PROTECCIÓN DE ACTIVOS

SEGURIDAD DE LA INFORMACIÓN

ASIS INTERNATIONAL
Advancing Security Worldwide®

PROTECCIÓN DE ACTIVOS

SEGURIDAD DE LA INFORMACIÓN

ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS International | 1625 Prince Street | Alexandria, VA 22314 USA | *www.asisonline.org*

Copyright © 2012 por ASIS International

ISBN 978-1-934904-12-1

El libro Protección de Activos está elaborado bajo la premisa de que la editorial no se compromete a prestar servicios legales, contables y otros servicios profesionales. Está diseñado como una guía y referencia de los temas tratados. Aunque se ha hecho todo lo posible para asegurar la precisión de los contenidos en este documento, no es una publicación oficial y el editor no asume ninguna responsabilidad por los errores u omisiones.

Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, traducida a otro idioma, almacenada en sistemas de recuperación o transmitida en cualquier forma o por cualquier medio, ya sea electrónico, mecánico, fotocopia, grabación o cualquier otro, sin el consentimiento previo por escrito del propietario de los derechos de autor copyright.

Impreso en Estados Unidos de América.

10 9 8 7 6 5 4 3 2 1

Traducido por OZ Translations, Santiago, Chile, 2014.
ISBN: 978-1-934904-71-8

AGRADECIMIENTOS

ASIS International (ASIS), la sociedad líder en el mundo para los profesionales de la seguridad, fundada originalmente en 1955 como Sociedad Americana para la Seguridad Industrial, adquirió Protección de Activos en diciembre de 2003. La adquisición de esta obra pone de relieve el papel de liderazgo de la sociedad en la educación profesional. Es el deseo sincero de ASIS y su personal de editorial seguir incrementando el valor de esta importante guía.

Protección de Activos, que ha estado en vigencia desde 1974, es reconocida como la referencia principal para profesionales de la seguridad y el editor desea agradecer a los dos autores fundadores y a los editores posteriores.

Timothy J. Walsh, CPP Richard J. Healy, CPP

Timothy L. Williams, CPP
Editor General

Editores Asociados
David G. Aggleton, CPP
Milton E. Moritz, CPP
Mike Hodge, J.D.
Sanford Sherizon, Ph.D., CISSP
Timothy J. Walsh, CPP, Editor Emeritus

A medida que avanzamos, enfrentados a problemas que representan un desafío para la industria de la seguridad, nuestra misión es asegurar que Protección de Activos proporcione las soluciones estratégicas necesarias para ayudar a los profesionales cumplen con las exigencias del siglo 21 y los venideros. También nos comprometemos a reunir a un grupo de expertos en la materia que mejore esta guía si fuera necesario para lograr nuestra misión.

Un agradecimiento por su valiosa colaboración en la revisión de la traducción a:

Alfredo Iturriaga, CPP
Jaime Owens, CPP
Jorge Creado, CPP

Michael E. Knoke, CPP
Editor General

Eva Giercuszkiewicz, MLS, Jefe de Proyecto
Evangeline Pappas, Jefe de Producción

Peter E. Ohlhausen, Editor Técnico

PREFACIO

OBJETIVOS DE *PROTECCIÓN DE ACTIVOS*

Este trabajo de referencia de *Protección de Activos (POA*) es proporcionado por una simple, básica razón: la anterior falta de disponibilidad de un recurso integral.

Aunque la disponibilidad de la literatura de seguridad está creciéndo rápidamente, con textos generales y especializados, no ha sido posible –hasta ahora- para un gerente de empresa o profesional de la proteccion encontrar en forma actualizada, precisa y práctica el manejo de la amplia gama de temas de protección de activos, estrategias y soluciones en una sola fuente.

La necesidad de un recurso tan exhaustivo es bastante generalizada, según los editores, escritores y muchos colegas profesionales cuyo consejo se ha buscado en la elaboración de este texto. El creciente tamaño y la frecuencia de todas las formas de pérdidas de activos, junto con el aumento de los costos y la complejidad relacionada con la selección de medidas, exigen una presentación sistemática y unificada de la doctrina de la protección en todos los ámbitos, así como las normas y especificaciones a medida que se emiten.
Por supuesto, sería presuntuoso asumir que un pequeño grupo de autores pudiera presentar este material sin ayuda. Es, por lo tanto, un objetivo fundamental de Protección de Activos el recurrir a la amplia base de fuentes calificadas que se haya desarrollado. Los autores, revisores y editores tratan de extraer de los datos disponibles, las características comunes o recurrentes, tendencias y otros factores que identifican o señalan las estrategias de protección vigentes. El objetivo es proporcionar un documento fuente, donde se puede obtener información sobre cualquier problema de protección.

LECTORES

Protección de Activos está destinado a un amplio número de lectores: todos los profesionales de la seguridad y administradores de empresas con responsabilidad en la protección de activos. La discusión coherente y el material de referencia pertinente en cada materia deben ayudar al lector a conducir una investigación única que sea eficiente y organizada. De particular importancia son las diversas formas, matrices y listas de comprobación que le dan al lector un comienzo práctico hacia la aplicación de la teoría de la seguridad de su propia situación. *POA* también sirve como una referencia central para los estudiantes que siguen un programa de protección de la seguridad o de activos.

DIÁLOGO

Esperamos que Protección de Activos se convierta en una importante fuente de conocimiento profesional para aquellos que lo lean y que estimule el diálogo serio entre los profesionales de la seguridad. Cualquier lector que esté lidiando con un problema de seguridad inusual, nuevo o difícil, que quisiera recibir opiniones de otros, se le agradece escribir en forma sucinta una descripción del problema y nos lo envíe a ASIS [protectionofassets@asisonline.org]. Si le lector lo solicita, su identidad se mantendrá anónima, pero el problema se publicará con las invitaciones para hacer comentarios. También se anima a los lectores a comunicar su acuerdo o desacuerdo con las estrategias o aplicaciones recomendadas en el *POA* y a sugerir alternativas. Nos reservamos el derecho de publicar o no el material presentado. Los editores también solicitan las opiniones de los lectores sobre políticas de protección de activos, en los que una visión transversal sería muy útil.

FORMACIÓN COMPLEMENTARIA

Los lectores con responsabilidades de supervisión o administración de personal de seguridad y protección de activos, encontrarán en el POA un recurso útil para asignar lecturas obligatorias. Estas lecturas pueden ser elementos de un programa de capacitación formal y pueden ser asignadas como parte de las sesiones de un curso.

Con todos estos objetivos en mente, presentamos a ustedes Protección de Activos, con la sincera convicción que le ayudará a mejorar su experiencia en el campo de la seguridad.

Michael E. Knoke, CPP
Editor General
Enero 2011

COLABORADORES

El éxito de esta publicación está directamente relacionado con el proceso de revisión reconocido por la mayoría de las profesiones. Muchos profesionales de la seguridad, académicos y otros expertos en la materia participaron con el aporte de información actualizada, la realización de la investigación, la revisión de las comunicaciones, y los comentarios constructivos para que fuéramos capaces de ofrecer una publicaciòn que sea reconocida como “la referencia” para los profesionales de la seguridad de todo el mundo.

Es con sincero aprecio que me gustaría dar las gracias a las personas que nombro a continuación que han contribuido a Protección de Activos.

Teresa M. Abrahamsohn, CPP
Sean A. Ahrens, CPP
Marene N. Allison
Randy I. Atlas, CPP
George J. Barletta, CPP
Mark H. Beaudry, CPP
Regis W. Becker, CPP
Brent Belcoff, CPP
Howard J. Belfor, CPP
Adolfo M. Benages, CPP
Lawrence K. Berenson, CPP
Alexander E. Berlonghi
Raymond J. Bernard, PSP
Henri A. Berube
Martin T. Biegelman, J.D.
Daniel E. Bierman, CPP, PSP
Patrick C. Bishop, CPP
Dennis R. Blass, CPP, PSP
Keith C. Blowe, CPP
Paul F. Boyarin, CPP, PCI
Tom Boyer
Pete Brake, Jr., CPP
Darryl R. Branham, CPP
Joseph P. Buckley, III
Lucien G. Canton, CPP
James P. Carino, Jr., CPP
Sue Carioti
James S. Cawood, CPP, PCI, PSP
Richard E. Chase, CPP

John C. Cholewa, III, CPP
Tom M. Conley, CPP
Geoffrey T. Craighead, CPP
Michael A. Crane, J.D., CPP
Bruce A. Dean, CPP
Fritz X. Delinski
Edward P. De Lise, CPP
David A. Dobbins, PSP
Clifford E. Dow, CPP
Christina M. Duffey, CPP
Brandon Dunlap
Cheryl D. Elliott, CPP, PCI
James W. Ellis, CPP, PSP
William R. Etheridge
Gregory Alan Ewing, CPP, PSP
Kenneth G. Fauth, CPP
Lawrence J. Fennely
Donald J. Fergus
Eugene F. Ferraro, CPP, PCI
James H. Fetzer, III, CPP
Michael T. Flachs, CPP
Richard H. Frank, CPP
Kenneth M. Freeman, CPP
Peter J. French, CPP
Mary Lynn Garcia, CPP
John W. Gehrlein, CPP
Eva Giercuszkiewicz, MLS
Gregory A. Gilbert, CPP
Frederick G. Giles, CPP
Timothy D. Giles, CPP, PSP
David H. Gilmore, CPP
Christopher Giusti, CPP
Brian D. Gouin, PSP
Richard P. Grassie, CPP
Benjamin P. Greer
Steven R. Harris
Ronald D. Heil, CPP
Richard J. Heffernan, CPP
Chris A. Hertig, CPP
William T. Hill, CPP
Ronald W. Hobbs, CPP

Mark D. Hucker, CPP
W. Geoffrey Hughes, PCI
John L. Hunepohl
Gregory L. Hurd, CPP
Gregory W. Jarpey, PSP
Sheila D. Johnson, CPP, PSP
Thomas R. Jost
Diane Horn Kaloustian
Cathy M. Kimble, CPP
R. Michael Kirchner, CPP
Glen W. Kitteringham, CPP
Michael E. Knoke, CPP
Terrence J. Korpal
James M. Kuehn, CPP
David Lam, CPP
Robert F. Leahy, CPP, PSP
Robert E. Lee
Todd P. Letcher
Emblez Longoria, CPP, PSP
Cynthia Long
Richard E. Maier, CPP
Loye A. Manning, CPP, PSP
Robert L. Martin, CPP
Roger B. Maslen, CPP
Judith G. Matheny, CPP
Edward F. McDonough, Jr., CPP
Richard A. Michau, CPP
Bonnie S. Michelman, CPP
Owen J. Monaghan, CPP
Patrick M. Murphy, CPP, PSP
Carla Naude, CPP
James W. Nelson
Robert L. Oatman, CPP
Gerald A. O'Farrell, CPP
Peter E. Ohlhausen
Leonard Ong, CPP
Harm J. Oosten, CPP
S. Steven Oplinger
Denis A. O'Sullivan, CPP
Jaime P. Owens, CPP
Gerard P. Panaro, J.D.

James F. Pastor, Ph.D.
David G. Patterson, CPP, PSP
John T. Perkins, CPP
Karl S. Perman
Kevin E. Peterson, CPP
Charlie R. A. Pierce
Patrick K. Quinn, CPP
Roy A. Rahn, CPP
John D. Rankin, CPP
William G. Rauen, CPP
David L. Ray, LL.B.
Joseph Rector, CPP, PCI, PSP
Ty L. Richmond, CPP
Lisa M. Ruth
Jeffrey J. Ryder, Jr., CPP, PSP
Mark A. Sanna, CPP
Stephen Saravara, III, J.D., CPP
Charles A. Sennewald, CPP
Dennis Shepp, CPP, PCI
Shari Shovlin
Marc Siegel, Ph.D.
Dennis Smith, CPP
Stan Stahl, Ph.D.
Paul J. Steiner, Jr., CPP
Pamela M. Stewart, PCI
Dan E. Taylor, Sr., CPP
Lynn A. Thackery, CPP, PSP
Mark L. Theisen, CPP
Dave N. Tyson, CPP
Darleen Urbanek
Karim Vellani, CPP
Barry J. Walker, CPP
Michael W. Wanik, CPP
Roger D. Warwick, CPP
Fritz Weidner
Richard C. Werth, CPP
Allan R. Wick, CPP, PSP
Anthony S. Wilcox, CPP
Donald S. Williams, CPP
Reginald J. Williams, CPP
Richard F. Williams, CPP

Timothy L. Williams, CPP
Coleman L. Wolf, CPP
Richard P. Wright, CPP
Richard Y. Yamamoto, CPP
Scott S. Young, CPP

TABLA DE CONTENIDOS

Prefacio

Colaboradores

Capítulo 1. **PROTECCIÓN DE ACTIVOS DE INFORMACIÓN**

1.1 Introducción

1.2 Historia del Espionaje y de la Recopilación de Inteligencia de Negocios

1.3 Enfoque de Gestión del Riesgo para la IAP
- 1.3.1 El Actual Entorno Global de la Información
- 1.3.2 Categorías de Amenazas y Ejemplos
- 1.3.3 Evaluación del Riesgo y Due Diligence
- 1.3.4 Lograr el Compromiso

