UNIVERSIDAD
Rafael Belloso Chacín.

Revista Electrónica de
Estudios Telemáticos

TÉLÉMATIQUE

SEGURIDAD EN ORGANIZACIONES CON TECNOLOGÍAS DE INFORMACIÓN

Luis J. Ugas M.
Universidad Rafael Belloso Chacín. Venezuela.

RESUMEN

La palabra "seguridad" encierra muchos significados dependiendo del entorno de aplicación o del contexto bajo el cual se esté definiendo. En función de los objetivos de este trabajo de investigación la seguridad fue enfocada hacia la protección lógica de los activos de información de la Empresa "Productora de Materia Prima". El propósito del trabajo fue el de identificar los factores organizacionales que incidían en la seguridad, evaluar los niveles de importancia y de riesgo de cada uno de esos factores y presentar el diseño de una propuesta de solución. La investigación desarrollada fue del tipo "proyecto factible" dado que se presentó una solución viable a un problema de seguridad planteado y su diseño fue "no experimental" puesto que las variables de investigación fueron observadas y evaluadas sin ninguna intervención. La metodología aplicada fue dividida en fases, actividades y tareas, que generaban uno o varios productos como salida y que a su vez eran usados como entradas para posteriores tareas o actividades. Se concluyó que los niveles de seguridad no técnica son insuficientes para garantizar la confiabilidad, la integridad y la disponibilidad de la información; y que las personas que integran la Empresa no poseen una Cultura Organizacional de Seguridad. Razón por la cual, se diseño un modelo de seguridad dinámico que sirviera de Marco Referencial para la implantación y mantenimiento de un esquema de seguridad.

PALABRAS CLAVES: Seguridad, Tecnología de Información, Proyecto Factible.

ABSTRACT

Many different meanings are covered by this word: "security", depending on the application environment or the context under which it is at. As per the scope of this research work, security was focused towards the logical protection of the information assets of the "Raw material producer" company. To identify the organizational factors affecting security was the goal of this work, as well as evaluating the importance-risks levels of every and each of the factors, and presenting a design of proposal for a solution. A "feasible project" type of investigation was developed, as a viable solution to a pre-posed security problem was presented. Its design was a "non-experimental"

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

one, as its investigative variables were observed and evaluated with no intervention whatsoever. The applied methodology was divided into Phases, Activities and Tasks, which were generating one or several products as a way out, and, at the same time, were used as ways in for future tasks or activities. It was then concluded that the levels for non-technical security were insufficient as to guaranty the reliability, integrity and availability of the information, and the personnel of the company do not show an organizational culture towards security. This was the reason why a dynamic model of security was designed, which might serve as well as a referential pattern for a security scheme developing and maintenance.

KEY WORDS: Security. Information Technology. Feasible Project.

INTRODUCCIÓN

La palabra "seguridad" encierra muchos significados dependiendo del entorno de aplicación o el contexto bajo el cual se este definiendo. En ese orden de ideas, el tema de este Trabajo de Investigación, "Seguridad en Organizaciones con Tecnologías de Información", fue enfocado hacia la protección lógica de los activos de información de la empresa objeto de estudio, que para efecto de proteger la confidencialidad de los datos proporcionados, fue identificada como "Productora de Materia Prima".

El propósito de este Trabajo de Investigación fue el de identificar los factores organizacionales que incidían en la seguridad de una Organización con Tecnologías de Información, evaluar los niveles de importancia y de riesgo de cada uno de esos factores sobre la seguridad total de la Organización y presentar el diseño de una propuesta de solución.

La Empresa "Productora de Materia Prima" ha expandido sus capacidades tecnológicas con el propósito; de cubrir los requerimientos de procesamiento, almacenamiento y transmisión de sus usuarios; de aprovechar las oportunidades de negocio y afianzar su estabilidad competitiva en el mercado. Ante este escenario lo que motivó al autor de este trabajo a proponer a dicha Organización este Tema de Investigación, fue la oportunidad de contribuir, con su experiencia y conocimientos a través de la aplicación de una metodología de investigación, a la solución del problema planteado.

