Metodología para la prevención de riesgos informáticos en una Pyme de la ciudad de Cali

Informating risk prevention in a Cali's city Pyme

Fecha de recepción: Febrero 15 de 2016 Fecha de aceptación: Mayo 10 de 2018

Brian Andrés Medina Cerquera
Fundación Universitaria Católica Lumen Gentium

Resumen

En la actualidad uno de los principales problemas que se presentan a los responsables de las áreas de sistemas en el ámbito organizacional, es el manejo acertado de los recursos y el aseguramiento del manejo correcto de los mismos, garantizando así, la integridad de la información.

A continuación, se exponen las razones fundamentales que justifican la implementación de una metodología para la prevención de riesgos informáticos en las pyme, dicho desarrollo por supuesto, para dicho desarrollo y aplicación se deberán tomar en consideración las características fundamentales de cada organización.

El trabajo de investigación base del presente artículo se desarrolló en una empresa dedicada al *outsourcing* en salud y en cuya experiencia se resaltan las siguientes conclusiones principales: 1) la información es uno de los más importantes bienes de una compañía. 2) en esta empresa no existían medidas claras para salvaguardar la información como su activo más importante, probablemente porque los costos que esto implica superan las posibilidades presupuestales de la compañía y porque adicionalmente no existe una cultura que respalde dicho comportamiento al interior de la organización. 3) durante la implementación de la metodología, es fundamental sensibilizar al personal de la compañía, pues la protección informática es tarea de todos, en la media que todos los miembros de la organización son al tiempo responsables y posibles factores de riesgo aun sin proponérselo.

Palabras claves: Riesgo informático, delito informático, procedimientos de seguridad, normatividad, políticas.

Abstract

At the present time one of the fundamental problems for you lead them and people in charge of the units of computer science of the companies are to manage to obtain resources to assure the digital assets, next expose the fundamental reasons that they justify the execution of a project of consultancy of computer science security for the platform of any organization. For the presentation of the information will be to some topics of

the computer science security like variables of decision and their corresponding situation within each organization.

Instruments of information harvesting were applied where it fundamentally analyzed the conditions of security of the information in a Pymes from Santiago de Cali to the sector of outsourcing, where they were obtained like more excellent conclusions: 1) the information is one of the most important assets for the company, 2) are not applied in our average documented alternatives to safeguard this assets; probably because of the cost that implies for the Pymes, to acquire a tool that allows to develop this activity them; in addition to a culture - hardly born- to design and to apply policies of computer science security and 3) the education to all the personnel used or directive of this sector, with respect to the importance of the security of the information and the fulfillment of the policies of computer science security, plays a roll of vital importance during the implementation of the process of protection of the information; besides to ensure in a high percentage the success of the same one.

Keywords: Informatics risk, Informatics crime, Safety procedures, legislation, policies.

Introducción

Algunos autores han definido las Políticas de Seguridad como el grupo de reglas y regulaciones que dictan cómo una organización protege, maneja y distribuye información sensible. Sin embargo, éste concepto debe abarcar una perspectiva más completa que considere la definición de una Política de Seguridad que determine el qué se quiere hacer en materia de seguridad en la organización con el objeto de, a partir de ello decidir mediante un adecuado plan de implementación el cómo se alcanzarán en la práctica los objetivos fijados.

Esta investigación se lleva a cabo con el fin de desarrollar una herramienta que permita cumplir con lo establecido en dichas Políticas de Seguridad, especialmente en el marco de las pequeñas y medianas empresas, las cuales no solo no disponen de los recursos tecnológicos y sistemáticos para contrarrestar los delitos informáticos, sino que también carecen de una concepción clara respecto a la importancia de la intervención en estos aspectos.

Con este trabajo se pretende brindar una opción de vigilancia y control informático a este sector de la economía, favoreciendo la optimización de su desempeño y su posición en el medio empresarial.

Materiales y métodos

El documento: metodología para detectar y prevenir riesgos informáticos en una pyme de la ciudad de Cali se realizó con el fin de brindar una herramienta eficaz para aquellas nacientes empresas que a pesar de contar con recursos limitados por su tamaño y capacidad productiva, igual están obligadas a protegerse de los riesgos informáticos que pueden afectarlas tanto como a cualquier otra organización.

Esta metodología se realizó partiendo de un estudio detallado de la realidad de una pyme dedicada a prestación de servicios de salud con el modelo de outsourcing. Se encontró que dicha empresa aunque contando con algunos recursos para la gestión informática, adolecía de una estructura que le permitiera realmente proteger su información de los riesgos informáticos y ambientales a los que está constantemente expuesta.

En el desarrollo del trabajo tanto en el campo como en su componente teórico, se tuvo en consideración el estado del arte nacional en cuanto a seguridad informática, es así como se consultaron entre otros, varios estudios publicados por la Asociación Colombiana de Ingenieros de Sistemas, ACIS, en donde se evidenció que lo encontrado en la expresa de estudio es un reflejo de la realidad nacional en la pequeña y mediana empresa con respecto al tema específico de la seguridad informática.

La metodología que a continuación se desarrolla está basada en la Norma ISO 27001 estándar internacional que adopta la estructura ISMS, que corresponde a las siglas en inglés del Sistema Administrativo de Seguridad de la Información (Information Security Management System).

Se adopta también el modelo "Plan-Do-Check-Act" (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:

- **Plan** (Establecer el ISMS): Implica, establecer la política ISMS, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguri-

dad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- **Do** (Implementar y operar el ISMS): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.
- **Check** (Monitorizar y revisar el ISMS): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
- **Act** (Mantener y mejorar el ISMS): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS[1].

Objetivos

General

Desarrollar una metodología para prevención de riesgos informáticos cuyas características la hagan económicamente viable y fácilmente implementable en una empresa con las características de una Pyme.

Específicos

- Diseñar procedimientos administrativos adecuados para la prevención de riesgos informáticos en una Pyme.
- Establecer un plan de implementación de fácil comprensión y manejo por parte de los funcionarios de la empresa a intervenir.
- Generar estrategias de evaluación y seguimiento de los procesos instaurados.
- Diseñar un plan para la identificación de debilidades y establecimiento de ajustes al sistema desarrollado.