1.4 Métodos para la Mitigación del Riesgo
- 1.4.1 Prácticas Básicas de Protección
- 1.4.2 Seguridad Física
- 1.4.3 Personal de Seguridad
- 1.4.4 Protección de la Privacidad
- 1.4.5 Prácticas Empresariales
- 1.4.6 Operaciones de Seguridad o Gestión de Riesgos de la Información
- 1.4.7 Seguridad de Viajes y Reuniones
- 1.4.8 Prevención y Detección de la Falsificación y Copia Ilegal

1.5 Protecciones Legales
- 1.5.1 Derechos de Autor
- 1.5.2 Marca Comercial, Imagen Comercial, Marca de Servicio
- 1.5.3 Patentes
- 1.5.4 Secretos Comerciales
- 1.5.5 Preocupaciones Internacionales
- 1.5.6 Acuerdos de no Divulgación y Contratos

1.6 Medidas Técnicas de Protección
- 1.6.1 Contramedidas de Vigilancia Técnica
- 1.6.2 Protección en un Entorno de TI
- 1.6.3 Protección en Entornos Especiales

1.7 Respuesta y Recuperación Después de una Pérdida de Información

1.8 Resumen

Capítulo 2. **LA CRECIENTE IMPORTANCIA DE LA SEGURIDAD DE LOS SERVICIOS DE INFORMACIÓN**

2.1 El Desafío Humano: Falta de Imaginación

2.2 Estado de La Seguridad de los Sistemas de Información

2.3 Economía de la Seguridad de los Sistemas de Información

2.4 Factores Críticos de Éxito

2.5 Implicaciones para la Seguridad Física en un Mundo Convergente

2.6 Cibercrimen: Un Desafío Nacional

Capítulo 3. **BASE DE CONOCIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

3.1 Los Elementos de Riesgo de la ISS
- 3.1.1 Términos de la ISS
- 3.1.2 Ecuación Fundamental de ISS
- 3.1.3 Amenazas del Sistema de Información
- 3.1.4 Vulnerabilidades de los Sistemas de Información
- 3.1.5 Objetivos de Control de los Sistemas de Información
- 3.1.6 Contramedidas de los Sistemas de Información

3.2 Cayendo por la Madriguera del Conejo: Lógica Informática, Complejidad del Sistema y Vulnerabilidad Inherente
- 3.2.1 Cómo Funcionan los Sistemas Informáticos
- 3.2.2 Gestión de la Infraestructura de TI
- 3.2.3 Sistemas Informáticos del Mundo Real
- 3.2.4 Conceptos Adicionales de Seguridad de la Información
- 3.2.5 Tecnologías de Seguridad de la Información

3.3 Marco para los Profesionales de ISS
- 3.3.1 Iso/Iec 27001:2005 E Iso/Iec 27002:2005
- 3.3.2 Cuerpo Común de Conocimientos CISSP
- 3.3.3 Gestión de la Seguridad de la Información: Guía para la Junta de Directores y Gerencia Ejecutiva
- 3.3.4 Principios de Seguridad de los Sistemas de Información Generalmente Aceptados (Gaisp)

3.4 El Nuevo Panorama Legal, Regulador y Contractual Relacionado al ISS
- 3.4.1 Payment Card Industry Data Security Standard (Pci Dss)
- 3.4.2 Health Care And Insurance Portability And Accountability Act (HIPAA)
- 3.4.3 Gramm-Leach-Bliley Act (GLBA)
- 3.4.4 Children's Online Privacy Protection Act (COPPA)
- 3.4.5 Sarbanes-Oxley Act (SOX)
- 3.4.6 Red Flag Rules
- 3.4.7 Medidas de Cumplimiento de la FTC
- 3.4.8 Divulgación de Incumplimiento Estatal y Leyes Relacionadas con los ISS y la Privacidad

3.4.9 Directiva de Protección de Datos de la Unión Europea
3.4.10 Nueva Jurisprudencia

3.5 Temas Especiales de los ISS
3.5.1 Evaluación del Riesgo y Vulnerabilidad de los ISS
3.5.2 Implementación de la Política del ISS
3.5.3 Respuesta a Incidentes

3.6 Gestión Total del ISS
3.6.1 ISO 27001 Sistema de Gestión de la Seguridad de la Información
3.6.2 Haciendo Posible la Mejora Continua

Capítulo 4. **DESAFÍOS EN CONVERGENCIA DE LA SEGURIDAD**

4.1 Riesgo para la Red
4.1.1 Estudio de Caso de Red: Sistema de Cámaras
4.1.2 Estudio de Caso de Red: Control de Acceso

4.2 Ataques de Comunicación
4.2.1 Ingeniería Social
4.2.2 Hacking Directo
4.2.3 Malware
4.2.4 Ataques a la Web

4.3 Sistema de Gestión de Seguridad de la Información
4.3.1 Política de Seguridad
4.3.2 Organización del ISS
4.3.3 Gestión de Activos
4.3.4 Gestión de Recursos Humanos
4.3.5 Seguridad Física y Ambiental
4.3.6 Gestión de Comunicaciones y Operaciones
4.3.7 Control de Acceso
4.3.8 Adquisición, Desarrollo y Mantención de los Sistemas de Información
4.3.9 Gestión de Incidentes de Seguridad de la Información
4.3.10 Gestión de Continuidad del Negocio
4.3.11 Cumplimiento
4.3.12 Resumen del ISMS

4.4 Conclusión

ÍNDICE

TABLA DE FIGURAS

2-1 Diseño Video-a-Grabador
2-2 Infraestructura de Video
2-3 Flujo Básico de Tarjeta de Control de Acceso
2-4 Flujo Básico de Wiegand
2-5 Sistema de Control de Acceso de Red

3-1 Objetivos Generales y Objetivos de Control del ISS
3-2 Componentes Básicos de una Operación Computacional
3-3 Comunicación Directa
3-4 Comunicaciones mediante Router
3-5 Puntos de Entrada Lógica a la Computadora
3-6 Autenticación
3-7 Tríada AAA
3-8 Tríada CIA ampliada
3-9 Firewall
3-10 Red Virtual Privada
3-11 Sistema PBX Tradicional
3-12 Oficina Central de la Compañía de Teléfonos
3-13 Sistema de voz sobre IP (VOIP)
3-14 Nivel de Madurez de la Gestión de Seguridad de la Información
3-15 Modelo Planificar-Hacer-Verificar-Actuar Aplicado a los Procesos ISMS

4-1 Sistema de Video Conectado a una Red
4-2 Sistema de Control de Acceso Conectado a una Red
4-3 Comunicación del Sistema de Control de Acceso: Lector al Controlador a la Red
4-4 Comunicación del Sistema de Control de Acceso: Servidor a la Red
4-5 Flujo Lógico de Comunicación
4-6 Elementos del Control de Acceso Conectados al Switch
4-7 Comunicación de la Capa 2
4-8 Comunicación de Control de Acceso mediante Router
4-9 Flujo de Datos del El puesto de trabajo al Servidor de Control de Acceso

CAPÍTULO 1
PROTECCION DE ACTIVOS DE INFORMACIÓN

1.1 INTRODUCCIÓN

La protección de activos consiste de información sensible e información patentada, datos con derecho a la privacidad, propiedad intelectual, activos intangibles e información definida bajo las leyes internacionales, federales, y estatales, que rigen los secretos comerciales, patentes y derechos de autor. Algunos activos de información específicos son los conocimientos científicos, las marcas, la reputación y los procesos de negocios.

Los activos de información existen en muchas formas, incluyendo el conocimiento de una persona, la información hablada, un proceso o procedimiento, la información escrita en papel, un elemento (como un modelo, prototipo, dispositivo o máquina), datos en una tecnología de información (TI) o sistema de comunicaciones, una transmisión electrónica y datos almacenados en medios electrónicos (CD, DVD, cinta magnética, disco, tarjeta de memoria, dispositivo USB, memoria volátil, etc.). La gran variedad de formas amplía el espectro de métodos de protección que se deben considerar.

Este capítulo aborda la protección de activos de información (IAP de ahora en adelante, por sus siglas en inglés), también conocida como seguridad de la información o protección de información patentada. El objetivo es ayudar al lector a formular un programa IAP, implementar una estrategia de mitigación basada en el riesgo, e identificar las brechas en la protección y las soluciones –al mismo tiempo que contribuir, no obstaculizar, la misión de la empresa u organización. Como señala Richard Heffernan, ex Presidente del Consejo de Protección de Activos de Información de ASIS, “Evaluar y abordar los riesgos *permite* trabajar”.

1.2 HISTORIA DEL ESPIONAJE Y DE LA RECOPILACIÓN DE INTELIGENCIA DE NEGOCIOS

A lo largo de la historia, las organizaciones han intentado robar los activos de información de otras organizaciones. Probablemente el primer registro de espionaje data de alrededor de 1274 a.C. durante la guerra del Faraón Ramsés con los Hititas (Crowdy, 2006, p.15). Posteriormente, alrededor del 500 a.C.,

el estratega militar chino Sun Tzu escribió acerca de cinco clases de espías: espías locales, espías internos, espías convertidos, espías condenados y espías sobrevivientes. Él los llama "la facultad más valiosa del soberano" (Sun Tzu, 1983, pag.78) y sugiere que ellos pueden ser utilizados más allá del campo de batalla, instando a sus lectores a "¡ser sutiles! y usar sus espías para cada tipo de negocios" (Sun Tzu, 1983, p.81).

El histórico comercio de seda entre Asia y Europa proporciona un ejemplo específico de la falta de protección de activos de información. Durante años China ha intentado mantener en secreto sus técnicas para crear gusanos y producir seda. En 552 d.C. el emperador Bizantino Justiniano envió dos monjes a China para sacar de contrabando huevos del gusano de seda y las semillas del árbol de morera (mulberry). Como resultado, China tuvo que enfrentar una significativa competencia en la producción de seda.

Otro ejemplo de recopilación de inteligencia involucra al zar de Rusia Pedro el Grande. En 1967-98, viajó hacia occidente para recoger información sobre tecnología. Con un equipo de expertos militares e industriales, viajó a Polonia, Alemania, Holanda e Inglaterra, estudiando la artillería, construcción naval, operaciones de puerto, cultura occidental, la comunidad científica y la casa de moneda en Inglaterra. A principios de 1700, Pedro estaba empleando mucha de la tecnología y conocimientos de negocios que había adquirido. Años más tarde, bajo otro liderazgo, Rusia usó en contra de Europa occidental el poder económico y militar obtenido por Pedro el Grande.

Uno de los primeros ejemplos de espionaje industrial en Estados Unidos involucra a Francis Cabot Lowell. En 1810, utilizando una historia ficticia de que estaba en Escocia por motivos de salud, Lowell "visitó varias fábricas [textiles] normalmente cerradas a los visitantes, y con su memoria fotográfica, fue capaz de evadir los inspectores de aduana británicos que buscaban planes y bosquejos robados. De regreso en casa, Lowell construyó su primera planta textil en Waltham, Massachusetts, y Estados Unidos entró en buen camino hacia la revolución industrial" (Poteat, 2001). La Agencia Nacional de Detectives Pinkerton, fundada en 1850, continuó la tendencia de Estados Unidos desarrollando un negocio en inteligencia y contrainteligencia.

Cerca del final del siglo diecinueve, Frederick Taylor, considerado el padre de la gestión científica, también se involucró en el espionaje industrial. Él usó varias técnicas subrepticias para investigar denuncias de violaciones de patentes:

- dirigir un agente para obtener un empleo en una compañía sospechosa bajo falsos pretextos
- dirigir un agente para que se haga amigo de los empleados de esa compañía para recopilar información de los procesos de fabricación propios
- dirigir un agente para establecer un falso acuerdo comercial con una compañía para aprender los detalles de sus procesos de fabricación
- reclutando un empleado de la compañía para que proporcione información de los procesos de fabricación

- desarrollando ingeniería inversa

Silencio Significa Seguridad
Cartel de Seguridad del Manhattan Project Era

En la década de 1940, los secretos de las armas nucleares de Estados Unidos fueron el blanco de muchos espías. Había demasiado en juego: "el espionaje soviético dirigido al Proyecto Manhattan probablemente aceleró al menos en 12-18 meses la adquisición soviética de la bomba atómica (United States Department of Energy, 2007).

Durante la Guerra Fría, el espionaje floreció tanto en el ámbito nacional y comercial. Gran parte de la actividad apuntaba a tecnologías de doble uso y a la información –aquellas con aplicaciones militares y comerciales. Desde la perspectiva occidental, la amenaza predominante era la del servicio de inteligencia soviético, la KGB, y su contraparte militar, el GRU. La Línea X de la KGB (Directiva de Ciencia y Tecnología) y sus agencias equivalentes en los estados de Europa del Este apuntaron a las tecnología de doble uso de las compañías privadas, las agencias de gobierno y las universidades.

En la década de 1970, para mitigar las amenazas de espionaje, la recopilación de fuentes abiertas y la búsqueda agresiva de objetivos (aggressive targeting), el FBI instauró el programa Developing Espionage and Counterintelligence Awareness (DECA), el cual estaba destinado a educar a la industria de Estados Unidos –particularmente a los contratistas de defensa- y solicitar su apoyo para reportar actividades sospechosas que podrían representar un blanco de inteligencia. El programa DECA evolucionó hacia el programa Awareness of National Security Issues and Response (ANSIR) y luego al programa Counterintelligence Domain. Actualmente es conocido como Programa de Alianzas Estratégicas de Contrainteligencia (Counterintelligence Strategic Partnerships Program). Estos programas de enlace del FBI fomentan el acercamiento al sector privado y se centran en la protección de la competitividad de Estados Unidos salvaguardando los activos de información de las empresas.

