios y privilegios de los mismos.

Con base en lo anterior y a partir de las políticas se podrá dar inicio a desarrollar las normas para posteriormente los procedimientos que serán la guía para el desenvolvimiento de las actividades.

Para lograr ilustrar mejor la estructura de las políticas, normas y procedimientos de la seguridad de la información al interior de la organización se presenta la siguiente figura [7] como una visión macro de cómo debe ser comprendida dicha estructura.

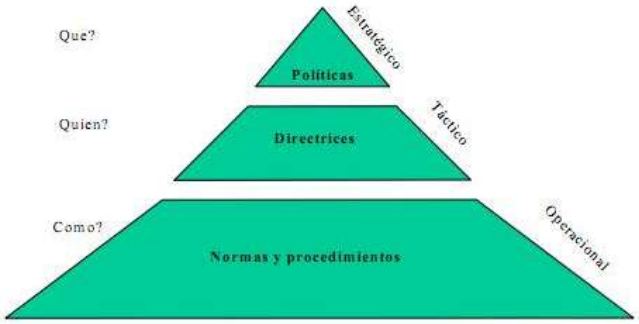

Fig. 2 Políticas, Planes y Procedimientos de seguridad [7].

¿Cómo desarrollar una política de seguridad? [8]

Identifique y evalúe los activos: Qué activos deben protegerse y cómo protegerlos de forma que permitan la prosperidad de la empresa:

- ✓ Hardware: terminales, estaciones de trabajo, procesadores, teclados, unidades de disco, computadoras personales, tarjetas, router, impresoras, líneas de comunicación, cableado de la red, servidores de terminales, bridges.
- ✓ Software: sistemas operativos, programas fuente, programas objeto, programas de diagnóstico, utilerías, programas de comunicaciones.
- ✓ Datos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.
- ✓ Personas: usuarios, personas para operar los sistemas.
- ✓ Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

Identifique las amenazas: ¿Cuáles son las causas de los potenciales problemas de seguridad? Considere la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran. Estas amenazas son externas o internas:

- ✓ Amenazas externas: Se originan fuera de la organización y son los virus, intentos de ataques de los hackers, retaliaciones de ex-empleados o espionaje industrial.
- ✓ Amenazas internas: Son las amenazas que provienen del interior de la empresa y que pueden ser muy costosas porque el infractor tiene mayor acceso y perspicacia para saber dónde reside la información sensible e importante.
- ✓ Evalué los riesgos: Debe calcularse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tienen el potencial para causar mucho daño. El costo puede ser más que monetario, se debe asignar un valor a la pérdida de datos, la privacidad, responsabilidad legal, etc.
- ✓ Asigne las responsabilidades: Seleccione un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa. Los principales integrantes del equipo serían el administrador de redes, un asesor

jurídico, un ejecutivo superior y representantes de los departamentos de Recursos Humanos y Relaciones Públicas.

- ✓ Establezca políticas de seguridad: Cree una política que apunte a los documentos asociados; parámetros y procedimientos, normas, así como los contratos de empleados. Estos documentos deben tener información específica relacionada con las plataformas informáticas y tecnológicas, las responsabilidades del usuario y la estructura organizacional. De esta forma, si se hacen cambios futuros, es más fácil cambiar los documentos subyacentes que la política en sí misma.

- ✓ Implemente una política en toda la organización: La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad y reconocer quién es el propietario de los sistemas y datos específicos. Éstas son las tres partes esenciales de cumplimiento que debe incluir la política:

Cumplimiento: Indique un procedimiento para garantizar el cumplimiento y las consecuencias potenciales por incumplimiento.

Funcionarios de seguridad: Nombre individuos que sean directamente responsables de la seguridad de la información.

Financiación: Asegúrese de que a cada departamento se le haya asignado los fondos necesarios para poder cumplir adecuadamente con la política de seguridad de la compañía.

- ✓ Administre el programa de seguridad: Establezca los procedimientos internos para implementar estos requerimientos y hacer obligatorio su cumplimiento

C. Desarrollo de normas.

Después de establecer la política, se podrá dar inicio a desarrollar las normas, las cuales son un grupo de lineamientos, controles, reglas y buenas prácticas entre otras, con la intención principal de respaldar la política de seguridad y sus objetivos, por medio de roles claramente definidos a través de un manual de funciones y responsabilidades, alcance de los puestos de trabajo, segregación de funciones, entre otras técnicas, todos estás encaminadas a cubrir y resguardar el objetivo principal de la política de seguridad.

Para tal fin es posible y de gran ayuda tomar como referencia la norma ISO/IEC 27001:2013 [9] que implementa controles y directrices para la organización, adicional de que puede ser certificable, lo que significa que a través de la revisión de una entidad certificadora confirma que la seguridad de la información ha sido implementada en la empresa en cumplimiento de la norma ISO 27001 lo que genera un plus de negocio ante el mercado, posible clientes potenciales, y mejoras en la relaciones comerciales con los ya existentes.

Esta norma no solo es un sello de garantía ante el mercado objetivo sino que permite ser mejor organizacionalmente a través del tiempo gracias a la implementación del ciclo de Deming como se ilustra en la figura 3 [11]

Fig 3. Descripción del ciclo de mejora continua

D. Procedimientos

Un procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los

procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización [12]

Los procedimientos indican **como** implementar al interior de las áreas clave del negocio la generalidad de las políticas definidas transversalmente en la entidad, como base del desarrollo de las necesidades de protección, la forma de llevarlas a cabo, tiempos, recurso humano, y canales o recursos a utilizar.