Con 15 años de experiencia en Institutos y Empresas con Tecnologías de Información, el autor ha observado que la mayoría de las vulnerabilidades de seguridad son originadas por factores organizacionales. De ahí que el autor

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

este de acuerdo con una de las conclusiones de la Organización Internacional Computer Emergency Request Team (CERT) (2.000) donde afirma que "el 80% de los incidentes de seguridad en las Organizaciones son originados por la falta de una Cultura Organizacional de Seguridad (p. s/n)".

PLANTEAMIENTO DEL PROBLEMA

En cualquier infraestructura de red, sin importar cual es la plataforma tecnológica utilizada, el elemento más importante es la información. Todas estas innovaciones van dirigidas hacia la transmisión, visualización, modificación, creación y almacenamiento de la información. Las empresas procesan, en forma distribuida y/o centralizada, información confidencial de diferentes tipos: como información gerencial, administrativa, de mercadeo, operativa, etc., que puede convertirse en objetivo de ataque por parte de intrusos informáticos (personas no autorizadas), quienes tratan de acceder esta información para ocasionar daños a la empresa, para beneficio propio o para simple satisfacción personal.

Estas innovaciones tecnológicas de servicios, hardware y software traen consigo ciertas debilidades o deficiencias de seguridad, convirtiéndose así en medios para el acceso no autorizado a la información, por parte de los intrusos. El fácil acceso a la infraestructura de redes pude convertirse en una invitación para los intrusos, de ahí el dicho que "la oportunidad hace al ladrón". Un ataque mal intencionado a la infraestructura tecnológica por parte de un hacker puede afectar la operatividad de la empresa en forma parcial o total y en forma temporal o permanente. Por esta razón, las empresas tienen que enfocar su atención a fortalecer la seguridad de cada uno de sus componentes de la infraestructura de redes, por el simple hecho que "una cadena es tan fuerte como su eslabón más débil".

Los deficientes mecanismos de seguridad implantados en las empresas, en algunos casos se deben, a que la velocidad con la que se desarrollan nuevas tecnologías es mayor que la velocidad de asimilación de estas por parte de los clientes. Estas empresas programan el entrenamiento para que el personal responsable se capacite para instalar, implantar y administrar los productos tecnológicos, en el tiempo planificado. Pero ni el entrenamiento ni el tiempo destinado para efectuar las pruebas antes de la puesta en producción son suficientes para que el personal se capacite lo suficiente para implantar el adecuado mecanismo de seguridad, y en los casos donde se considera la ejecución de pruebas de seguridad, estas no son diseñadas con la suficiente profundidad debido al desconocimiento de la tecnología. Ante esta situación, los profesionales responsables de implantar estas nuevas tecnologías y de mantener, además la continuidad operativa de los servicios,

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

no estarán en ningún momento capacitados para garantizar la integridad, confiabilidad y disponibilidad de la información manejada por nuevos servicios de tecnología. Es necesario fortalecer la seguridad en las empresas con políticas y estrategias de seguridad tendientes a garantizar que toda implantación de nueva tecnología debe ir acompañada: de un adecuado entrenamiento y capacitación profesional; y de un procedimiento de evaluación de los riesgos de seguridad de esa tecnología para detectar las vulnerabilidades y posibles amenazas de ataques contra la seguridad.

Frente a esta problemática, ISACA (1.998) expone que ha sido cada vez más evidente para los directivos, usuarios y proveedores de servicios la necesidad de un Marco Referencial para la seguridad y el control de tecnologías de información (TI). Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

La creciente dependencia en información y en los sistemas que proporcionan dicha información;

La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información;

La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y

El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

TIPO Y OBJETIVO DE LA INVESTIGACIÓN

La investigación desarrollada fue del tipo "proyecto factible" dado que presentó una solución viable a un problema de seguridad planteado y su diseño fue "no experimental" puesto que las variables de investigación (factores organizacionales) fueron observadas en su contexto natural, sin ningún tipo de interferencia, para evaluar su incidencia sobre la seguridad de la organización.

La metodología aplicada para desarrollar el trabajo de investigación es una recopilación de partes de las metodologías tomadas como referencia y adaptadas a las necesidades de este proyecto factible. La metodología

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

aplicada fue dividida en fases, actividades y tareas, que generaban uno o varios productos como salida y que a su vez eran usados como entradas para posteriores tareas o actividades.