Un hito en la lucha para proteger las tecnologías comerciales y de doble uso en Estados Unidos fue la promulgación de la Economic Espionage Act (EEA) de 1996. La ley transformó en una ofensa federal robar secretos comerciales y dio al FBI la autoridad para investigar el espionaje económico. La ley fue redactada con el aporte de ASIS International y su Consejo de Protección de la Información Privada, ahora el Consejo de Protección del Activo de Información (http://www.asisonline.org/councils/SPI.xml).

Con los años, mientras que las tecnologías empleadas en el espionaje han avanzado enormemente, las

tácticas y técnicas generales se han mantenido muy consistentes. Incluso los planteamientos defendidos por Sun Tzu y Frederick Taylor siguen siendo ampliamente usados hoy en día.

1.3 ENFOQUE DE GESTIÓN DEL RIESGO PARA LA IAP

Todas las organizaciones poseen y usan los activos de información que merecen protección. La naturaleza de esa protección debiera basarse en un buen enfoque de la gestión del riesgo.

El siguiente es un proceso de evaluación para uso en la IAP:

- Identificar los activos de información.
- Valorizar los activos de información (asignando un valor cuantitativo, como dólares, o un valor cualitativo, como alto, medio o bajo).
- Evaluar amenazas para los activos de información. Evaluar los probables adversarios.
- Evaluar la probabilidad de ocurrencia de las amenazas.
- Identificar las vulnerabilidades existentes y las previstas.
- Evaluar el impacto de un evento de pérdida o divulgación en la organización.
- Identificar los controles de seguridad existentes y planificados u otras opciones para enfrentar el riesgo.
- Evaluar y priorizar los riesgos, basado en su probabilidad e impacto organizacional.

Una estrategia de protección de la información debe ser diseñada para apoyar los objetivos, la estrategia y la cronología de la organización. Tal como señala el autor Ira Winkler (2005, p.35):

> Sólo cuando usted comprende los verdaderos componentes del riesgo puede crear una estrategia efectiva y apropiada para proteger su organización y gestionar sus riesgos. Abordando sus vulnerabilidades y *optimizando*, en lugar de *maximizando*, sus esfuerzos de contraespionaje, usted puede mejorar enormemente su seguridad.
>
> Por lo que el objetivo de su programa de seguridad es optimizar el riesgo, nunca minimizarlo. Esta es una diferencia extremadamente importante.

1.3.1 EL ACTUAL ENTORNO GLOBAL DE LA INFORMACIÓN

En términos de intercambio de información, el mundo está interconectado como nunca antes. Debido a este nivel de interconectividad enorme –de hecho global-, las amenazas a los activos de información han llegado a ser más difusas y difíciles de reconocer y pueden actuar más rápido. El nivel de riesgo está aumentando. Como señala Michael D. Moberly, ex presidente del Consejo de Protección de Activos de Información de ASIS International (2006):

> Una lamentable realidad de las transacciones comerciales internacionales es que la probabilidad de que una compañía…experimente alguna forma…de infracción, apropiación indebida, falsificación o piratería de productos, es cada vez mayor.

Hoy en día, los activos de información que están en peligro son casi siempre imposibles de recordar o contener en términos de diseminación (ASIS International, *Trends*, 2007, p.41). Ellos pueden estar en cualquier parte o en todas partes en un instante.

La Office of the National Counterintelligence Executive de Estados Unidos, en su *Annual Report on Foreign Economic Collection and Industrial Espionage* (2006), reconoció los desafíos del entorno global de la información cuando afirmó:

> La feroz competencia económica global permanente alimentará el robo de tecnología comercial…[y] las adquisiciones ilegales de elementos militares y de doble uso…En la medida que la globalización continúa presionando a las compañías estadounidenses para mover importantes tecnologías e incluso instalaciones de investigación y desarrollo en el extranjero, lugares en terceros países pueden llegar a ser cada vez más importantes para la adquisición de tecnología de Estados Unidos. Tanto la seguridad como el marco legal para la protección de las tecnologías en el exterior tienden a ser más débiles…

1.3.2 CATEGORÍAS DE AMENAZAS Y EJEMPLOS

Un elemento clave del modelo de evaluación de riesgos es un estudio exhaustivo de las amenazas existentes y proyectadas. Ellas pueden incluir las amenazas intencionales, naturales e involuntarias.

Amenazas Intencionales

Históricamente, gran parte de la atención se ha centrado en las amenazas intencionales. Para evaluarlas, uno identifica los potenciales adversarios y evalúa sus capacidades e intenciones de dirigirse hacia los activos de información clave. Es importante pensar en términos amplios cuando se consideran los potenciales adversarios. Además de los competidores extranjeros y nacionales, los adversarios pueden incluir gobiernos extranjeros, grupos activistas, grupos terroristas, organizaciones criminales, agentes de información y vándalos.

El FBI (2011) entrega el siguiente resumen del entorno de amenazas actuales:

> La Guerra Fría no ha terminado, simplemente se ha trasladado a un nuevo escenario: el mercado global. El FBI estima que cada año billones de dólares se pierden por los competidores extranjeros y nacionales que deliberadamente apuntan a la inteligencia económica en la floreciente industria y tecnologías estadounidenses, y que sacrifican la inteligencia al dejar de lado las tecnologías explotando las fuentes abiertas de información y los secretos comerciales de la compañía. Los competidores extranjeros que buscan criminalmente información económica, por lo general operan de tres maneras:
>
> 1. Ellos apuntan agresivamente y reclutan personas informadas (a menudo de los mismos antecedentes nacionales) trabajando para empresas estadounidenses e instituciones de investigación;
> 2. Ellos realizan inteligencia económica a través de operaciones como soborno, intrusiones cibernéticas, robo, hurgando en la basura (en búsqueda de propiedad intelectual o prototipos desechados), interceptando teléfonos y;
> 3. Ellos establecen relaciones de negocios aparentemente inocentes entre compañías extranjeras e industrias de Estados Unidos para reunir inteligencia económica incluyendo los secretos comerciales.

La investigación sobre las capacidades e intenciones de los adversarios puede ser desarrollada internamente o mediante un consultor de confianza o una empresa de análisis de amenazas.

Amenazas Naturales

Después de los desastres naturales, muchas compañías se disuelven, no porque perdieron sus instalaciones, sino porque perdieron su información. Por lo general, no tenían un plan de preparación eficaz (incluyendo un respaldo de la información crítica fuera de la instalación y un sitio listo (hot site) o semi-listo (warm site) como parte de un plan integral de continuidad del negocio. A menudo, las compañías que dejan de operar son pequeñas, de un solo sitio, sin funciones robustas de seguridad y gestión de riesgos. Todas la entidades, grandes y pequeñas, deben prepararse para desastres naturales que puedan afectar gravemente sus operaciones.

Amenazas Involuntarias

Tal vez, las amenazas que con mayor frecuencia se pasan por alto son las amenazas involuntarias. Estas también son las más difíciles de identificar y evaluar, pero no pueden ser ignoradas. Como señala Winkler (2004, pp.53-54):

> A pesar que la gente quiere escuchar acerca de los terroristas y hackers (piratas informáticos), el hecho es que las pérdidas más grandes son de la gente en el espejo (people in the mirror)…Las personas cometen errores y esos errores lo más probable es que les hagan daño…Los errores humanos y los accidentes…causan cientos de billones de dólares (en pérdidas) al año. Cuando no se han anticipado apropiadamente, los incidentes pueden literalmente destruir una vida o una compañía.

Las amenazas involuntarias pueden ser atribuidas a un inadecuado entrenamiento de los empleados, malos entendidos, falta de atención a los detalles, aplicación relajada de la seguridad, presión para producir entregas, insuficiente personal u otros factores. Por lo tanto, es esencial desarrollar, promulgar y hacer cumplir políticas prácticas para la IAP.

Unas cuantas amenazas específicas merecen ser mencionadas, porque son prevalentes o representan una tendencia. Los siguientes temas deben ser considerados, según corresponda, cuando se realiza una evaluación de riesgos de IAP o para desarrollar estrategias de mitigación.

Minería de Datos

De acuerdo a *Trends in Proprietary Information Loss* (ASIS International, 2007), el informe de una encuesta realizada por ASIS International, la minería de datos (basada en un software de recopilación de datos de fuentes abiertas e información pública) se ha convertido en una amenaza importante. Del mismo modo, la Office of the National Counterintelligence Executive (2006) expresa las siguientes preocupaciones por el futuro:

> La continua expansión de vínculos internacionales…crearán agentes mundiales especializados en el movimiento de tecnologías a través de las fronteras y socavando la capacidad…para controlar las exportaciones.
>
> Una gran preocupación es el hecho que las naciones mejor preparadas para usar las herramientas cibernéticas para acceder a las tecnologías estadounidenses también son los países que tradicionalmente han sido los más agresivos.

Las entidades del sector gubernamental y privado están usando cada vez más las herramientas

automatizadas para recopilar, filtrar, organizar, analizar y diseminar la información. Un resultado es el crecimiento de los agentes de información. Otro es el desarrollo sitios Web de cursos de recopilación, libros de cómo hacerlo e incluso "inicie su propio negocio casero" en el tema de la minería de datos y corretaje de información. De mayor preocupación es que grupos terroristas internacionales están utilizando la minería de datos y las técnicas avanzadas de gestión del conocimiento para apoyar su obtención de inteligencia y planificación de actividades de ataque.

Personas Informadas (Insiders)

Trends in Proprietary Information Loss (ASIS International, 2007) encontró que la explotación de relaciones de confianza también es una creciente amenaza. Las personas en ese tipo de relaciones incluyen a proveedores, clientes, socios de empresas mixtas (joint venture), subcontratistas y proveedores externalizados. Asimismo, un informe del Defense Personnel Security Research Center (Kramer, Heuer & Crawford, 2005) señala:

> Debido a su conocimiento de las agencias públicas y compañías privadas que los emplean, su familiaridad con los sistemas computacionales que contienen información clasificada y patentada, y su conciencia del valor de la información protegida en el mercado global, los insiders constituyen una importante área de vulnerabilidad para la seguridad nacional…
>
> La revolución de la información, la competencia económica global, la evolución de los nuevos y no tradicionales adversarios de inteligencia y otros cambios en el entorno nacional e internacional, han convergido para crear un campo inusual y fértil para el espionaje de los insiders. Las principales conclusiones de esta investigación son las siguientes:

- Los avances tecnológicos en el almacenamiento y recuperación de la información están mejorando dramáticamente la capacidad de los insiders para acceder y robar información clasificada y patentada.
- El mercado global para la información protegida de Estados Unidos se está expandiendo. Los insiders estadounidenses pueden vender tipos de información a una amplia gama de compradores extranjeros como nunca antes.
- La internacionalización de la ciencia y el comercio está colocando más empleados en posiciones estratégicas para establecer contactos con científicos, empresarios y recolectores de inteligencia extranjeros, y para transferirles material científico y tecnológico.
- El aumento de la frecuencia de viajes internacionales está creando una nueva oportunidad para los vendedores de información motivados para establecer contacto con y transferir información a entidades extranjeras. Los compradores extranjeros tienen mayores oportunidades para contactar y evaluar las vulnerabilidades del personal estadounidense con acceso a información protegida.
- La expansión global de Internet está proporcionando nuevas oportunidades para el espionaje interno. Internet permite a los vendedores y buscadores de información permanecer en el anonimato y proporciona los medios por los cuales se pueden transmitir grandes cantidades de material digitalizado a terceros en el extranjero de manera segura.
- Los estadounidenses son más vulnerables a experimentar graves crisis financieras debido a hábitos de gasto agresivo de los consumidores y otros factores. Los problemas financieros son una fuente común de motivación para el espionaje interno.

- La creciente popularidad de las apuestas y la prevalencia de los trastornos del juego sugieren que un mayor número de insiders cometerán delitos en el lugar de trabajo, tales como el espionaje, para pagar deudas y mantener las actividades de juego.
- Debido a que la lealtad organizacional está disminuyendo, menos empleados pueden ser disuadidos de cometer espionaje debido a al sentido de obligación con sus empleadores. Las condiciones cambiantes en el lugar de trabajo en Estados Unidos sugiere que un mayor número de insiders pueden ser motivados a robar información de sus empleadores para vengarse por el maltrato recibido.
- Ahora, más insiders tienen vínculos étnicos con otros países, se comunican con sus amigos y familiares en el extranjero, e interactúan con empresarios y gobiernos extranjeros. Las conexiones en el extranjero le proporcionan a los insiders oportunidades para transmitir información fuera de Estados Unidos, y los vínculos extranjeros pueden proporcionar la motivación para hacerlo.
- Más estadounidense ven la sociedad humana como un sistema evolutivo de diversidad étnica e ideológica, de grupos y personas interdependientes. Si bien esto es beneficioso en muchos aspectos, también es posible que algunos insiders con una orientación global en los asuntos mundiales, verán el espionaje, en circunstancias extremas, como moralmente justificable si ellos sienten que compartiendo la información beneficiarán la comunidad mundial.