Habitualmente se trabaja sobre los recursos y en concordancia a los niveles de seguridad actuales, se lleva a cabo un programa de seguridad informática que permita visualizar paso a paso las actividades a realizar, con la finalidad de llegar a niveles superiores.

Esto finalmente se convierte en actividades del día a día, de las rutinas laborales que desarrollan las personas involucradas en los procesos de la seguridad informática al interior de las organizaciones como ejemplo se describen algunas actividades a considerar como referentes:

- ✓ Políticas del mínimo privilegio (asignar o eliminar el acceso de los funcionarios a las tecnologías de información y como controlarlo.
- ✓ Establecer perfiles de trabajo acorde con sus funciones.
- ✓ Autorizar o negar servicios a los funcionarios. (Ejemplo: Correo electrónico personal o acceso a internet)
- ✓ Políticas de manejo y gestión de claves de acceso a los sistemas de información.
- ✓ Políticas de Back-up
- ✓ Cláusulas de confidencialidad.
- ✓ Planes de trabajo en Auditoria
- ✓ Política de manejo de log´s
- ✓ Derechos de autor en caso de desarrollo de software
- ✓ Contratos de mantenimiento de los sistemas
- ✓ Planes de recuperación
- ✓ Planes de contingencia
- ✓ Planes de continuidad de negocio
- ✓ Mapas de riesgos
- ✓ Planes de seguridad industrial

II. CONCLUSIONES

Es claro que los sistemas informáticos funcionan según como se hayan concebido, para los fines y con los parámetros que previamente el diseñador o arquitecto estableció, así las cosas, y, si solo se dependiera de los sistemas, los sistemas de información serían perfectos, como en dichos procesos interviene el recurso humano se requiere elaborar o documentar procesos que eviten el error humano.

Como se describió en este artículo el mejor documento hasta ahora desarrollado para evitar estas inconsistencias humanas y de desarrollo, es la política de seguridad de la información, donde se concientiza a la organización que la clave del éxito consiste en desarrollar un programa efectivo de seguridad de la información que permita recordar que las políticas, estándares y procedimientos son un grupo de documentos interrelacionados que a su vez es lo que dificulta su desarrollo, resaltando que sin lugar a dudas es una herramienta poderosa cuando se pone en práctica.

Muchas empresas en su esfuerzo por simplificar el proceso de desarrollo de las políticas ignoran dicha interrelación, sin embargo, las mismas relaciones son las que permiten que las organizaciones puedan exigir y dar cumplimiento a los mismos requerimientos establecidos de seguridad.

Muchas empresas diseñan e implementan políticas de seguridad no por necesidad propia de la empresa, sino por necesidades del mercado que solicitan desarrollo e implementación en este tema, especialmente por regulaciones legales, jurídicas o contractuales.

Para lo cual es claro que se requieren algunos recursos adicionales, que representa inversión la cual se hace perentorio ver como una inversión y no como un gasto; para cumplir eficientemente con el uso de este nuevo presupuesto se sugiere a la hora

de evaluar las necesidades de inversión tener en cuenta:

- ✓ Saber qué información se tiene y en donde está.
- ✓ Reconocer el valor de la información que se tiene y el costo de volver a generarla en caso de pérdida.
- ✓ Identificar y establecer los perfiles de usuarios que están autorizados para acceder a la información y que pueden hacer con la misma.
- ✓ Identificar la disponibilidad de la información, y establecer la misma en caso de pérdida.

Por todo lo descrito anteriormente se llega a la conclusión que el recurso humano es el motor de las organizaciones y se hace necesario capacitar al personal con el fin de que tomen un papel activo dentro de la empresa con la finalidad de aplicar su conocimiento en las diversas tareas que realiza dentro y fuera la empresa con el propósito único de proteger de una forma adecuada la información que se le confía como si fuera la propia

REFERENCIAS

[1] WIKIPEDIA, Concepto de confidencialidad [Online] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad

[2] WIKIPEDIA, Concepto de integridad [Online] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Integridad

[3] WIKIPEDIA, Concepto de disponibilidad [Online] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Disponibilidad

[4] WIKIPEDIA, Concepto de Autenticidad [Online] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Autenticaci.C3.B3n_o_autentificaci.C3.B3n

[5] WIKIPEDIA, Concepto de No repudio [Online] http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#No_repudio

[6] Figura 1. (Estructura piramidal por dominios de control) http://www.monografias.com/trabajos42/iso-informatica/iso-informatica2.shtml.

[7] Figura 2. (Políticas, Planes y Procedimientos de seguridad) http://seguridadinformaticaufps.wikispaces.com/Politicas%2C+Planes+y+Procedimientos+de+Seguridad

[8] Hermoso Aurelio, Implantación de una política de seguridad de los sistemas de información.

[9] ISO/IEC 27001 http://www.iso27001standard.com/es/que-es-iso-27001/

[10] El ciclo de Deming http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-

[11] Figura 3. Ciclo de trabajo de mejora continua PDCA http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

[12] Gomez Vieites Alvaro, Enciclopedia de la seguridad informática pág. 25

Edwin Fernando Arévalo Pinzón, Ingeniero Industrial Universidad Autónoma de Colombia, estudiante de la "Especialización en Seguridad de la Información" Universidad Piloto de Colombia 2014.