Planeación

Identificación de la organización

Para empezar, se debe identificar todos aquellos aspectos de la organización que son relevantes para la implementación de la metodología de seguridad informática, se requiere especificar lo relacionado con la industria en la cual se mueve la compañía, su tamaño, ubicación, tecnología, estructura y orientación administrativa y gerencial.

Para lo anterior se recomienda seguir lo siguientes pasos:

- Establezca en conjunto con la cabeza de la organización los objetivos y principios que se tendrán en cuenta a lo largo de todo el proceso.
- Indague por los requisitos legales que la organización tiene de acuerdo a su sector de labores y / o los compromisos que en este sentido pueda haber adquirido contractualmente.
- Identifique las directrices y procesos llevados a cabo en materia de seguridad informática.
- Determine, en conjunto con la dirección de la organización, los estándares para la valoración de riesgo y cuáles son en el caso concreto de la organización los riesgos aceptables.
- Identifique los procesos clave para la generación y manejo de la información primordial de la empresa
- Establezca claramente cuáles son las áreas clave y los funcionarios encargados de los procesos neurálgicos en materia de seguridad informática en la organización.

Análisis

Identificación de riesgos

Elabore un inventario de los activos involucrados en los procesos de manejo de la información, clasificándolos según su naturaleza, en términos de niveles de riesgo especificando las amenazas a las cuales están expuestos.

Este inventario debe ser complementado con una evaluación de impactos en caso de violación de la seguridad informática de la organización, recuerde que esta labor es importante no solo para el diseño mismo de la metodología sino como información relevante a ser tenida en cuenta en el proceso de sensibilización a los funcionarios involucrados en la generación y manejo de la información.

Valoración de riesgos

A partir de la anterior identificación de riesgos, valore la posibilidad de ocurrencia real de una violación

1 CORLETTI ESTRADA, Alejandro. Análisis de la Norma ISO-27001

a la seguridad informática de la Compañía, identificando así cuáles son las áreas o activos con mayor nivel de vulnerabilidad.

Verificación de servicios y procedimientos
De acuerdo a lo indagado en materia de procedimientos, verifique por su cuenta si éstos están siendo efectivamente implementados.

Indague con los responsables de estos procedimientos lo relacionado con periodicidad, tiempo de implementación, tanto en la ejecución del procedimiento como en la instauración de la política, y posibles antecedentes referidos a violaciones o alertas de seguridad.

Recuerde tomar en cuenta las medidas que la compañía tenga implementadas en lo referente a seguridad, esto le servirá para identificar además la verdadera funcionalidad de las mismas y si son o no efectivas con respecto al objetivo para el cual fueron creadas.

Determinación de vulnerabilidades
Haga una lista de las vulnerabilidades identificadas, estimando sus niveles de riesgo frente al nivel aceptable, establecido previamente con la dirección de la organización
Tenga en cuenta que esta determinación debe hacerse tomando como base la opinión e información de diversas fuentes primarias y secundarias, remítase a la información documentada y solicite también la opinión de diversos funcionarios involucrados en mayor o menor medida con la operación, no se quede con una sola fuente.

Revisión de las políticas de seguridad y privacidad
Si la organización tiene documentadas sus políticas, remítase especialmente a aquellas relacionadas con seguridad y privacidad de la información. Aunque en muchas organizaciones pequeñas y medianas este tipo de documentación no es muy frecuente, si es posible que existan políticas generales de las cuales Usted. Deberá extractarlo referente a prevención de riesgos informáticos. Esta pude ser una tarea dispendiosa pero necesaria, asesórese y no la pase por alto.

Identificación de posibles acciones
Con base en la información recolectada, pregúntese cuáles podrían ser las posibles acciones para remediar los riesgos identificados y prevenir algunos más que posiblemente se presenten en el futuro, para esto tome en cuenta las siguientes recomendaciones publicadas por el Instituto Colombiano de Normas Técnicas, ICONTEC, en el documento Sistemas de Gestión de la Seguridad de la Información (SGSI):

- Mitigar los riesgos aplicando los controles apropiados.
- Aceptar los riesgos en conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- Evitar riesgos.
- Transferir los riesgos asociados con el negocio, a otras partes, por ejemplo: aseguradoras, proveedores, etc.
- Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
- Preparar una declaración de aplicabilidad.
- Obtener la aprobación de la dirección sobre la propuesta de los riesgos residuales y la autorización para aplicar las medidas vinculadas a la metodología de prevención de riesgos.

Diseño de instrumentos

Una vez finalizada la exploratoria, y para la determinación de las acciones específicas a implementar, es necesario recolectar la mayor cantidad posible de información pertinente, por parte de los involucrados en el proceso, es por esto que el diseño correcto de los instrumentos es de la mayor relevancia.

Se debe elegir el instrumento más adecuado para recoger la información, de acuerdo al enfoque escogido. En general existen dos opciones respecto al instrumento de investigación:

1. Elegir un instrumento ya desarrollado y disponible, el cual se adapta a los requerimientos del estudio en particular.
2. Construir un nuevo instrumento de medición acorde a las necesidades y características particulares de la empresa.

Si bien resulta un procedimiento más dispendioso que el de adaptar un instrumento existente, se recomienda construir un instrumento acorde a la realidad institucional particular, para esto se deben contemplar al menos los siguientes puntos:

1. Listado de las variables a definir.
2. Definición conceptual de las variables
3. Definición operacional de las variables.
4. Elegir o construir un instrumento (determinar los ítems o preguntas).
5. Determinar el nivel de medición de cada ítem.
6. Establecer la codificación.
7. Prueba piloto.
8. Ajuste del instrumento.

Una vez que se ha diseñado el instrumento de recogida de datos, es necesario, aplicar una prueba piloto, que consiste en la realización de algunas pruebas con grupos similares a los que se usarán en la investigación. Su propósito es verificar si el instrumento ha sido correctamente elaborado y si es claro para los entrevistados, los encargados de aplicarlo y el tiempo que tomará aplicarlo.