Un estudio de 49 incidentes de insiders concluyó lo siguiente (United States Secret Service, 2005, pp.11-16):

- De los autores, el 59 por ciento eran ex empleados o contratistas de la organización afectada, mientras que el 41 por ciento eran actuales empleados o contratistas.
- El rango de edad de los autores era de 17 a 60 años.
- Tres de diez autores tenían registros de arrestos anteriores.
- Un evento negativo relacionado con el trabajo gatilló sus acciones en casi todos los casos.
- En el 80 por ciento de los casos, el autor llamó la atención de la gerencia debido a comportamientos inapropiados antes del incidente (v.gr, atrasos, ausencias, discusiones con los compañeros de trabajo, o un deficiente desempeño laboral).
- En el 31 por ciento de los casos, otros tenían información acerca de los planes del autor de causar daño; en el 20 por ciento de los incidentes se realizó una amenaza directa.

Falsificación y Piratería

Desde los tejanos (jeans) y las carteras hasta los productos químicos y farmacéuticos, la falsificación y la piratería son problemas cada vez mayores, con implicancias tanto económicas como de seguridad. En una declaración reciente, la United States General Accountability Office (2007) afirmó que:

> Los esfuerzos del gobierno para proteger y hacer valer los derechos de propiedad intelectual (IP de ahora en adelante, por sus siglas en inglés), en el país y en el extranjero son cruciales para prevenir billones de dólares en pérdidas para la industria estadounidense y los los propietarios de derechos IP y para evitar los riesgos de salud y seguridad asociados al comercio de productos falsificados y pirateados.

La amenaza de falsificación y piratería tiene grandes consecuencias, particularmente sobre las pequeñas empresas, las cuales están entrando cada vez más al mercado global y operando internacionalmente. Como señala Moberly (2006):

> Emprendimientos, empresas en etapa inicial y pequeñas y medianas empresas que son ricas en activos intangibles, por lo general no reconocen el alcance o impacto económico de la falsificación y piratería a nivel mundial. Tampoco parecen darse cuenta de cuán reactivas son la mayoría de las defensas convencionales (v.gr., patentes, derechos de autor, marcas registradas) frente a la piratería de nanosegundos y la falsificación.

1.3.3 EVALUACIÓN DEL RIESGO Y DUE DILIGENCE[1]

A veces, en el mundo de los negocios se dice que "usted no puede gestionarlo si no puede medirlo". Las evaluaciones de riesgos deben identificar los riesgos, cuantificarlos y priorizarlos de acuerdo al criterio de aceptación del riesgo de la organización. Los resultados de la evaluación deben ayudar en la selección y priorización de las acciones para gestionar los riesgos.

Se deben realizar evaluaciones regularmente e incluir un seguimiento de los riesgos para enfrentar los cambios en los requerimientos de seguridad, así como los cambios en la naturaleza de los activos de información, amenazas, frecuencia de ocurrencia de la amenaza, vulnerabilidades e impactos. Además, el seguimiento ayuda a evaluar la efectividad de la seguridad y otras medidas de mitigación de riesgo.

1.3.4 LOGRAR EL COMPROMISO

EL compromiso de los ejecutivos es esencial para la IAP. Debido a que la información, los activos intangibles y la propiedad intelectual son parte integral de casi cualquier organización, se podría esperar que fuera fácil convencer a los ejecutivos de adoptar y apoyar un programa de protección de activos de información. Sin embargo, a menudo es difícil lograr tal compromiso, debido a la naturaleza intangible de los activos. Por lo tanto, los profesionales de IAP deben esforzarse para tener un argumento de negocios (business case) convincente a favor de estrategias proactivas, dedicación de recursos y la capacidad de hacer aportes al proceso de toma de decisiones del negocio –en otras palabras, para conseguir un puesto en la mesa.

Un paso hacia este fin es articular los impactos en el negocio de un evento de pérdidas. De acuerdo a *Trends in Proprietary Information Loss* (ASIS International, 2007), los principales impactos en el negocio son los siguientes:

- pérdida de la reputación/imagen/predisposición comercial de la empresa
- pérdida de la ventaja competitiva de un producto/servicio
- reducción del retorno o rentabilidad proyectada/anticipada
- pérdida de las tecnología o procesos fundamentales del negocio
- pérdida de ventajas competitivas en múltiples productos/servicios

Otros impactos de la pérdida de información patentada incluyen la pérdida de uso, propiedad o control de los derechos de propiedad intelectual, así como la pérdida de información confidencial o prototipos que facilitarían la falsificación del producto.

El personal de gestión de seguridad también puede destacar que la IAP beneficia el negocio porque hace lo siguiente (Moberly, 2007):

- mejora la supervisión fiduciaria, el control y la administración de activos intangibles clave
- alinea los activos de información con las operaciones del negocio y la visión estratégica de la organización
- permite una asignación más eficiente de los recursos de seguridad tradicionales y de TI
- permite una búsqueda más oportuna de los compromisos de los activos de información y de las violaciones a los derechos de propiedad intelectual (IPR de ahora en adelante, por sus siglas en inglés)
- sirve como ventaja en la negociación de la cobertura y de las primas de seguros de propiedad intelectual (IP) y de tecnología de información (TI)
- proporciona consistencia en los informes reglamentarios de activos intangibles
- estandariza el manejo interno y externo de los activos intangibles
- identifica las fuentes internas y externas clave de activos intangibles y capital intelectual

Otros enfoques sugeridos por Moberly incluyen el uso de métodos cuantitativos por parte de los profesionales de IAP cuando sea posible y asumir el rol de un recurso de negocios (uno facilitador, no un impedimento) para la empresa. Finalmente, la responsabilidad por la protección de los activos de información recae en los líderes de una organización.

Gerentes de nivel medio, también, deben ser convencidos para que un programa IAP tenga éxito (Winkler, 2005):

> Obtener el apoyo de la gerencia de primer y segundo nivel es fundamental. Los gerentes que ven a los empleados todos los días son los que realmente estarán allí para darse cuenta cuando las personas siguen las prácticas de seguridad y cuando no. Estas son las personas que más pueden influir en seguridad.

Finalmente, el programa de IAP debe ser asimilado por cualquier otra persona –dentro o fuera de la empresa- que tenga acceso a los activos de información de la compañía.

1.4 MÉTODOS PARA LA MITIGACIÓN DEL RIESGO

Gran parte del siguiente contenido proviene de *Information Asset Protection Guideline* (2007) de ASIS International.

1.4.1 PRÁCTICAS BÁSICAS DE PROTECCIÓN

El FBI (2011) enumera los siguientes pasos para proteger una empresa del espionaje:

- Reconocer que hay una amenaza interior y una exterior a su empresa.
- Identificar y valorar los secretos comerciales.
- Implementar un plan proactivo para proteger los secretos comerciales.
- Tener versiones físicas y electrónicas de los secretos comerciales.
- Circunscribir el conocimiento intelectual sobre la base de la "necesidad de saber".
- Hacer una capacitación a los empleados sobre el plan de propiedad intelectual y de seguridad de la compañía.

Las medidas que siguen son consistentes con el enfoque del FBI. La mayoría puede ser aplicada a cualquier organización privada o pública.

Sensibilización y Políticas de la IAP

Políticas claras, prácticas y bien promulgadas fortalecen cualquier programa de seguridad. Al desarrollar una política, hay varios pasos vitales:

- La dirección de la organización debe demostrar su compromiso con la IAP, proporcionando los recursos apropiados y exigiendo a todas las unidades de la empresa que desarrollen las estrategias para alinear los negocios y los objetivos de protección.
- Un grupo, persona o departamento específico debe ser asignado a la gestión y auditoría de la política
- Se les debe exigir adherirse a la política a todas las unidades de la empresa, personal, empleados temporales, proveedores, consultores, contratistas y socios del negocio.
- Se debe entregar en forma reiterada una capacitación de la IAP en las sesiones de orientación para los nuevos empleados; durante las inspecciones, en conferencias con todo el personal, y visitas a otras instalaciones; en la intranet de la empresa; los boletines; y como parte de la capacitación de TI o de recursos humanos.
- Los esfuerzos de sensibilización y capacitación de la IAP deben ser documentados.

Es importante identificar qué información debe ser protegida y cuándo, y luego identificar las muchas formas que puede tomar esta información durante su ciclo de vida. Sólo un cierto segmento de la información de la organización puede justificar la protección. Una vez que esa información es identificada, se debe clasificar de modo que los activos de información más importantes reciban el mayor grado de protección.

La declaración de la política establece el tono para la organización y, si se hace cumplir, puede apoyar acciones legales si se vuelve necesario. La política debe clarificar que la información es uno de los

recursos más importantes de la organización, que toda la información necesita ser evaluada apropiadamente según su sensibilidad, y que las medidas de protección deben ser suficientes para garantizar la confidencialidad, integridad, disponibilidad, responsabilidad, capacidad de recuperación, auditabilidad y autenticación de la información, tanto en el entorno físico y cibernético. Se deben realizar al azar para asegurar el cumplimiento de la política de IAP.
En el Anexo A se encuentra un ejemplo de declaración de política para IAP.

Identificación y Marca de la Información Protegida

La información que merece protección debe ser adecuadamente identificada y marcada. Se usan varios niveles para distinguir el grado de sensibilidad o el grado de protección que requiere: confidencial, restringida, limitada, no pública, etc. La mayoría de las organizaciones usan dos o cuatro niveles de sensibilidad.

Por ejemplo, muchas empresas dividen la información en tres categorías: aprobada para divulgación externa (acceso sin restricción), interna (limitada a los empleados y contratistas) y confidencial (limitada por una necesidad de conocimiento específica). La información puede ser electrónica, oral, escrita u otras formas. Siempre que sea práctico, el material debe ser marcado o etiquetado. Generalmente, quien originó la información determina el nivel de clasificación y los usuarios autorizados no pueden divulgar los contenidos sin la aprobación del propietario.

El acceso a la información interna debe restringirse al personal de la compañía u otras personas que hayan firmado un acuerdo de no divulgación. Las normas para autorizar el acceso también pueden incluir una investigación de antecedentes satisfactoria. El acceso de un empleado se debe basar en su función de trabajo actual y en la necesidad de conocimiento, no solamente en el cargo o nivel de gerencia.

1.4.2 SEGURIDAD FÍSICA

Los profesionales de IAP deben coordinar estrechamente con el personal de seguridad física para armonizar los esfuerzos de protección en varias categorías.

Protección en Capas (Defensa en Profundidad)

Este concepto, que aplica una visión de anillos o capas concéntricas de protección para cualquier activo, comúnmente se utiliza más en términos de seguridad física. El mismo enfoque, no obstante, debe ser empleado en la protección de los activos de información sensible. La defensa en profundidad puede ser vista desde tres perspectivas diferentes, en las cuales los anillos concéntricos o capas de protección representan lo siguiente:

- Incremento de los niveles de confianza para aquellos a quienes se les da acceso a capas sucesivas. Por ejemplo, un miembro del personal de mantenimiento probablemente tendrá un nivel de confianza menor (y por lo tanto acceso) que el director de investigación y desarrollo de la empresa. Basado en sus respectivos niveles de confianza, cada uno de ellos tendría niveles de acceso apropiados, pero diferentes, a la información o instalaciones.

- Diferentes tecnologías o medidas de seguridad que operan concertadamente. Mediante la aplicación de tecnologías o medidas de seguridad superpuestas y diversas, el personal de seguridad puede identificar y llenar los vacíos en la cobertura de protección. Los beneficios deben ser sopesados con los costos.
- Capas sucesivas empleadas para demorar, detectar y disuadir a los intrusos. Cada capa de protección sucesiva puede demorar aún más a un adversario, ofrecer una oportunidad adicional para detectar la intrusión y disuadir al adversario de avanzar.

Estas perspectivas aplican igualmente a los sistemas de protección automatizados y a la información en otras formas (disco duro, proceso, conocimiento, intangible, etc.).

Para implementar la protección en capas, un profesional de IAP debe hacer lo siguiente:

- Aplicar múltiples niveles o capas de medidas de protección a los activos de información críticos, apropiados a su sensibilidad y exposición a la pérdida.
- Garantizar que los sucesivos niveles o capas de medidas de protección se complementen en lugar de entrar en conflicto entre ellas.
- Elaborar una estrategia coordinada que integre diferentes familias de medidas de protección, tales como seguridad física, personal de seguridad, seguridad técnica, control de acceso, educación y concienciación, y políticas y procedimientos.

Normalmente, las instalaciones y los sistemas de información de la compañía deben contar con protección de entrada no autorizada en todo momento. El acceso a información interna o confidencial debe requerir autenticación vía presentación de credenciales de acceso única, previamente autorizadas, físicas y lógicas. El nivel de acceso otorgado debe ser consistente con el nivel de información que la persona necesita para su trabajo.

Manejo de Documentos y Registros

Estas funciones representan la gestión diaria de la información sensible en papel o en forma electrónica. Se recomiendan los siguientes pasos de protección:

- Colocar trituradoras o receptáculos seguros de recolección cerca de las impresoras, fotocopiadoras y máquinas de fax.
- Colocar avisos en esas áreas para recordar a los empleados que deben destruir las copias sobrantes o con error de impresión.
- Cuando corresponda, documentar cualquier transferencia (interna y externa) de registros o documentos sensitivos.
- Seleccionar cuidadosamente los contratistas que destruyen registros, documentos o información sensible.
- Destruir registros e información sensible de manera que impida una reconstrucción consistente con

su nivel de sensibilidad, y documentar la fecha y lugar de destrucción.