Como objetivos específicos se planteó: Identificar los factores organizacionales que podrían incidir en la seguridad de una Organización con Tecnologías de Información. Determinar qué importancia tienen estos factores organizacionales sobre el nivel de seguridad de la Organización. Determinar cuál es el riesgo de que estos factores organizacionales afecten el nivel de seguridad de la Organización. Determinar qué impacto podría tener esta situación sobre la Organización.

Analizar y diagnosticar la situación actual de la Organización con respecto a la seguridad organizacional (no técnica). Efectuar un estudio de factibilidad de las propuestas de solución. Seleccionar y diseñar una propuesta de solución.

JUSTIFICACIÓN DE LA INVESTIGACIÓN

En este punto el autor presenta las motivaciones de carácter teórico–práctico, metodológico y académico que llevaron al planteamiento y desarrollo de este trabajo de investigación.

ANÁLISIS DE LOS RESULTADOS

Como resultado de los análisis efectuados en relación a los niveles de riesgo e importancia que tienen algunos factores organizacionales sobre los niveles de seguridad de la organización, se estableció el siguiente diagnostico:

El Factor Evaluación de Riesgos, que se corresponde con el proceso P09 (Evaluar Riesgos) de COBIT puede impactar sobre todos los Recursos de TI incidiendo del grado Primario sobre la Confiabilidad, la Integridad y la Disponibilidad. El segundo Factor de Riesgo es la Seguridad de los Sistemas que se corresponde con el proceso DS5 (Garantizar la Seguridad de los Sistemas) puede impactar sobre la Confiabilidad y la Integridad de todos los Recursos de TI. Sin embargo, el nivel de importancia dado por la Organización fue de 35 y 46 (sobre 100) respectivamente.

En base a estos resultados se puede concluir que existen algunos Factores que tienen un alto nivel de riesgo, que no han recibido la debida atención o importancia convirtiéndose en vulnerabilidades presentes en la Seguridad Corporativa de la Organización. Por lo tanto, se puede asegurar

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

que la organización no posee un esquema de seguridad coherente e integral que le dé, el debido valor a cada uno de los Factores que intervienen en el entorno organizacional y que en mayor o menor medida son una amenaza a la seguridad.

Dado que la seguridad total es la suma del nivel de seguridad de cada uno de sus componentes, se puede deducir que la Seguridad Organizacional (no técnica) es la suma de los niveles de seguridad de cada uno de los Factores Organizacionales, en consecuencia cualquier factor cuyo nivel de seguridad sea bajo se convierte en un punto débil y por ende un punto vulnerable susceptible a ataques de Hackers o Crackers.

A pesar que la evaluación de la seguridad técnica o tecnológica no fue el propósito de este trabajo de investigación sería muy acertado deducir que la misma tiene altos niveles de riesgo, puesto que los factores seleccionados para efectos de la investigación son base de toda Infraestructura Tecnológica de cualquier organización. Esta base organizacional es la garantía para que en cada una de las tecnologías presentes en la organización se analicen, diseñen, implanten y mantengan los mecanismos de seguridad adecuados.

Si por un lado se establece un robusto mecanismo de Firewall para el acceso a Internet, pero no se capacita y concientiza al usuario sobre la importancia de la confidencialidad de la clave de acceso, igualmente la Organización sigue siendo vulnerable a los ataques de Hackers.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez S. (1.995). *Psicología de la seguridad. Algunas consideraciones sobre atención sostenida en tareas de vigilancia*. Revista de Seguridad Corporativa. España. Disponible en ubicación electrónica: http://www.seguridadcorporativa.org/seguridadcorporativa/tareasdevigilancia.htm (Nov 1.999).