Con base a la prueba piloto aplicar el instrumento a la muestra seleccionada. Hay básicamente 4 formas de aplicar un instrumento:

1. Aplicación dirigida: es aquella en la que el encargado debe estar presente mientras el encuestado o grupo de encuestados responden por escrito el instrumento.
2. Aplicación mediante entrevista: es aquella en la que el encargado debe aplicar oralmente el instrumento a los examinados de manera individual.
3. Auto aplicación: es aquella que no requiere de la presencia del encargado. En estos casos **él** se entrega el instrumento y se revisa en el momento en que éste le es devuelto.
4. Observación: en este caso el encargado es quien contesta algunas preguntas en función de lo que observa[2].

Una vez recolectada la información mediante la aplicación del instrumento, se debe clasificar la información de manera que sea fácilmente analizable en sus implicaciones, al tiempo que correlacionarla teniendo cuidado de incorporar todos aquellos elementos que han surgido durante el proceso investigativo y que ayuden a elaborar conclusiones sólidas.

Implementación y operación

Una vez efectuado el diagnóstico y establecidas las posibles acciones a tomar en cuenta para remediar las vulnerabilidades encontradas, se debe formular un plan coherente para el manejo de riesgos, que parta de la identificación de la acción administrativa apropiada, las responsabilidades y prioridades en la gestión de los activos informáticos de la organización.

Teniendo en cuenta la necesidad de la participación de diversas personas al interior de la empresa en las diferentes áreas funcionales, se requiere generar un proceso de sensibilización frente a la importancia del control y prevención de riesgos informáticos, teniendo como base los siguientes objetivos:

- Identificar claramente los posibles efectos que para la empresa conllevaría una violación de seguridad de la información en sus diferentes niveles.
- Conocer la importancia de su papel en la cadena de aseguramiento de la información.
- Entender la importancia de sus aportes en todos los pasos de la implementación y funcionamiento de la metodología.

La implementación del plan establecido debe tener en cuenta unos objetivos de control previamente identificados, los recursos económicos disponibles y el apoyo de la dirección en la asignación de funciones y responsabilidades.

En conjunto con la dirección de la empresa, se deben seleccionar y establecer los controles requeridos para salvaguardar la seguridad y privacidad de la información de la compañía. Estos controles deben ser debidamente documentados y difundidos entre los funcionarios de manera que se asegure su adecuado cumplimiento.

Seguimiento

Paralelamente a la implementación del plan de control de riesgos informáticos, se debe implementar un plan de seguimiento que permita:

- Detectar rápidamente los errores o fallas en el sistema.
- Identificar y solucionar con prontitud los posibles incidentes de seguridad.

2 Elementos para la ejecución de una propuesta de investigación. http://www.ninvus.cl/matdocente/tecnicas.htm

- Evaluar el desempeño de las personas involucradas en los procesos de gestión de la información al interior de la compañía.
- Priorizar las acciones a ser desarrolladas de acuerdo a lo establecido en concordancia con las estrategias y directrices generales de la organización.

Es necesario implementar un sistema de revisión periódica de la metodología en su totalidad (al menos una vez al año) debido a los cambios que en el tiempo se puedan generar gracias al crecimiento corporativo, cambio de objetivos estratégicos o cualquier otra eventualidad que afecte la empresa en sus procesos, estructura o niveles de responsabilidad de sus funcionarios.

Como elemento fundamental del seguimiento y en general de todos los procesos vinculados a la metodología, se deben disponer herramientas de documentación y sistematización de los procesos y procedimientos, de los posibles incidentes ocurridos y de las acciones tomadas a raíz de éstas de manera que éstos registros se constituyan en herramienta para la toma de decisiones acerca de la metodología y sus posibles ajusten en el futuro.

Mantenimiento

Una vez efectuado el seguimiento, mediante el cual se identificaron las posibles falencias, debilidades o elementos a renovar, desde lo físico hasta lo lógico, se deberán emprender las acciones correctivas y preventivas a las que haya lugar.

La determinación de las medidas correctivas debe estar apoyada por la documentada a lo largo de su implementación y debe responder a la realidad de la organización, soportada desde la dirección, pues debe responder a los objetivos estratégicos de la misma, fijados a corto y mediano plazo.

Como complemento a las medidas correctivas, se debe notificar a todos los involucrados con respecto a las mismas, es así como se evitarían posibles fallos basados en la ignorancia de los nuevos procedimientos o políticas organizacionales.

Vale la pena recalcar que las medidas a tomar deber estar aladas por la alta gerencia, responsable final de las decisiones que implican cambios de fondo en la organización.

Resultados

En la realización del trabajo de campo, se encontró que la empresa solo contaba con unos pocos niveles de seguridad, los cuales por si solos no cumplían a cabalidad con su tarea preventiva, permitiendo así salvaguardar información valiosa tanto de la organización misma como de sus clientes.

Como resultado del trabajo, se obtuvo una metodología de costo módico, fácilmente adaptable y ejecutable para que una pyme perteneciente a cualquier industria pueda implementar en su interior.

La Corporación Gestión Humana es una Pyme cuya estructura en la ciudad de Cali se encuentra en expansión, infortunadamente dicho crecimiento sin ser debidamente planeado ha generado diversas dificultades logísticas especialmente en lo que a informática se refiere.

Al momento de la llegada del investigador a la Corporación Gestión Humana se identificaron falencias de tipo estructural, tecnológico y procedimental, las cuales se fueron corrigiendo a raíz de la intervención.

Si bien se estaban efectuando esfuerzos por solidificar el área de informática como transversal a todos los procesos de la Compañía, la implementación de la metodología propuesta trajo consigo la oportunidad para poner de relieve la gran importancia que el Área, no solo en lo operativo sino también en lo estratégico.

Como resultado adicional, se reportó igualmente por los encargados del Área de Recursos Humanos, un "alivianamiento" del clima organizacional, en la medida que la instauración de la metodología propuso el acercamiento de los grupos operativos alrededor de los temas de seguridad informática, al tiempo que fue la ocasión de acercar la gerencia a todos los funcionarios, cosa que no era acostumbrada organizacionalmente.

Aunque se propusieron cambios en la plataforma tecnológica, al momento de la finalización de la implementación aún no se conocía de una decisión real al respecto.

Discusión

La seguridad informática es un tema de gran relevancia en la actualidad para todo tipo de compañías, la información es el más valioso activo de las mismas y en esa medida se esperaría que fuera custodiado, a pesar de lo anterior, se observa que en los currículos

de las universidades en las cuales se forma a los gerentes del mañana, el tema de la seguridad informática brilla por su ausencia.