- Destruir los registros obsoletos regularmente, conforme a la programación de retención de registros.
- Destruir los registros incidentales y duplicados sobre una base regular.
- Almacenar los medios en espera de destrucción en contenedores seguros.
- Si es posible, evitar desechar los medios destruidos en receptáculos de basura accesibles al público.
- Cuando los registros y la información estén siendo transportadas, protegerlos con contenedores cerrados, sellos, escoltas, etiquetas de identificación de radiofrecuencia, registros de transporte y otros medios.

En el Anexo E se presenta más información sobre la eliminación y destrucción de documentos.

Protección de la Información en Forma Física

- Prototipos y modelos
  - A estos se les debe otorgar la misma seguridad física, control de acceso, clasificación, investigación de antecedentes de los empleados, verificación y documentación que a los otros activos de información.
  - Los prototipos, modelos y artículos de prueba obsoletos deben ser destruidos de modo que no se pueda realizar ingeniería reversa.
  - Los contratistas y proveedores encargados de prototipos, modelos o artículos de prueba deben ser contractualmente obligados a protegerlos de acuerdo a las políticas y procedimientos del propietario. Además, se les deben dar las instrucciones para la devolución o disposición de los artículos cuando ya no se necesiten.
- Equipos y Procesos de Fabricación
  - El acceso a las instalaciones de producción o procesamiento se debe restringir a los empleados que necesitan acceso para llevar a cabo sus responsabilidades
  - Se debe restringir la fotografía en las áreas de producción o procesamiento
  - Los contratistas con acceso a las áreas de producción o procesamiento deberían firmar acuerdos de no divulgación como los que se requieren para el manejo de otra información sensible
  - Los empleados, contratistas y visitantes que entran a las áreas de producción o procesamiento deben mostrar sus credenciales de identificación indicando su estado y nivel de acceso autorizado. Además, los visitantes deben ser obligados a firmar en un sistema automatizado de control de visitas o registro de visitas
  - Los equipos de producción obsoletos o dañados, así como la chatarra, deben ser eliminados de manera que no se ponga en peligro o se divulgue información respecto al área de producción o procesamiento.

  - La información relacionada con la actividad del muelle de carga (como materiales y cantidades recibidas en los envíos) también pueden requerir protección
- Compartimentación y barreras físicas o visuales
  - La información de diferentes clasificaciones deben ser almacenadas separadamente
  - Se deben usar protecciones como barreras y cubiertas cuando la información sensible pueda ser expuesta a la vista de personas no autorizadas

1.4.3 PERSONAL DE SEGURIDAD

La seguridad del personal juega un rol clave en un IAP. Esto incluye aspectos como investigación de due diligence de potenciales socios, investigaciones estándar de selección previas al empleo e investigación de antecedentes de subcontratistas, proveedores y consultores.

El proceso de selección a menudo está fuera del control de seguridad, gestión de riesgos o las funciones de IAP, y en su lugar pueden ser manejados por los departamento de recursos humanos o legal. Un desafío adicional es que esas investigaciones por lo general requieren largos plazos. Por lo tanto, los procedimientos a veces son eludidos, y posiblemente ponen los activos de información en mayor riesgo.

Para superar estos desafíos, el profesional de IAP debe establecer un canal de comunicación eficaz con los otros elementos organizacionales involucrados en estas funciones de selección; garantizar que la investigación de antecedentes cubra todas las potenciales personas de confianza con quienes la información protegida pudiera ser compartida; y revisar periódicamente la selección de personal, due diligence y procedimientos de investigación de antecedentes.

1.4.4 PROTECCIÓN DE LA PRIVACIDAD

Todas las organizaciones manejan información privada que pertenece a sus empleados, la gerencia, sus relaciones, clientes u otras personas. En algunas organizaciones esto incluye información que es clasificada como “Información de Identificación Personal” o “PII” (por sus siglas en inglés). Para mantener la confianza y cumplir los requerimientos legales, los profesionales de IAP deben hacer lo siguiente:

- Establecer políticas de privacidad específicas y designar un empleado responsable de implementar y administrar el programa de privacidad.
- Evaluar la información de privacidad relacionada con los empleados, proveedores, clientes y otras personas, y determinar los requerimientos legales y reglamentarios.
- Asegurar los sistemas establecidos para proteger la privacidad de empleados y clientes.
- Proporcionar un mecanismo para investigar el compromiso de la privacidad de la información (incluyendo el robo de identidad) e informar los incidentes a las personas u organizaciones

afectadas (víctimas) según corresponda.

- Revisar las directrices federales, estatales e internacionales aplicables, tales como aquellas mostradas en el sitio Web de U.S. Federal Trade Commission (www.ftc.gov/privacy) y en varias directivas de protección de los datos de la Union Europea para garantizar el total cumplimiento con las leyes y reglamentos aplicables.
- Marcar claramente la privacidad de la información para indicar cómo se usará la información y cómo se pondrá a disposición de otros, qué notificaciones y acciones se deben realizar si se ve comprometida y las instrucciones para su destrucción o disposición cuando la información ya no sea necesaria.
- Realizar un programa de auditoría para garantizar que las políticas de privacidad se han implementado apropiadamente.

1.4.5 PRÁCTICAS EMPRESARIALES

ASIS International sostiene que la seguridad es una función de negocios. Por lo tanto, los principios de IAP deben ser incorporados a las prácticas cotidianas y a la cultura de la empresa. Por otra parte, los aspectos clave de la misión y filosofía de negocios de la organización deben ser incluidas en la estrategia de la IAP. Los siguientes son algunos pasos para la armonización de la IAP y las prácticas generales de negocios:

- Coordinar las materias de IAP con todos los medios apropiados de la compañía: legal, recursos humanos, seguridad, gestión de riesgos, protección, TI, investigación y desarrollo, contrataciones, marketing, relaciones públicas, capacitación, logística, inteligencia competitiva, relaciones internacionales, contabilidad y finanzas, instalaciones y otros.
- Incorporar la IAP en el plan de continuidad del negocio de la organización para garantizar que la información crítica conserva su disponibilidad, confidencialidad e integridad durante todas las fases de situaciones de crisis, incluyendo la respuesta y recuperación.
- Incorporar el material relacionado a la IAP en los programas de capacitación y desarrollo profesional de los empleados.
- Comunicar los asuntos de la IAP a todos los niveles de gestión.

Una actividad de negocios que plantea riesgos especiales para la información de una compañía es el establecimiento de relaciones (tales como sociedades o acuerdos de externalización) con otras compañías, nacional e internacionalmente. En esas relaciones, las compañías pueden bajar la guardia sin darse cuenta respecto a la protección de la información. En estados Unidos, miles de compañías de fachada se han establecido, a menudo a través de gobiernos extranjeros, para recolectar información de las empresas estadounidenses. Por lo tanto, es esencial realizar investigaciones de due diligence antes de asociarse con –y compartir información con- otras compañías.

1.4.6 OPERACIONES DE SEGURIDAD O GESTIÓN DE RIESGOS DE LA INFORMACIÓN

Seguridad de las operaciones (OPSEC de ahora en adelante, por sus siglas en inglés) es un método de protección desarrollado en las fuerzas armadas para proteger la información no clasificada que pudiese revelar planes y operaciones sensibles. En 1988, en Estados Unidos, la National Security Decision Directive instituyó la OPSEC en toda la rama ejecutiva del gobierno federal. Desde entonces, ha sido aplicada con éxito a la protección de la investigación y desarrollo de información sensible, información técnica, datos de prueba de productos, información sensible de los organismos encargados de hacer cumplir la ley y a la información comercial de los esfuerzos de inteligencia competitiva.

En efecto, OPSEC es un sistema de "gestión de riesgos de la información" y a veces es llamado por ese nombre en el sector privado. Llama a visualizar el panorama general e identificar cualquier vacío en la protección que permanezcan a pesar de las actuales medidas de seguridad. Esos vacíos representas caminos por los cuales los activos de información podrían estar en peligro, ya sea intencionalmente o involuntariamente. Los vacíos pueden existir, por ejemplo, entre las estrategias legales y de seguridad o entre las medidas de protección en diferentes países. OPSEC o gestión del riesgo de la información se debe practicar en las organizaciones de cualquier tamaño, pero es particularmente valiosa para las pequeñas empresas que pueden no tener una gran cantidad de personal de seguridad o de IAP o de recursos de seguridad (Peterson, 2005).

OPSEC responde al hecho que pequeños pedacitos de información tomada de distintas fuentes pueden ser combinadas para revelar información sensible. Los siguientes pasos pueden ayudar a las organizaciones a prevenir la revelación de esos pequeños, pero combinables pedacitos de información:

- Desarrollar políticas de IAP específicas, hechas a medida para los proyectos clave.
- Asegurarse que la información periférica (como las órdenes de suministro o planes de contratación), mejoras a la instalación y otras actividades observables e indicadores no proporcionen inteligencia valiosa a un adversario o competidor.
- Considerar la vulnerabilidad de la información revelada a entidades externas como parte acuerdos con una empresa mixta o socio de confianza (proveedor, vendedor, cliente). La otra entidad puede no tener suficientes medidas de IAP.
- Examinar la información de la compañía disponible al público para determinar si, en su conjunto, revela información sensible. Revisar periódicamente el sitio Web de la compañía y los sitios de cualquier socio.
- Evaluar las vulnerabilidades adoptando la perspectiva del adversario. Defenderse de las técnicas de recolección realistas.
- Implementar un proceso de autorización para cualquier presentación, ponencias, o artículos que puedan contener información pertinente a actividades sensibles o planes.

1.4.7 SEGURIDAD DE VIAJES Y REUNIONES

La información sensible puede ser particularmente vulnerable cuando los empleados viajan, asisten a ferias y participan en reuniones dentro o fuera de la empresa.

Viajes Nacionales e Internacionales

Circunstancias especiales, amenazas y vulnerabilidades pueden surgir durante un viaje de negocios. Los que viajan por negocios con cualquier forma de información sensible pueden hacer lo siguiente para reducir el riesgo de esa información:

- Tenga una reunión informativa de seguridad previa al viaje o consultar las recomendaciones de viajes, notificaciones, servicios de información y publicaciones antes de la salida. El U.S. Department of State's Overseas Security Advisory Council (OSAC) es una fuente para esa información.
- Mantener un bajo perfil para minimizar ser un blanco. Evitar usar elementos que visiblemente divulguen el empleador del viajero o identidad personal o nacional.
- Restringir la información que se lleva a lo que es estrictamente necesario.
- Portar la información personalmente, no en equipaje facturado, y no entregar el equipaje que contiene información sensible a encargados de equipaje o botones.
- Estar consciente del riesgo de la vigilancia técnica (interceptación electrónica).
- Evitar trabajar o conversar información sensible en áreas públicas o en transporte público.
- Usar filtros de privacidad para pantallas, candados de cable y otras medidas para proteger la información en las computadoras.
- Evitar el uso de máquinas de fax de hoteles, instalaciones de fotocopias y centros de negocios para la información sensible.
- Si es necesario transferir archivos electrónicos a la computadora de otra persona para facilitar la impresión, copia o proyección, asegúrese después de borrar esos archivos y cualquier archivo temporal.
- Reportar el intento, sospecha o real obtención de información durante el viaje.

Ferias Profesionales

Las ferias profesionales son un lugar de reunión tradicional para la recolección de inteligencia empresarial y gubernamental. La U.S. Office of the National Counterintelligence Executive (2006) llama a las convenciones y exposiciones una amenaza particular:

> Estas visitas siguieron proporcionando información útil a los recolectores. Las convenciones, exposiciones y seminarios ofrecían fantásticas oportunidades de recolección para las entidades extranjeras, debido a que vinculaban directamente los expertos extranjeros con los especialistas, programas y tecnologías estadounidenses. Más aun, estos lugares dieron a los especialistas extranjeros la oportunidad de comparar y contrastar las diferentes tecnologías y hacer preguntas técnicas para llenar los vacíos de inteligencia.

Los siguientes pasos pueden ayudar:

- Establecer un programa de sensibilización para la IAP y un mecanismo de información adaptado a

las personas que viajan a las ferias profesionales, conferencias, simposios, y reuniones técnicas. El programa debe abordar las técnicas de obtención, entre otros tópicos, y recordar a los viajeros de cualquier acuerdo de no divulgación.

- Identificar los viajeros de alto riesgo basado en sus cargos, proyectos, accesos o acreditación dentro de la compañía. Desarrollar procedimientos especiales para ese tipo de viajeros.
- Considerar documentar toda la información y equipamiento (tales como computadoras portátiles o dispositivos portátiles) que se llevarán a las reuniones. Si corresponde, hacer copias de respaldo de la información.
- Interrogar a los viajero a su vuelta cuando sea apropiado (por ejemplo, viajero de alto riesgo o viajeros que asisten a conferencias técnicas en el extranjero).