Arenillas J. M. (1.995). *¿Es la seguridad una profesión?, Artículo a Favor*. Revista de seguridad: Seguridad Corporativa, España. Disponible en la ubicación electrónica: http://www.seguridadcorporativa.org/seguridadcorporativa/pro.htm (Nov. 1.999)

Byron H. (1.997). *Historias de Hackers-3*. Disponible en la ubicación electrónica: http://www.personal.redestb.es/hugo/byron/pirata3.htm (1.999)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

Computer Emergency Request Team (CERT). (2000). Disponible en la dirección electrónica: http://www.cert.org, (2.000) http://www.cert.org/advisories/ http://www.cert.org/annual_rpts/ http://www.cert.org/stats/cert_stats.html

Common Methodology for Information Technology Security Evaluation (August 1.999). *Evaluation Methodology, part 2.* Disponible en la ubicación electrónica: http://www..nist.gov/cc (1.999) http://www.radium.ncsc.mil/tpep

Cruz F. (s/f). *Seguridad en redes y Sistemas*. Disponible en ubicación electrónica: http://www.bbs.ingedigit.com/articulos/segredes.htm (1.999)

Ford M., Lew H.K., Spanier S. Y Stevenson (1.998). *Tecnología de Interconectividad de Redes*. Editorial Prentice Hall, Mexico. Traducción al español de publicación original en ingles de: Internetworking Technologies Handbook.

Gate B. (1.996). *Camino al Futuro*. Editorial McGraw Hill. Segunda Edición. Traducción al español de publicación original en ingles de: The Road Ahead. Madrid. España.

Hernández C. (1.999). *Hackecrs, Los clanes de la red 2000*. Disponible en ubicación electrónica: http://www.criptomicrom.com (1.999)

Howard J.D. (1.997). *An Analysis of Security Incidents on The Internet 1.989 - 1.995.* Carnegie Mellon University, Pittsburgh, Pennsylvania, EEUU. Disponible en ubicación electrónica: http://www.cert.org/research/jhthesis/start.html. (2.000)

Information Systems Audit and Control Association (ISACA) (April 1.998). *Control Objectives for Information and Related Technology (COBIT Methodology)*, 2nd Edition, EEUU, Disponible en CDROM.

Information Technology Security Evaluation Criteria (ITSEC) (1.991). Disponible en la ubicación electrónica: http://packetstorm.security.com/papers/evaluation/itsec.txt (1.999)

Manunta C. (1.995). *Seguridad la Introducción*. Revista de Seguridad. Seguridad Corporativa. España. Disponible en ubicación electrónica: http://www.seguridadcorporativa.org/seguridadcorporativa/presentacionlibro.htm (Nov. 1.999).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002

Microsoft (2.000). *Microsoft Security. Technical Information*. Disponible en CDROM.

Microsoft (1.999). *Microsoft Security Bulletin*. Disponible en la ubicación electrónica: http://www.microsoft.com/security/bulletins/ (1.999)

Microsoft (2.000). *Security*. Disponible en ubicación electrónica: http://www.microsoft.com/technet/security (2.000)

Microsoft Venezuela (1.999). *Designing a Secure Microsoft Windows 2000 Network Course.* Dictado por CTT. Maracaibo. Venezuela.

Ministerio de Administraciones Públicas (MAP), Concejo Superior de Informática (1.995). *Guía para la Adaptación de los Sistemas de Información de la Administraciones Públicas del año 2000 (ASI2000),* España. Disponible en la ubicación electrónica: http://www.map.es/csi/asi2000/capitulo0/0asi2000.htm (Nov. 1.999)

Ministerio de Administraciones Públicas (MAP), Concejo Superior de Informática (1.995*). Metodología de Planificación y desarrollo de Sistemas de Información (METRICA) versión 2.1*, España. Disponible en la ubicación electrónica: http://www.map.es/csi/pg5m41.htm (Nov. 1.999).

National Institute of Standarts Technology . *Executive Guide to the Protection of Information Resources.* Disponible en ubicación electrónica: http://www.packetstorm.security.com/papers/evaluation/exeguide.txt

PriceWaterHouseCoopers (1.999). *Microsoft Windows NT 4.0. Seguridad, Auditoría y Control.* Editorial McGraw Hill.Primera Edición. España. Traducción al español de publicación original en ingles de: Microsoft Windows NT 4.0, Security, Audit and Control.

Request For Comments (RFCs). *RFCs about "Security*". Disponible en ubicación electrónica: http://www.cert.dfn.de/esource/rfc/ (1.999)

Unión Internacional de Telecomunicaciones (UTI). *Recomendaciones o Normas Internacionales*. Disponible en la ubicación electrónica: http://www.uti.org (2.000)

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 1 Edición No 1 – Año 2002