Es claro que lo referente a los aspectos técnicos de dicha seguridad, el diseño de estructuras para la misma, al igual que su implementación exitosa son competencia directa del ingeniero de sistemas, sin embargo, se observa como los tomadores de decisión en la alta gerencia carecen en su mayoría de elementos de contexto para contemplar este como un aspecto a tomar en cuenta en sus planes de negocio, planes estratégicos y presupuestos. La creencia generalizada es que toda entidad debe ser robusta en lo que a plataforma tecnológica se refiere, considerando solo para esto lo que a hardware y software se refiere para el procesamiento de la información, sin embargo, los procedimientos y políticas no acompañan efectivamente este robustecimiento tan necesario para el crecimiento de dichas entidades.

El asunto económico, siempre presente en primer lugar en las decisiones organizativas, no es ajeno al panorama de la seguridad informática pues, si bien se ha empezado a entender por parte de algunos los beneficios de la implementación de estrategias para brindar a sus organizaciones a este respecto, aún falta un buen trecho que andar, no solo porque los recursos económicos siempre son escasos, sino porque la prioridad en la destinación presupuestal no se da al tema informático como una estrategia integral sino como esfuerzos aislados y puntuales para solucionar dificultades presentadas en la coyuntura del día a día.

Conclusión

Las causas de esta situación van más allá de la falta de recursos económicos, tienen que ver con el desconocimiento y con la falta de interés en el tema, lo cual ha generado que en muchas de estas empresas se delegue la responsabilidad sobre esta área a una sola persona quien se convierte en el "dueño" de toda la información, tanto de procesos como de procedimientos, lo que lo perfila como un "dictador" ya que esta responsabilidad única se convierte en conocimiento único y, por consecuencia, en poder único.

Si bien se pretende que las responsabilidades estén claramente delimitadas y que haya responsables concretos sobre los procesos, también se busca que éstos sean de conocimiento general. Esta democratización tiene como resultado inmediato un mejor manejo de los recursos informáticos de la organización, la optimización de esfuerzos y la minimización de riesgos. En otras palabras, se debe hacer partícipe a toda la organización respecto a los procesos adecuados para preservar la información, lineamiento que más allá de la norma debe trascender a la sensibilización sobre las consecuencias que puede acarrear una falla en esta área y el efecto que podría en un momento dado tener sobre todos los integrantes de la organización; no se requieren funcionarios entrenados, se necesitan colaboradores responsables y comprometidos.

No se debe perder de vista además que para lograr el óptimo funcionamiento de éstas herramientas, los gremios empresariales deben diseñar e implementar políticas de seguridad que incluyen las categorías que conforman la denominada Seguridad Informática: en primer lugar la integralidad, confidencialidad y disponibilidad de la información.

Como conclusiones básicas del trabajo, es relevante anotar la desprotección en la cual se encuentran muchas de las pequeñas y medianas, empresas de nuestro medio, lo cual genera un impacto mayor al individual, la suma de los riesgos se configura en una verdadera amenaza a la economía de la región.

Desde el punto de vista interno, cabe resaltar el papel decisivo que la voluntad gerencia cumple en el éxito de la implementación de cualquier proceso o política, pues es desde la cima el mejor lugar para iniciar el proceso de sensibilización de todos los miembros de la organización y, es gracias a su concurso, que es posible destinar los recursos necesarios al cumplimiento de una empresa de esta magnitud e importancia.

El tema de la informática en general no ha tenido una política nacional o un ente regulador. Las normas están desarticuladas y desactualizadas. Nuestra legislación penal, huérfana, como se encuentra aún, en estas materias que no alcanzan, como es evidente a ser cubiertas por los delitos o tipos tradicionales, como la estafa, el hurto, daño en cosa ajena, abuso de confianza y falsedad.

Colombia se encuentra ante un retraso notorio frente a otros países que de tiempo atrás cuentan con una normatividad que respalda los avances y aplicaciones de la informática.

La evolución tecnológica ha permitido la aparición de conductas ilícitas, que al recaer en un objeto material particular puesto que la tradición legal requiere su CORPOREIDAD (Casos perceptibles por los sentidos) imposibilita su adecuación a los tipos penales actuales, esto radica en la originalidad

del bien de la información considerado por la doctrina como bien intangible, diferente de los bienes materiales e inmateriales reconocidos por el derecho. Aquí radica la importancia de la labor del Ingeniero de Sistemas como actor influyente en éste proceso.

Normas y estándares

En primera instancia se listan las organizaciones de orden nacional e internacional encargadas de elaborar las normas técnicas de seguridad informática, al igual que las normas más relevantes de acuerdo a su especialidad. Posteriormente, se presentan de forma resumida las propuestas y recomendaciones referentes a la seguridad de los sistemas de información por parte de distintos y reconocidos organismos internacionales, para al final, se realiza un breve análisis comparativo de las mismas a modo de conclusión.

Organizaciones internacionales que elaboran normas técnicas de seguridad para las tecnologías de la información:

- ISO (International Standardization Organization).
- ITU (International Telecommunication Union).
- CCITT (Consultative Committee International Telephony and Telegraphy).
- IEC (International Engineering Consortium).
- CSASCC (Canadian Standards Association and Standards Council of Canada).
- DoD (Defense Departament).
- IETF (Internet Engineering Task Force)
- RSA
- V & M (Visa and MasterCard Internacional.
- AENOR (Asociación Española de Normalización y Certificación).
- IRAM (Instituto Argentino de Normalización y Certificación).
- INN (Instituto Nacional de Normalización) Chile.
- ONN (Oficina Nacional de Normalización) Cuba.

Algunas normas relevantes en la especialidad de seguridad de la información:

Normas de arquitecturas de seguridad

- ISO 7498 (Modelo Básico de referencia para los Sistemas de Información Abiertos). Modelo de 7 capas.
- ISO 7498-2 (Arquitectura de Seguridad). Servicios de Seguridad, Mecanismos de Seguridad, Relaciones de Seguridad entre capas y Gestión de la Seguridad.

Normas de encriptación y dato.

- ANSI X3.92 (Algoritmo de encriptación simétrico DES).
- ANSI X3.106 (Modos de operación DES).
- ANSI X9.23 (Sector Financiero)

Normas de gestión de llaves.