Reuniones Dentro y Fuera de la Empresa

La reuniones dentro y fuera de la empresa, especialmente aquellas de naturaleza comercial o científica, tienen una larga historia de ser blancos de recolección de información y desarrollo de relaciones con los asistentes. Los siguientes pasos pueden ayudar a los profesionales de IAP a reducir el riesgo que representan ese tipo de reuniones:

- Obtener un programa anual de las reuniones de negocios estratégicas y críticas de la organización y desarrollar una estrategia de IAP para cada reunión si es necesario, basado en la evaluación de riesgos.
- Antes de confirmar un lugar, obtener los planos del piso y detalles relativos a las telecomunicaciones e infraestructura audiovisual del lugar.
- Alentar a los planificadores de reuniones a seleccionar sitios y habitaciones basados en cuestiones de protección de la información.
- Organizar eventos de bajo perfil cuando sea apropiado, minimizando la señalización y anuncios electrónicos de los eventos, patrocinadores, ubicación de las salas y horarios. Usar nombres de reuniones que no sugieran el tema o identifiquen a los asistentes.
- Determinar la necesidad de realizar una inspección técnica de contramedidas de vigilancia antes y durante las reuniones. Las vulnerabilidades pueden incluir micrófonos inalámbricos no encriptados, auriculares inalámbricos, salidas de audio, equipos electrónicos traídos por los participantes u otras personas, y equipos de telecomunicaciones sin seguridad, cables y terminales.
- Determinar la necesidad de envíos y almacenamiento seguro antes, durante y después del evento.
- Mantener la seguridad de los materiales impresos y los medios informáticos durante la reproducción, transporte y almacenamiento.
- Minimizar la distribución de información impresa.
- Asegurarse de que las presentaciones electrónicas están protegidas durante la creación, edición, transmisión y presentación. También, asegurarse que sean completamente eliminadas de cualquier computadora usada para la presentación que no sea de propiedad de la compañía.

- Asegurarse que los proveedores siguen prácticas de seguridad de la información apropiadas.
- Hacer los arreglos necesarios para limitar el acceso a las salas de reuniones. Si corresponde, usar oficiales de seguridad para proveer seguridad durante las 24 horas en las salas de reunión y equipos electrónicos, incluyendo las computadoras portátiles
- Recoger la información y notas dejadas por los asistentes. Hacer los arreglos para su eliminación segura

1.4.8 PREVENCIÓN Y DETECCIÓN DE LA FALSIFICACIÓN Y COPIA ILEGAL

Los siguientes pasos pueden ayudar a los profesionales de IAP a prevenir y detectar la falsificación y copia ilegal:

- Monitorear Internet para identificar los productos falsificados.
- Entrenar a los empleados para observar productos falsificados y sospechosos conocidos, competidores u otros esquemas comunes.
- Exigir a todos los empleados, proveedores, subcontratistas que firmen acuerdos de no divulgación (NDA por sus siglas en inglés).
- Emplear tecnología anti-falsificación.
- Numerar todos los informes y memorandos técnicos.
- Realizar regularmente auditorias de cumplimiento y control de inventario, dentro y fuera de la organización.
- Trabajar con los organismos encargados de hacer cumplir la ley y las agencias fiscales en la detección, conciencia, alertas e intercambio de información
- Considerar la participación en el programa U.S. Customs and Border Protection (CBP) Intellectual Property Rights e-Recordation (https://apps.cbp.gov/e-recordations). Bajo el programa, los dueños de propiedad intelectual pueden registrar sus derechos de autor y marcas aunque mediante un proceso de registro electrónico. Este programa de inscripción permite a CBP detener cualquier producto registrado sospechoso de ser una violación de los derechos de autor o leyes de marca registrada de Estados Unidos, y a notificar al propietario del activo.

1.5 PROTECCIONES LEGALES

En Estados Unidos, la privacidad de la información protegida está regulada específicamente por la Health Insurance Portability and Accountability Act (HIPAA), la Ley de Privacidad y Ley de los Servicios Financieros (Gramm-Leach-Bliley Act); en la Unión Europea por la Data Protection Directive; y por otras leyes y reglamentos en todo el mundo[2]. Todos los programas exitosos de IAP asignan a un especialista la responsabilidad de monitorear la legislación y reglamentos en trámite relacionados con la

protección de los activos de información. Es muy importante evaluar cualquier posible efecto que esos cambios puedan tener en la organización.

A continuación se enumeran los temas a discutir con el asesor legal de la organización:

- tomar medidas coercitivas sobre cualquier patente, derecho de autor, o violación a una marca comercial/de servicio
- conocer los actuales protocolos legales y jurisprudencia para ayudar a determinar la pérdida de beneficios (lucro cesante) y daños financieros y decidir las estrategias de protección apropiadas
- conocer el estado de protección de los derechos de propiedad intelectual y la naturaleza de las violaciones en cada jurisdicción donde la organización planea hacer negocios

Además, los propietarios de los activos de información deben reconocer que las protecciones legales son eficaces sólo si el propietario está dispuesto a perseguir el recurso cuando se produce una violación. Esta actividad puede consumir una gran cantidad de tiempo y recursos financieros. Los propietarios de los activos deben analizar por anticipado el criterio previsto para resolver violaciones cuando ocurran.

Según la Patent and Trademark Office de Estados Unidos (2007), una patente es un derecho de propiedad concedido a un inventor para excluir a otros de fabricar el invento, usarlo, ofrecerlo para la venta, o venderlo el invento por tiempo limitado; una marca comercial consiste de palabras, nombres, símbolos, dispositivos, o imágenes aplicadas a productos o usadas en relación a bienes o servicios para identificar su origen; y un derecho de autor es usado para proteger la expresión de ideas en obras literarias, artísticas y musicales.

La mejor manera de empezar a abordar la infracción de patentes, derechos de autor y marcas comerciales es registrando esos derechos. Es responsabilidad del dueño de la propiedad intelectual conocer y cumplir los requisitos relacionados con la protección de esos derechos en cada jurisdicción relevante. Es importante buscar la ayuda de un experto cuando se registren patentes, marcas comerciales y derechos de autor y cuando se enfrente una potencial infracción. También puede ser útil la participación en organizaciones de lucha contra la falsificación.

El Departamento de Estado de Estados Unidos proporciona asesoría en los temas de derechos de propiedad intelectual en muchos países, generalmente listados bajo “IPR Tool Kit” (kit de herramientas de derechos de propiedad intelectual) en el sitio Web de la embajada específica. Por ejemplo, los temas de derechos de propiedad intelectual en China se discuten en http://beijing.usembassychina.org.cn/ipr.html.

1.5.1 DERECHOS DE AUTOR

Según el derecho internacional, los derechos de autor no tienen que ser registrados para ser protegidos. No obstante, un autor o poseedor de derechos de autor puede formalizar su propiedad a través del registro de gobierno, el cual puede ayudar en cualquier acción de cumplimiento posterior.

El titular de los derechos de autor no debe permitir que el control de los derechos caiga en manos de los agentes o distribuidores de la organización. Es importante hacer lo siguiente:

- Incorporar los derechos de autor en los contratos y estrategias de marketing.
- Suscribir contratos escritos que exijan que agentes, proveedores, distribuidores y empleados protejan los derechos de autor.
- Negarse a ceder o autorizar los derechos de autor hasta que las consecuencias sean totalmente comprendidas.
- Asegurarse que los derechos de autor se mantienen en la organización hasta el término de la cesión, licencia, transacción o inversión.

Si una organización descubre que su derecho de autor ha sido violado, es esencial adoptar medidas inmediatamente. Las herramientas de respuesta incluyen:

- contratación de un asesor legal;
- informar a las autoridades correspondientes;
- realizar investigaciones, allanamientos e incautaciones; y
- iniciar litigios civiles, procedimientos administrativos y procesos criminales.

Al decidir qué herramientas usar, ayuda el formularse las siguientes preguntas:

- ¿El derecho de autor está registrado o susceptible de protección en el país en particular?
- ¿El daño se está causando en ese país o en el extranjero?
- ¿Cuál es el origen del daño: competidores, empleados, agentes o contratistas?

1.5.2 MARCA COMERCIAL, IMAGEN COMERCIAL, MARCA DE SERVICIO

Los nuevos participantes del mercado deben desarrollar una estrategia para proteger la propiedad intelectual de la compañía en las primeras etapas de planificación de la actividad comercial en cualquier país. El registro de las marcas comerciales antes de que el producto entre en la corriente del comercio en cualquier país es el medio más importante para asegurarse que la marca es susceptible de protección bajo las leyes de ese país y garantizar que la infracción de la marca comercial puede ser remediada a través de procedimientos administrativos o judiciales. También es importante aplicar la marca comercial o de servicio apropiada y los avisos a materiales producidos por la compañía.

Cuando se realizan negocios fuera del país de origen de la organización, la mejor arma es la prevención. Los siguientes son algunos pasos prácticos:

- Familiarizarse con los derechos de la organización antes que el producto cruce la frontera.
- Desarrollar y registrar una versión en el idioma del país anfitrión. De lo contrario, el mercado puede hacerlo, creando un apodo para el producto. A la compañía puede que no le guste ese

nombre, o alguien más en el país puede registrarlo, obligando a la compañía a comprar los derechos.

- Registrar la marca comercial en los países vecinos para proporcionar la protección para una potencial expansión y evitar que otros registren las marcas en productos que los consumidores pueden confundir con los de la compañía.
- Realizar una investigación para identificar los productos que infringen la marca comercial o que tenga una marca registrada tan similar que se puede confundir con la de la compañía, pero registrada por un tercero.

1.5.3 PATENTES

Un inventor puede proteger una invención patentándola o considerándola un secreto comercial. Las patentes conllevan una serie de beneficios, pero requieren que el inventor divulgue públicamente los elementos de la invención, y una patente dura sólo 20 años. Por el contrario, un secreto comercial no es divulgado y puede durar indefinidamente. Además, mientras que el robo de un secreto comercial puede violar leyes criminales, no existen leyes criminales relacionadas a la infracción de patentes (United States Department of Justice, 2006). Lo que sigue es un enfoque para la protección de invenciones:

- Seguir las directrices del secreto comercial para todos los procesos o productos recientemente descubiertos hasta que la patente haya sido emitida.
- Asegurarse que la protección de la patente es adquirida en todas las jurisdicciones correspondientes.
- Considerar el uso de la U.S. International Trade Commission como un lugar para resolver las controversias sobre patentes.

1.5.4 SECRETOS COMERCIALES

Los secretos comerciales no necesitan ser registrados en ninguna agencia externa, así el propietario puede mantener un mayor grado de control sobre el activo. Para que la información sea considerada un secreto comercial, el propietario debe ser capaz de probar que la información añadió un valor o beneficio al propietario, el secreto comercial fue específicamente identificado y el propietario proporcionó un nivel razonable de protección al secreto comercial. El término “razonable” implica un alto estándar; el propietario debe demostrar un programa de seguridad robusto y medidas de protección estrictas que estén clara y consistentemente definidas, comunicadas y que se hagan cumplir.

Los siguientes pasos deben ayudar a la organización a proteger sus secretos comerciales:

- Documentar la identificación y valoración de los secretos comerciales, su rol en el establecimiento de una ventaja competitiva en la industria y el alcance total de las medidas de protección instituidas para protegerlos.

- Asegurar que existen medidas de seguridad, tradicionales y cibernéticas, razonables para evitar el acceso no autorizado a los secretos comerciales.
- Realizar auditorias de seguridad aleatorias y periódicas, para asegurar su cumplimiento
- Llevar a cabo acuerdos de no divulgación con los empleados, proveedores, consultores, y otras personas antes de cualquier divulgación.
- Establecer los criterios de necesidad-de-conocimiento para garantizar que las personas tengan acceso sólo a la información específica que necesitan para hacer sus trabajos.
- Instituir notificaciones de información de advertencia eficaces para garantizar que las personas están conscientes de lo que exactamente necesita ser protegido.
- Adoptar medidas apropiadas para la destrucción de materiales que ya no se necesiten.

1.5.5 PREOCUPACIONES INTERNACIONALES

Una compañía que planea introducir propiedad intelectual en otro país debe trabajar con los abogados con mucha antelación, y esos abogados deben tener experiencia en el mercado previsto. La compañía también debe inventariar su propiedad intelectual y otra información sensible y desarrollar planes para proteger cada tipo de información.

Además de solicitar las patentes, la asignación de cualquier derecho de autor y licencias de tecnología según corresponda, las compañías deben evaluar los riesgos que representan las relaciones contractuales. Muchas disputas de propiedad intelectual surgen entre compañías que hacen negocios en conjunto. Las compañías deben utilizar los acuerdos de no divulgación en las negociaciones y contratos, identificar y restringir la divulgación de toda información técnica sólo a aquellos que tienen necesidad de saber, y compartimentar el conocimiento. Algunas formas de información, tales como herramientas, matrices o fórmulas, pueden ser protegidas a través de medidas de seguridad física tradicionales.

La compañía también debe realizar una investigación de due diligence de propiedad intelectual, revisando el mercado del país bajo consideración por infracciones de los derechos de la compañía y analizar las experiencias de compañías similares en ese país. Más aún, la compañía debe familiarizarse con las normas y reglamentos de propiedad intelectual del país. Los titulares de licencias deben consultar abogados cualificados para determinar qué proporción de una licencia debe ser registrada para garantizar que los derechos de los titulares no se vean afectados.

Una excelente fuente de consejos para hacer negocios en el extranjero es el U.S. State Department's Overseas Security Advisory Council (OSAC). Su sitio Web (www.osac.gov) proporciona una variedad de documentos útiles, incluyendo las Security Guidelines for American Enterprises Abroad. OSAC también ofrece consejos sobre normas y leyes de propiedad intelectual de un país específico, así como información de las tendencias en infracciones.