- ANSI X9.17 (Métodos de generación, distribución, almacenaje y destrucción de llaves secretas)
- ANSI X9.24 (Como la anterior pero para el sector financiero).

Normas de firmas digitales.

- Firma Digital RSA (CCITT X.509 v.3)
- Firma Digital RSA (ANSI X9.31) Hash.
- Firma Digital RSA (ISO 9796) PKS
- Firma Digital DDS (NIST FIPS 186) DSA

Normas de Directorio y Certificación

- CCITT X.500 (ISO-9594-x)
- CCITT X.509 (ISO-9594-8) Autenticación.
- CCITT X.511 (ISO-9594-3) Servicios.
- CCITT X.518 (ISO-9594-4) Modelos.
- CCITT X.519 (ISO-9594-4) Protocolos.
- CCITT X.520 (ISO-9594-6) Atributos.
- CCITT X.525 (ISO-9594-9) Replicados

Norma de Correo Electrónico.

- CCITT X.400. (Sistema de manipulación de mensajes).
- CCITT X.411. (Sistema de transferencia de mensajes MTS).
- CCITT X.420. (Seguridad de los mensajes) (Cuerpo del mensaje cifrado)

NIST (National Institute of Standards and Technology)

El NIST (National Institute of Standards and Technology), organismo dependiente del Departamento de Comercio de Estados Unidos, ha elaborado una

extenso documento sobre políticas de seguridad conocido bajo el nombre "Internet Security Policy: a Technical Guide" (1997) que se complementa con su otra publicación "An Introduction to Computer Security: The NIST Handbook". La guía, que cuenta con 107 páginas, está dirigida a:

- **altos directivos** (para hacerlos consientes de los riesgos e implicaciones del uso de Internet y de la necesidad de asignar recursos y responsabilidades respecto a su seguridad)
- **directivos medios** (que serán los que van a tener que establecer las políticas)
- **bajos directivos y personal técnico** (que necesitan comprender las raíces de las políticas que ellos van a tener que implementar y transmitir a los usuarios).

El término política de seguridad significará para cada uno de ellos cosas distintas, pero que, según el NIST, todas son **componentes de una política de seguridad**:

- **programa estratégico de seguridad** donde se establecen los objetivos y directivas estratégicas de la organización y se asignan responsabilidades
- **políticas específicas** que son las directivas concernientes a temas específicos como la privacidad del email o seguridad del fax
- **políticas específicas-sistema** que son reglas de seguridad aplicadas a los distintos sistemas particulares. Uno de los mayores retos a los que se enfrenta una organización en el establecimiento de una política de seguridad es que ésta no muera en un documento formalmente correcto pero careciente de una implicación real de la organización en su implantación práctica (implantación que debe fundamentalmente afectar la actitud y comportamiento de los usuarios).

Una política de seguridad sienta las bases para la implementación de controles de seguridad que reducen las vulnerabilidades y reducen el riesgo a los que está sometida una organización. Por eso, previamente a su desarrollo, hay que realizar algún nivel de **análisis de riesgos** para determinar los requisitos que debe cumplir la política en función de:

- el **nivel de amenaza** al que se enfrenta la organización y la visibilidad de la organización al mundo exterior
- la **sensibilidad** de la organización a las consecuencias de los potenciales incidentes de seguridad
- **aspectos legales** o regulatorios que marquen niveles formales de análisis de riesgos

A partir del nivel de amenaza/visibilidad y la sensibilidad de la organización se establece el **perfil de riesgo/protección** (bajo, medio o alto) que debe asegurar la política y que puede variar según departamentos o servicios.

La guía del NIST dedica la mayor parte de su contenido a los principales requisitos de negocio relacionados con servicios basados en Internet (acceso remoto, dial-in, Telnet, email, WWW, comercio electrónico, etc.) y a los **controles específicos de seguridad** que existen para protegerlos:

- Identificación y autenticación (política de gestión de password, firmas digitales y certificados, etc.)
- Control de importación de software (prevención, detección y eliminación de virus, control de software interactivo, etc.)
- Encriptación
- Nivel de sistema/arquitectura (acceso remoto al sistema, acceso a bases de datos internas, cortafuegos, etc.)
- Gestión de incidentes
- Administrativa (asignación de responsabilidad de seguridad, política de uso apropiado (AUP), política de privacidad, etc.)
- Conciencia y educación

La guía realiza un detallado estudio de cada una de estas áreas de seguridad para distintos entornos de riesgo/protección (bajo, medio y alto) y propone la siguiente estructura interna común en la definición de todas estas políticas:

- Definición del tema general de la política
- Declaración de la posición de la organización respecto a la misma
- Aplicabilidad de la política (dónde, cómo, cuándo, a quién, a qué)
- Asignación de roles y responsabilidades
- Obediencia, para algunas políticas conviene definir qué infracciones son inaceptables y las consecuencias de este comportamiento.
- Puntos de contacto e información suplementaria

CERT (Computer Emergency Response Team)

Para el CERT (*Computer Emergency Response Team*, de la *Carnegie Mellon University*, en EE. UU.), una de las más antiguas agencias dedicadas a la problemática de la seguridad informática, una política de seguridad es un documento que contiene un plan de alto nivel para la seguridad de la información y computación de toda una organización.

Debe servir como esquema para tomar decisiones específicas, tales como qué mecanismos defensivos utilizar o cómo configurar los distintos servicios, siendo además la base para desarrollar líneas maestras, procedimientos de administración y utilización. Y debe evitar, en la medida de lo posible, detalles tecnológicos, de manera a asegurar una futura vigencia de la misma a largo plazo.

En particular, una política de seguridad **deberá incluir**:

- Una **descripción de alto nivel** del ambiente tecnológico, del ambiente legal (leyes y
- regulaciones), de la autoridad tras la política y la filosofía básica a utilizar para interpretar la política.
- Un **análisis de riesgos** que identifique los valores, las amenazas y los costes de recuperación de ataques.
- **Líneas maestras para administradores** sobre cómo administrar los sistemas cubiertos.
- Definición de lo que constituye el **uso aceptable de los sistemas**.
- Líneas maestras de **cómo reaccionar a un ataque** (ej. cómo tratar con los medios de comunicación, las autoridades y en qué casos se debe bloquear de inmediato el acceso a los sistemas o mantenerlo bajo vigilancia).
- Según el CERT hay un conjunto de **factores que contribuyen al éxito** de una política de seguridad, a saber:
    - – Compromiso y apoyo de la cúpula directiva (*management commitment*),
    - – Soporte tecnológico para implementar la política,
    - – Diseminación y comunicación efectiva de la política,
    - – Conciencia de seguridad de todos los usuarios.

La dirección deberá asignar responsabilidades de seguridad y debe de disponer de fondos y de personal para este fin. Se pretende que el resultado sea una implementación automática y consistente de la política de seguridad, por ejemplo para el control de accesos y autenticación.

Las opciones tecnológicas de soporte incluyen (entre otras):

- Sistemas de autenticación de pregunta/respuesta.
- Sistemas de auditoría
- Sistemas de encriptación, tanto para la transmisión como para el almacenamiento de datos.
- Dispositivos de protección de red, tales como cortafuegos y servidores *proxy*.
- El CERT clasifica el soporte tecnológico en dos grandes grupos: tecnología operacional y criptografía. El objetivo de la tecnología operacional es el de mantener y defender la disponibilidad de los recursos de una manera segura. El objetivo de la criptografía es la de garantizar la confidencialidad, integridad y autenticidad de esos recursos.

En complemento de la política de seguridad, el CERT establece una serie de Procedimientos de seguridad y de Prácticas de seguridad.

Los **Procedimientos de seguridad** son guías prácticas (paso a paso) definidas en base a la política de seguridad. Tratan de temas como el acceso al *site* desde casa o durante un viaje, el uso de la encriptación, la autenticación de usuarios y los modos de monitorización.

Las **Prácticas de seguridad** están dirigidas a los administradores de sistemas y tienen un papel clave en la seguridad. Estos documentos pueden ser del tipo *checklist* y tratan de asuntos como tamaños y caducidad de *passwords*, instalación de *patches* de fabricantes y otros similares. En total existen más de 60 Prácticas de seguridad CERT que se acompañan, cada una de ellas, de varias implementaciones adaptadas a los distintos sistemas operativos (Unix, Windows NT y otras tecnologías) y que se reagrupan tal como sigue:

- Prácticas sobre el endurecimiento y la seguridad de sistemas
- Prácticas sobre la preparación para la detección y respuesta a intrusiones
- Prácticas sobre la detección de intrusiones
- Prácticas sobre la respuesta a intrusiones

- Prácticas sobre la mejora del sistema de seguridad
- Prácticas relacionadas a los contratistas de seguridad informática

Al margen de estas recomendaciones prácticas, el CERT también propone un **sistema de auto-evaluación** de amenazas, bienes y vulnerabilidad llamado **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) que puede resultar muy útil tanto de base para la definición de una estrategia y política de seguridad como de herramienta de medición de las prácticas de seguridad actuales. De momento el método OCTAVE sólo está definido para grandes organizaciones y el desarrollo del sistema adaptado a pequeñas y medianas organizaciones está en curso.

SANS Institute

El SANS (System Administration, Networking and Security) Institute, establecido en 1989 como una organización de cooperación para la investigación y enseñanza, comienza por decir que una política de seguridad es algo más que tener un cortafuegos y software antivirus actualizado. Empieza por un Plan de Seguridad de Información.

Como base, aconseja consultar el conjunto de artículos sobre cómo construir una política de seguridad del NIST. Otras fuentes a considerar serán Swanson y Guttman; "Generally Acceptable Principles and Practices for Securing Information Technology Systems." así como las RFC's (por supuesto la original y obsoleta RFC1244 "Site Security Handbook" y la más reciente RFC2196 "Site Security Handbook").

Según el SANS Institute, la política de seguridad debe de ser flexible porque los diferentes departamentos de la organización pueden necesitar políticas específicas y una cierta flexibilidad de procedimientos.

La política de seguridad deberá estar organizada en varios niveles, teniendo las unidades Organizacionales libertad de escribir políticas adicionales en las áreas de su responsabilidad, pero sin abandonar la hegemonía de la política global de seguridad.
Existirán, por supuesto, algunas secciones comunes que serán utilizadas por todos departamentos, por ejemplo, autenticación de usuarios, protección contra intrusiones (incluyendo monitorización de accesos tentados y conseguidos), control de acceso físico a los sistemas (incluyendo armarios de cables y centrales telefónicas), procedimientos de salvaguarda (incluyendo equipamiento de red, *firewalls*, sistemas de detección de intrusiones, etc.), sin olvidar almacenamiento *off-side*. Otros asuntos importantes son la planificación de catástrofes y la definición de auditorías.

Algunos temas a considerar en una política de seguridad completa son el uso de *modems* (dialin, dial-out), procedimientos de substitución de personal y resolución de incidentes. La resolución de incidentes deberá ser descrita con detalle suficiente, definición de funciones y responsabilidades, incluyendo un procedimiento paso-a-paso desde la identificación del incidente hasta el post-mortem final.

El **SANS Security Pólice Project** es un proyecto del SANS Institute que pretende aportar todo lo necesario para el rápido desarrollo e implementación de políticas de seguridad. Para ello se ha puesto a disposición pública una veintena de plantillas sobre las políticas de seguridad desarrolladas, a lo largo de 80 años, por un equipo de expertos para una gran organización.

JISC (Joint Information Systems Committee)

El JISC es una organización responsable de la coordinación de las políticas relacionadas con los sistemas de información del medio educativo del Reino Unido.

En un artículo sobre seguridad, el JISC considera que los sistemas de información y la información que contienen son de importancia vital para el funcionamiento de las instituciones. Esas instituciones deben ser capaces de confiar en tres aspectos clave de la seguridad de la información:

- Disponibilidad (saber que la información está siempre accesible)
- Integridad (saber que la información es correcta y actual, y no fue modificada de ninguna manera, deliberadamente o no)
- Confidencialidad (saber qué información sensible sólo puede ser accedida por aquellos
- debidamente autorizados)

Justamente, como no hay nada completamente fiable, las instituciones deben estar preparadas para responder con rapidez y apropiadamente a cualquier inci-

dente de seguridad, retomando el funcionamiento normal de los sistemas lo más pronto posible.