1.5.6 ACUERDOS DE NO DIVULGACIÓN Y CONTRATOS

Los acuerdos escritos de no divulgación (NDA) garantizan un comprensión común y una obligación legal respecto a la protección de los activos de información. Los NDA deben reconocer que cualquier información sobre cualquier medio que registre comunicaciones comerciales o transacciones es considerado un registro oficial ante las leyes y será manejado de acuerdo a las políticas y procedimientos relacionados con los activos de información. Las obligaciones de confidencialidad pueden necesitar ser extendidas a los miembros del consejo, empleados, agentes u otras personas.

Todos los empleados deben firmar una NDA como una condición de empleo. Mediante el acuerdo, ellos deben reconocer que todos los activos de información relacionados con el empleador, proveedores y clientes son considerados confidenciales. El NDA de los empleados también debe incluir la verificación de que el empleado ha leído, entendido y se atendrá a las políticas y procedimientos de IAP. Cuando su empleo termine, a los empleados se les debe recordar que su obligación bajo el NDA continúa.

Del mismo modo, un contratista, subcontratista, consultor o proveedor con acceso a los activos de información deben estar contractualmente obligados a proteger la información en la misma medida en que se encuentra protegida en la empresa.

En el Anexo C se proporcionan ejemplos de NDA.

1.6 MEDIDAS TÉCNICAS DE PROTECCIÓN

Esta sección aborda los medios de mitigación de las amenazas de recolección técnica. La incorporación de medidas tradicionales de protección con estos métodos técnicos representa una aplicación de convergencia en la protección de activos. Muchos de estos métodos descritos aquí requieren conocimientos especializados, y puede ser necesario externalizar algunos servicios. Es esencial seleccionar cuidadosamente los socios para externalización, ya que ellos necesariamente obtendrán acceso a información sensible.

1.6.1 CONTRAMEDIDAS DE VIGILANCIA TÉCNICA

Las contramedidas de vigilancia técnica (TSCM de ahora en adelante, por sus siglas en inglés) son servicios, equipos y técnicas diseñadas para localizar, identificar y neutralizar actividades de vigilancia técnica (escuchas clandestinas). Las TSCM deben ser parte de la estrategia global de protección de la organización.

Como parte de los esfuerzos de TSCM, los profesionales de IAP deben disponer inspecciones periódicas de los equipos de telecomunicaciones, cables y terminales con equipos, métodos y personal capaz de detectar las amenazas actuales. Las oficinas y salas de reuniones deben ser inspeccionadas regular y aleatoriamente para detectar vulnerabilidades de vigilancia técnica y también inmediatamente antes de

cualquier conversación sensible.

1.6.2 PROTECCIÓN EN UN ENTORNO DE TI

Esta sección presenta los aspectos más destacados de los problemas de seguridad de TI relacionados con los programas de IAP. La seguridad de TI está cubierta en mayor detalle en otras secciones de *Protección de Activos*.

Debido a que existe mucha información en forma electrónica, los profesionales de IAP deben considerar la protección de redes (alámbricas e inalámbricas) y también de las computadoras independientes. Lo más eficaz es un enfoque estratificado que integre las medidas de protección físicas, de procedimientos y lógicas. Los siguientes son algunos pasos recomendados:

- Cambiar las contraseñas por defecto, nombres de usuarios y cuentas administrativas.
- Asignar adecuadamente los privilegios administrativos. Los administradores deben usar cuentas sin privilegios cuando no están realizando la administración del sistema.
- Limitar y monitorear los accesos físicos a los componentes de la red.
- Asegurar una separación de responsabilidades para el personal de TI cuando sea posible.
- Instalar y actualizar el software de antivirus y cortafuegos en los servidores de la red y los dispositivos de clientes (computadoras portátiles, estaciones de trabajo y dispositivos electrónicos personales). Los cortafuegos pueden proteger la información de intrusiones externas e internas.
- Implementar protocolos formales de gestión de parches y gestión de configuración.
- Capacitar a los usuarios en la conciencia de seguridad informática, incluyendo los riesgos asociado a accesos remotos, accesos móviles y tecnología inalámbrica.
- Exigir a las organizaciones externas con acceso a los sistemas de información de la compañía que mantengan una postura de seguridad equivalente.

Un sistema de detección de intrusión (IDS de ahora en adelante, por sus siglas en inglés) supervisa programas maliciosos y cambios no autorizados de archivos y configuraciones. También supervisan el tráfico de la red y proporcionan alarmas para los ataques a la red. Para algunos entornos, se debe considerar un sistema de prevención de intrusión, especialmente donde el personal podría no estar disponible para monitorear activamente o actuar en las alertas del IDS. Adicionalmente, se pueden configurar sistemas de prevención de extrusión para prevenir la salida de información no autorizada.

Especial atención se debe dar a la protección de datos y al control de acceso en entornos informáticos en la nube y/o cuando terceros tengan algún acceso legítimo a los recursos informáticos o contenido de la información. Esto también aplica cuando una organización emplea un respaldo en línea, una almacenamiento de datos o proveedor de administración de archivos.

Los profesionales de IAP también deben estar conscientes de lo siguiente:

- **Control de acceso lógico a la red**. Este es el proceso por el cual los usuarios son identificados y se les otorga privilegios para la información, sistemas, o recursos.
- **Seguridad de las aplicaciones**. Las aplicaciones comerciales modernas generalmente consisten de un código personalizado, software de terceros y uno o más servidores. La integración inadecuada de estos componentes puede resultar en una vulnerabilidad que posteriormente puede ser explotada para obtener acceso no autorizado a los datos.
- **Desinfección de los sistemas de información y medios de comunicación**. La desinfección es el proceso de eliminación de datos de un medio de almacenamiento (como un disco duro) antes de que el medio sea reutilizado. Los métodos incluyen sobrescribir y desmagnetización (borrado magnético). Una alternativa es la destrucción física.
- **Encriptación.** La encriptación obscurece el significado de la información alterándola o codificándola de tal manera que sólo pueda ser decodificada por las personas a quienes va destinada
- **Firma digital.** Esta autentifica la identidad del remitente de un mensaje. Las firmas digitales son especialmente importantes para el comercio electrónico y los correos electrónicos.
- **Entorno inalámbrico.** Las redes de área local inalámbricas (WLAN de ahora en adelante, por sus siglas en inglés) son convenientes pero pueden introducir riesgos. Ellas por lo general son consideradas menos seguras que las redes alámbricas (LAN), de modo que los tipos de datos transportados por ellas deben ser cuidadosamente evaluados.

1.6.3 PROTECCIÓN EN ENTORNOS ESPECIALES

Varios entornos plantean requerimientos especiales para la protección de los activos de información.

Teléfonos Móviles, Computadoras Portátiles y Asistentes Digitales Personales (PDA)

Los dispositivos móviles o portátiles por lo general no están protegidos por la infraestructura de seguridad de TI de la empresa o de la seguridad física de una instalación cerrada. Las personas a menudo no reconocen la cantidad e importancia de los datos almacenados y comunicados en ese tipo de dispositivos. Los siguientes pasos pueden mejorar la seguridad de los dispositivos portátiles:

- Exigir a los empleados que reconozcan, por escrito, que los equipos emitidos por la empresa y toda información producida o almacenada en ellos es de propiedad del empleador.
- Controlar y desincentivar el uso de dispositivos móviles con cámaras incrustadas, particularmente alrededor de materiales sensibles o en áreas restringidas.
- No almacenar números de seguridad social, números de tarjetas de crédito o contraseñas en dispositivos inalámbricos.
- Bloquear los teléfonos móviles cuando no están en uso.
- Considerar la instalación de un software que pueda bloquear remotamente un teléfono o borrar sus

datos si el teléfono se pierde o es robado.

- Etiquetar o grabar las computadoras portátiles con el nombre, dirección, y teléfono de la organización para aumentar las probabilidades de recuperar los objetos perdidos.
- Evitar que se visualice el nombre del último usuario que inició sesión.
- Utilizar un maletín difícil de describir.
- Tenga cuidado cuando utilice un punto de servidor inalámbrico (como en un hotel o aeropuerto). Existe un riesgo de que se inicie sesión en una computadora cercana que puede ser utilizada para el robo de identidad.
- Configurar la computadora para que no se conecte automáticamente a puntos de acceso inalámbricos listados como poco seguros.
- Chequear regularmente con el fabricante del dispositivo para ver las actualizaciones de software o noticias de vulnerabilidades de seguridad.

Conferencias Electrónicas

Las reuniones vía video, teléfono y tecnologías basadas en la Web son convenientes, pero no necesariamente seguras. El profesional de IAP debe averiguar cómo protege la información el proveedor del servicio. También es importante averiguar las políticas del proveedor respecto a las contraseñas. Cuando sea posible, se debe utilizar la encriptación para la transferencia de datos.

A menos que las medidas de seguridad puedan ser validadas, los usuarios deben asumir que sus conversaciones no son privadas.

Externalización

La externalización transfiere el control operacional y la responsabilidad a terceros y puede aumentar el riesgo de los activos de información. En ciertos casos, los riesgos de la información no son fácilmente identificables y pueden ser el resultado de cláusulas sutiles u ocultas en los contratos. Debe realizarse una due diligence para los potenciales proveedores. Los siguientes son algunos pasos sugeridos:

- Revisar el desempeño financiero y la reputación, incluyendo las violaciones a los derechos de propiedad intelectual, denuncias comerciales, asuntos de control de exportaciones, vínculos con gobiernos extranjeros y vínculos con empresas sospechosas.
- Establecer acuerdos, individuales y corporativos, de no divulgación con los proveedores y sus subcontratistas
- Llevar a cabo revisiones de la seguridad en el sitio del proveedor antes de firmar un acuerdo de externalización y posteriormente en forma periódica.
- Identificar, física y lógicamente, dónde trabajará el personal subcontratado y asegurarse de que existen medidas apropiadas de seguridad física y de tecnología de información en el sitio
- Consultar un asesor legal sobre las leyes y reglamentos (de todos los países participantes) sobre

exportaciones e importaciones de tecnología, personal e información privada, e implementar procedimientos de protección para ayudar a asegurar el cumplimiento

1.7 RESPUESTA Y RECUPERACIÓN DESPUÉS DE UNA PÉRDIDA DE INFORMACIÓN

Los siguientes son pasos clave a tomar después de una pérdida de información:

Investigación

- Investigar exhaustivamente la información comprometida ya conocida y la que se sospecha para apoyar a los encargados de hacer cumplir la ley, las causas judiciales, recuperación de activos, identificación de la causa raíz del incidente, prevención de futuros incidentes y evaluación de las pérdidas o daños.
- Establecer un plan de investigación y coordinar con el asesor.
- Identificar los recursos de investigación que se requieren de las fuentes internas o externas.
- Establecer y mantener enlaces con los organismos encargados de hacer cumplir la ley y los proveedores de servicios de investigación así como con diversas fuentes de información.

Evaluación del Daño

- Tan pronto y lo más completamente posible, determinar cuál es la información que ha sido comprometida.
- Determinar las implicancias del compromiso en términos de pérdidas económicas, demora en los proyectos, impacto operacional, imagen corporativa, confianza de los accionistas, responsabilidad legal y relaciones corporativas (con socios, proveedores, vendedores, subcontratistas, etc.).
- Informar el impacto real y potencial al nivel de gerencia correspondiente.

Recuperación y Seguimiento

- Darse cuenta que los dos elementos primordiales de la recuperación son (1) volver el negocio a las operaciones normales tan pronto como sea posible y (2) implementar medidas para evitar una recurrencia del problema.
- Implementar cualquier parte aplicable del plan de continuidad de negocios de la organización.
- Realizar un análisis de la causa raíz e implementar acciones correctivas basadas en sus conclusiones. Mantener una base de datos de incidentes (incluyendo denuncias y presuntos incidentes) para apoyar el análisis de la causa raíz y analizar cualquier tendencia.

1.8 RESUMEN

En la protección de los activos de información, una estrategia de protección eficaz comienza con una política clara y práctica que es compartida con todas las partes interesadas y aplicada imparcialmente. La adecuada combinación de medidas de protección varía en cada organización. Generalmente, una organización necesitará emplear tanto las medidas de seguridad (personal, equipos, entrenamiento de conciencia) como las medidas legales (derechos de autor, patentes, marcas registradas, acuerdos de no divulgación, cláusulas de contratos) para proteger sus activos de información.

Un programa de IAP debe esforzarse para evitar la pérdida de información, pero también debe estar preparado para responder a las pérdidas que se producen, y recuperarse de un evento de pérdida que involucre los activos de información. Finalmente, para una gestión de riesgos penetrante, el programa de IAP debe ser desarrollado en paralelo con las principales operaciones del negocio y la planificación de continuidad de negocios para garantizar estrategias de protección consistentes y bien orquestadas.

ANEXO A

EJEMPLO DE POLÍTICA DE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

El siguiente ejemplo de política protección de activos de información puede ser adaptado a cualquier organización y difundido en papel y en la intranet de la empresa. Ha sido adaptado de la política de ASIS International *Information Asset Protection Guideline* (2007).

A. RESUMEN DE LA POLÍTICA

Estamos comprometidos a proteger los activos de la organización, incluyendo empleados, información y entorno laboral, que nos permiten lograr nuestras metas de negocios. Por lo tanto, hemos establecidos esta política de protección de activos de información (IAP). Establece los principios rectores respecto de la protección de los activos de información de la organización.