Una política de seguridad es necesaria como forma de justificar los gastos relacionados con la seguridad, que deberán ser significativos (por ejemplo en tiempo consumido por los profesionales responsables). Este esfuerzo sólo puede ser precisado en el contexto de una política de seguridad que valore correctamente las consecuencias de posibles ataques y los costes asociados a su prevención.

Otro beneficio de una política de seguridad de la información es que ofrece un esquema dentro del cual se pueden definir tareas y responsabilidades relacionadas con la seguridad, formular y justificar reglas que sean necesarias y hacer explícitas las sanciones a tomar en respuesta a acciones concretas que resulten en algún tipo de daño para la institución. Por ejemplo, el *Data Protection Act* 1998 obliga a que todas las organizaciones que procesen datos personales a mantener standards de privacidad y confidencialidad.

Según JISC los objetivos de una política de seguridad son: definir qué comportamientos están permitidos y cuáles no, por quién y en qué circunstancias. Así se pretende establecer un modelo de privilegios y responsabilidades. Es sabido que los usuarios de sistemas de información están más dispuestos a aplicar las prácticas de seguridad cuanto más conocedores de las causas y efectos de las mismas son. Políticas muy restrictivas no tendrán éxito una vez que se vuelva difícil convencer a las personas que tendrían que seguirlas que realmente lo hagan.

Visto de una forma práctica y operacional, la política deberá proporcionar el contexto para un conjunto de líneas maestras y de procedimientos que establecerán detalladamente cómo se implementará la seguridad en todos los sistemas de información.

La visión del JISC es que la estructura debe ser constituida por un documento sencillo de alto nivel –la política de seguridad– con distribución obligatoria a todos colaboradores, y que este documento de alto nivel debería complementarse con un conjunto de documentos más específicos. La política de seguridad debe entonces incluir:

- Objetivo – objetivos y razones, incluyendo obligaciones legales
- Ámbito – descripción de los sistemas sobre los que se aplica la política y de las partes interesadas (*stakeholders*).
- Responsabilidades
- Contactos – a quien informar sobre incidentes.
- Sanciones – acciones a tomar después de determinar culpables de incidentes.
- Más información – lista de referencias a documentos adicionales que no sean de interés general.

Otros documentos necesarios (muchos de estos documentos podrán ser sencillos, por ejemplo, de una o dos páginas):

Documentos que afectan un número significativo de usuarios:

- Política de utilización aceptable (*Acceptable Use Policy*)
- Política de acceso a información administrativa
- Política de acceso remoto (incluyendo acceso por Internet, o dial-up)
- Política de utilización de máquinas personales
- Política institucional de privacidad
- Política de conexión a la red

Documentos menos generales, sobre áreas técnicas particulares:

- Política de configuración de cortafuegos
- Política de configuración de base de red (incluyendo los equipamientos de backbone y VPN, se existir)
- Política de encriptación y gestión de claves
- Política de equipos de tipo Wireless

Documentos para administradores de sistemas departamentales (si es necesario)

- Líneas maestras de gestión de seguridad – incluyendo los estándares de seguridad que los equipos departamentales deben respetar (este documento se vuelve más importante si la responsabilidad es más descentralizada)
- Procedimientos: éstos acompañan las políticas, sirviendo como instrumentos para ponerlas en práctica. Ejemplos son procedimientos de back-up y de almacenamiento off-site de información clave o la desactivación de cuentas cuando una persona abandona la institución.

Dos procedimientos importantes que toda organización debe definir son:

- Procedimiento de resolución de incidentes de seguridad.
- Procedimiento de búsqueda (scanning) de vulnerabilidades conocidas en sistemas conectados a la red, incluyendo test de penetración.

El JISC recomienda usar como base la norma británica BS7799 - ISO Standard (ISO27001) como líneas maestras para desarrollar los procesos internos de seguridad.

ISO (International Standard Organisation)

La ISO (International Standard Organisation) ha desarrollado recientemente (2000) un *standard* de seguridad, el ISO 27001. Este *standard* se divide en dos partes:

- Parte 1: ISO/IEC 27001 que es un **código de buenas prácticas** de seguridad a seguir
- Parte 2: 27000-1 que es una **especificación para Sistemas de Gestión de Seguridad de la Información** (*Information Security Management Systems - ISMS*). Un ISMS es el medio a través del cual los directivos de una organización pueden monitorizar y controlar su seguridad.

Parte 1: Código de buenas prácticas

La ISO/IEC 27001 define 127 prácticas de seguridad (que se desarrollan en más de 500 elementos de buena práctica) estructurados bajo las 10 áreas siguientes:

- Planificación de continuidad del negocio
- Control de acceso al sistema
- Desarrollo y mantenimiento del sistema
- Seguridad física y del entorno
- Conformidad
- Seguridad del personal
- Seguridad de la organización
- Gestión de la informática y las operaciones
- Clasificación y control de los bienes
- Política de seguridad

El *standard* subraya que una organización no necesita desarrollar todas las guías propuestas, tan sólo aquellas que le conciernan.

Parte 2: Especificación para ISMS

El standard BS7799 instruye sobre cómo aplicar el ISO/IEC 27001 y cómo construir un ISMS.
Define un proceso de 6 etapas:

- **Política de información**. Ante todo hay que identificar qué información es importante y por qué.
- **Ámbito** (general de toda la organización, particular, etc.)
- **Valoración del riesgo**. Una vez identificada la información y su valor resulta sencillo evaluar el riesgo de perderla.
- **Gestión del riesgo**. La decisión de gestionar los riesgos se desarrolla a nivel de tecnología, gente, procedimientos administrativos y elementos físicos (puertas, candados, etc.)
- Elección de las **salvaguardas**
- Declaración de **aplicabilidad**

El Sistema de Gestión de la Seguridad de la Información (ISMS)

La ISO está estableciendo unos **esquemas de certificación** de sistemas ISMS respecto al standard 27000. Existen ya varios Organismos Nacionales de Acreditación en todo el mundo que operan bajo el principio de "mutuo reconocimiento", de manera que las certificaciones emitidas en un país sean válidas en otro. Para obtener una certificación, un sistema ISMS deberá ser auditado por un asesor 27000-1 que trabaje para un Organismo de Certificación y estar sometido a revisiones periódicas.

Con este servicio de certificación, la ISO quiere establecer un sello internacional que garantice las prácticas de seguridad de cualquier organización.

OECD (Organisation for Economic Co-operation and Development)

Ante el crecimiento explosivo del uso de sistemas de información para todo tipo de aplicación a cualquier nivel de la esfera de la vida (económica, social o política), la Organización para la Cooperación y Desarrollo Económicos - OECD (Organisation for Economic Co-operation and Development) decidió establecer en 1990 un grupo de expertos para preparar las "Líneas Guía para la Seguridad de Sistemas de Información".

Para ello, la OECD ofrece a los gobiernos un foro en donde para intercambiar esfuerzos y compar-

tir experiencias para buscar soluciones a los problemas comunes.

La OECD mide la productividad y los flujos mundiales de intercambios e inversión, analiza y compara los datos con la finalidad de predecir tendencias futuras y establece normas internacionales en diversos sectores. La organización ha jugado un papel fundamental en la expansión de la economía mundial hacia la liberalización del comercio internacional.

Actualmente, la OECD se enfoca principalmente en:

- Mejorar la regulación económica y la eficacidad de la gobernanza para restablecer la confianza en el mercado y en las instituciones y empresas que lo hacen funcionar.
- Sanar las finanzas públicas de los Estados, que son la base del crecimiento económico duradero.
- Estimular nuevas fuentes de crecimiento a través de la innovación, de estrategias de "crecimiento verde" y el desarrollo de economías emergentes.
- Asegurar que todas las personas, sin importar su edad, puedan obtener las competencias necesarias para los empleos del mañana y para acceder a un trabajo productivo y satisfactorio.

El objetivo de seguridad para un sistema de información es su protección frente a los daños resultantes de fallos a nivel de disponibilidad, confidencialidad e integridad. La OECD establece 9 principios para asegurar este objetivo:

- **Principio de responsabilidad**. La responsabilidad de los propietarios, proveedores y usuarios de los sistemas de información debe ser clara y explícita.
- **Principio de conocimiento**. Los propietarios, proveedores y usuarios de los sistemas de información deben tener conocimiento y ser informados de las medidas, prácticas y procedimientos de seguridad.
- **Principio de ética**. Los sistemas de información y su seguridad deben de tener en cuenta y respetar los derechos y legítimos intereses de los demás.
- **Principio de multidisciplinaridad**. Las medidas, prácticas y procedimientos de seguridad deben de incluir los puntos de vista técnico, administrativo, organizativo, operacional, comercial, educacional y legal.
- **Principio de proporcionalidad**. Los costes, medidas, prácticas y procedimientos de seguridad deben ser apropiados y proporcionados al valor de la información y a la probabilidad y vulnerabilidad frente a los riesgos de seguridad.
- **Principio de integración**. Las medidas, prácticas y procedimientos de seguridad de sistemas de información deben de integrarse dentro del sistema general de seguridad de la organización.
- **Principio de oportunidad**. Las distintas partes, públicas y privadas, nacionales e internacionales, deben de actuar coordinadamente frente a un ataque a la seguridad de los sistemas de información.
- **Principio de revisión**. La seguridad de los sistemas de información debe ser revisada periódicamente.
- **Principio de democracia**. La seguridad de los sistemas de información debe ser compatible con el uso legítimo y el flujo de información en una sociedad democrática.

La OECD recomienda que los gobiernos, el sector público y el privado tomen las medidas de seguridad adecuadas para proteger y dar seguridad a los sistemas de información siguiendo los principios anteriores. En particular aconseja actuar en los niveles siguientes:

- **Desarrollo político**. (Armonización de estándares; promoción de competencia y buenas prácticas; formación y validez de contratos; asignación de riesgos y fiabilidad; sanciones; competencia jurisdiccional)
- **Educación y enseñanza** para usuarios, directivos ejecutivos, técnicos, auditores, etc.
- **Aplicación y restablecimiento**. Se deben aplicar los medios adecuados para ejercer y aplicar los derechos relacionados con la seguridad de los sistemas de información y para restablecerse de las violaciones de dichos derechos.
- **Intercambio de información** relacionada con la seguridad entre gobiernos, sector público y privado.
- **Cooperación** entre gobiernos, sector público y privado en el desarrollo de medidas, prácticas y procedimientos de seguridad a fin de evitar conflictos u obstáculos.

Bibliografía

ACISSI – Agé, Marion; BAUDRU, Sébastien; CROCFER, Nicolas; CROCFER Robert; EBEL, Franck; HENNECART, Jérôme; LASSON, Sébastien; PUCHE, David; RAULT, Raphaël. "Seguridad Informática" En: *Ethical Hacking*. 2. Edición. 2011

AGUILERA LÓPEZ. *Seguridad Informática*. 2011.

CANO, Jeimy. Arquitecturas de Seguridad Informática: Entre la administración y el gobierno de la Seguridad de la Información. En: *seminario de actualización en seguridad informática.* Documento Módulo I Seminario de Actualización en Seguridad Informática. Bucaramanga: Facultad de Ingeniería Informática, Bucaramanga: 2008, p 28.

CRUZ ACOSTA, Arafet. *Libro electrónico: Virus y Antivirus Seguridad Informática*. 2012.

ECHEVERRÍA. *Procedimientos y Medidas de Seguridad Informática- conceptos básicos de seguridad de redes*. 2011.

GARCÍA-CERVIGON, Alegre Ramos. *Antivirus seguridad informática.* 2011.

PORTANTIER. *Seguridad Informática: Aprenda como implementar soluciones desde la visión del experto.* 2013.

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. 2009. Ley 1273 de 2009.

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. 2012. Ley 1581 de 2012.

REVISTA ACIS 115 Seguridad informática: Colombia en la mira. *XIII encuesta nacional ACIS, 2013.*

Datos del autor

Brian Andrés Medina Cerquera es Ingeniero de Sistemas y Telecomunicaciones egresado de la Universidad Libre seccional Cali y magíster en Educación de la Universidad Libre seccional Bogotá. Es docente de la Fundación Universitaria Católica Lumen Gentium.