La información es un activo organizacional clave y será protegido de acuerdo a su valor y basado en los resultados de las evaluaciones de riesgos periódicas. La estrategia de protección se basa en los siguientes principios:

- La protección de los activos de información consistirá en la identificación, valoración, clasificación y etiquetaje en un esfuerzo para protegerlos contra el acceso no autorizado, uso, divulgación, modificación, destrucción o negación.
- Los controles representarán medidas rentables en función de los riesgos coherentes con otras políticas y objetivos estratégicos de la organización.
- La estrategia IAP integra la seguridad tradicional, la seguridad de la tecnología de la información y las funciones legales y administrativas.
- La responsabilidad y obligación se extiende a todos los empleados, así como a los consultores, contratistas, subcontratistas, empleados de tiempo parcial, empleados temporales, pasantes, equipos asociados y socios.
- Cumpliremos todos los requerimientos legales y reglamentarios aplicables.

B. GERENTE DEL PROGRAMA IAP

Todas las preguntas, problemas y preocupaciones relacionadas con esta política serán dirigidas al gerente del programa IAP *(proporcionar la información de contacto)*.

C. APLICABILIDAD

La política IAP aplica a todos los empleados y a toda la empresa, es decir, individuos y entidades con acceso a los activos de información de la organización, personas e instalaciones.

D. ACTIVOS DE INFORMACIÓN

Nuestros activos de información se encuadran en una variedad de categorías, algunas de las cuales

están sujetas a leyes y reglamentos específicos. En esos casos, cumpliremos con todas las leyes y reglamentos aplicables. Esto puede llegar a ser complicado en algunas circunstancias cuando puedan aplicar todas las leyes y reglamentos locales, estatales, federales e internacionales. Contactar al asesor legal de la organización o al gerente del programa IAP para recibir orientación en casos específicos.

Las principales categorías de los activos de información incluyen la información privada, información patentada, secretos comerciales, patentes, derechos de autor, marcas comerciales, datos financieros e información regulada. Cada categoría garantiza ciertas protecciones según la política de IAP.

E. CLASIFICACIÓN E INTERCAMBIO DE INFORMACIÓN

Es esencial compartir información tanto interna como externamente para logar los objetivos del negocio. Sin embargo, también es nuestra responsabilidad asegurar que los activos de información sensible estén protegidos de pérdidas o compromiso. Todos los empleados y miembros de nuestra empresa son responsables por compartir la información adecuadamente y protegerla de divulgaciones inapropiadas, modificaciones, uso indebido o pérdidas.

Para proteger la información (papel, electrónica, oral, etc.) según su valor para el negocio, hemos desarrollado políticas, prácticas y procedimientos como parte de nuestro programa de IAP. Está incluido un mecanismo para clasificar nuestros activos de información en cuatro categorías: altamente restringida, restringida, uso interno y sin restricciones:

- *Altamente restringida*: es usada para la información patentada que podría permitir a los competidores tomar acciones que podrían dañar seriamente nuestra posición competitiva o que, si se divulga, podría dañar significativamente las finanzas de la organización o la posición competitiva. Se usan precauciones estrictas para eliminar la divulgación accidental o deliberada y para detectar los intentos de acceso no autorizado. El acceso para los empleados está limitado a las personas específicamente autorizadas. El acceso para los que no son empleados está limitado a las personas que están autorizadas y cubiertas por un acuerdo de no divulgación (NDA).
- *Restringida*: se utiliza para la información que es organizacionalmente o competitivamente sensible o que podría presentar riesgos legales o de la privacidad de los empleados. Las precauciones se toman para reducir la divulgación accidental o deliberada. El acceso para los empleados se basa en el rol de cada individuo. El acceso para los que no son empleados está limitado a las personas que están aprobadas y cubiertas por un NDA.
- *Uso interno*: es utilizada para la información generada dentro de la organización que no está diseñada para su distribución pública. Se usan las precauciones de sentido común para proteger razonablemente esta información. El acceso generalmente está limitado a los empleados. El acceso para los que no son empleados está limitado a las personas que están aprobadas y cubiertas por un NDA.
- *Sin restricciones*: es usada para la información que puede ser compartido dentro y fuera de la

organización.

Todo el mundo está obligado tomar estas medidas:

- Seguir todos los procedimientos y prácticas respecto a la protección de los activos de información.
- Participar en la gestión de incidentes, evaluaciones de riesgos, procesos de trabajo y mecanismos de control para apoyar la política.
- Garantizar que existen controles de acceso adecuados para toda la información que se ha creado o propia.
- Usar el sentido común y la previsión en la divulgación de información relacionada con la organización.

A los empleados en determinados roles se les ha dado responsabilidades específicas para el despliegue, implementación y mantenimiento de la política de IAP. Estos roles y responsabilidades son los siguientes:

- El *gerente del programa IAP* es responsable de la política en general, incluyendo:
  - la determinación de los niveles y la protección que requiere en cada nivel
  - proporcionar la línea de base de la seguridad de la información mediante la infraestructura tecnológica de la organización
  - proporcionar informes de la gestión del iap según corresponda
  - coordinar el programa con los otros miembros de la organización
- *Otros gerentes y directores* son responsables de la comprensión y cumplimiento de los empleados de la política de IAP así como las prácticas y procedimientos organizacionales. Estos gerentes y directores pueden ser responsables de:
  - capacitación de los empleados sobre todos los niveles de clasificación
  - garantizar que los procesos de trabajo y controles apoyen la política
  - garantizar que las evaluaciones de riesgos son realizadas en la medida que se necesitan y que los incidentes son gestionados dentro del marco de la política de IAP

F. PRIVACIDAD DE LOS EMPLEADOS

La información de los empleados es un recurso que debe ser protegido contra la alteración, pérdida o divulgación no autorizada. Protegemos la información que es esencial para el funcionamiento del negocio y protegemos esta información de su divulgación a cualquier persona que no tenga una necesidad comercial legítimamente o el derecho legal de tenerla.

Se debe garantizar la privacidad y confidencialidad de los registros del personal. Cualquier información personal recopilada por la organización, será necesaria y relevante y se obtendrá y mantendrá utilizando métodos que respeten el derecho a la privacidad del individuo así como las

leyes y reglamentos aplicables. Además, todo empleado tiene el derecho a saber qué tipo de información personal mantiene la organización acerca de ella o él y cómo es o puede ser usada.

Se pueden realizar auditorías periódicas para garantizar el cumplimiento de la política organizacional, así como las leyes y reglamentos relacionadas con la gestión de la información privada y personal.

G. ASEGURAR NUESTRA PROPIEDAD

Estamos comprometidos a proporcionar seguridad a nuestros activos tangibles e intangibles para evitar pérdidas. Cada uno de nosotros debe hacer lo siguiente:

- Ayudar a asegurar que el acceso a las instalaciones de la organización se limite a las personas autorizadas o las visitas aprobadas.
- Usar y mostrar la identificación adecuada según lo definido por la política organizacional.
- Enfrentar los problemas de seguridad de manera proactiva, buscando desde el inicio la participación del departamento de seguridad en las iniciativas de nuevas marcas, construcción de proyectos y temas relacionados.
- Tener en cuenta y tomar las medidas apropiadas acerca de los potenciales riesgos de seguridad en el trabajo.

Los gerentes de las sucursales de la compañía garantizarán que las instalaciones cumplan los estándares de control de acceso recomendados y cumplan con las otras directrices de seguridad y responderán a los incidentes o preocupaciones de seguridad, asegurándose de informar adecuadamente al departamento de seguridad.

El departamento de seguridad, en conjunto con otros departamentos, tiene la responsabilidad de realizar cualquier actividad investigativa en casos, conocidos o presuntos, de pérdida, compromiso, robo, manipulación, denegación de acceso, fraude o conflicto de intereses respecto de la información. Seguridad también tiene la responsabilidad de hacer partícipe a las autoridades locales según corresponda. Cuando corresponda, se debe contactar especialistas externos a través de proveedores de confianza.

Las medidas específicas para el manejo, marcado, almacenamiento, transmisión, transporte, copia, desclasificación y destrucción de información sensible se encuentran en las prácticas y procedimientos de la organización, disponibles en nuestra intranet.

H. CONCIENCIA Y ENTRENAMIENTO DE SEGURIDAD

Todo empleado y miembro de la empresa es responsable por la protección de los activos de información. Cada persona debe también estar consciente de las razones o necesidades de controles, así como de las prácticas y procedimientos que conforman nuestro programa de IAP. Seguridad, en conjunto con el gerente del programa de IAP, proporcionarán entrenamiento periódico de conciencia de seguridad que incluirá una información actualizada sobre los riesgos de los activos de información y de las medidas defensivas prudentes. La concienciación también será facilitada regularmente a

través de artículos en el boletín de noticias, recordatorios y recursos basados en la Web.

Nuestra intención es mantener la seguridad en el primer plano de la mente de las personas y darle a cada una las herramientas de IAP necesarias, así como un fácil y rápido acceso a las prácticas y procedimientos de la compañía y a respuestas útiles para cualquier pregunta.

I. COMUNICACIÓN PÚBLICA DE LA INFORMACIÓN

Dirigir todas las preguntas de los medios de comunicación al director de relaciones externas para garantizar que la información pública se presenta consistentemente y que las solicitudes de información son monitoreadas.

J. PUBLICACIONES Y PRESENTACIONES

Estimulamos el adecuado intercambio de información a través de presentaciones y publicaciones. Ese intercambio fomenta la innovación, las redes de trabajo, el desarrollo del mercado, las relaciones públicas y la sensibilización de la comunidad.

Cualquier intercambio de información debe seguir las políticas de IAP respecto a las precauciones de seguridad para cada respectivo nivel de clasificación. Contacte a su gerente si usted tiene preguntas relacionadas con la información que va a ser compartida.

El departamento de relaciones externas debe ser informado de todas las presentaciones planificadas y publicaciones para el público externo. Las presentaciones y publicaciones que potencialmente podrían incluir información restringida o altamente restringida deben ser consistentes con la política de IAP de la organización.

K. PLANIFICACIÓN DE LA SEGURIDAD DE VIAJES

Los activos de información son particularmente vulnerables cuando nuestros empleados y asociados viajan. Por lo tanto, debe desarrollarse un entrenamiento de seguridad de viajes enfocada en la IAP. El entrenamiento debe abordar el entorno de seguridad del destino del viaje y revisar las prácticas y procedimientos relevantes de seguridad. Estos pueden incluir solicitud de visitas o notificaciones, procedimientos para presentación de informes, material de empaquetado o reenvío y la preparación de los medios de almacenamiento. Cualquier problema de seguridad, actividad sospechosa u otro problema encontrado durante el viaje, debe ser informado al departamento de seguridad, al gerente del programa de IAP o al propio gerente del viajero.

Las computadoras y dispositivos portátiles son particularmente vulnerables al robo durante los viajes. El uso de dispositivos inalámbricos y redes fuera de las instalaciones de la organización está sujeto a restricciones descritas en las prácticas y procedimientos de la organización. Además, los empleados no deben conversar temas de información sensible en lugares públicos donde las conversaciones puedan ser escuchadas o grabadas o con personas que no tienen necesidad de saber.

L. NUEVOS PROYECTOS E INICIATIVAS

Todas las nuevas investigaciones, desarrollos, línea de productos o iniciativas de marca, deben ser

protegidas usando los principios y estrategias de seguridad detalladas en la política de IAP y en las prácticas y procedimientos de apoyo. Se debe considerar un plan de IAP para cada proyecto que implique información restringida o altamente restringida.

M. RECURSOS DE TI

Las computadoras, periféricos y dispositivos portátiles e inalámbricos pertenecientes u otorgados por la organización siguen siendo propiedad de la organización y están destinados sólo para uso del negocio. Todos esos sistemas y la información contenida en ellos están sujetos a monitoreo o revisión por parte de los ejecutivos o representantes de la organización y no existe expectativa de privacidad en la posesión o uso de esos sistemas.

Los individuos (empleados y miembros de toda la empresa) son responsables del adecuado manejo y protección de todo hardware, firmware, software, datos e información asociada a esos sistemas. Esto incluye asegurar que el software tiene su respectiva licencia y que el equipamiento está razonablemente protegido de robo, falsificación y mal uso.

Además, las personas son responsables de la protección de toda la información que puede residir en esos sistemas, independientemente de su sensibilidad o contenido. La información debe ser protegida correctamente mientras resida en el sistema y mientras está siendo procesada, copiada, transmitida, recibida o intercambiada.

Aunque en algunos casos se puede tolerar una cantidad limitada y razonable de uso no relacionado con el negocio (por ejemplo, la recepción de una llamada telefónica personal en un teléfono móvil de la compañía), ese uso debe ser mínimo y se aplicarán las medidas de seguridad adecuadas. Bajo ninguna circunstancia se accederá, descargará, almacenará, transmitirá o procesará materias inapropiadas (por ejemplo, pornografía, actividades ilegales, material difamatorio, amenazas, etc.) en sistemas pertenecientes o emitidos por la empresa.

N. PRESENCIA EN LA WEB

Las personas deben asegurarse de que cualquier información que ellos publiquen en línea siga la política de procedimientos del IAP para el uso de información altamente restringida, restringida e interna.

O. RELACIONES DE CONFIANZA (TODA LA EMPRESA)

Las obligaciones específicas, prácticas y procedimientos para la IAP serán documentados en acuerdos escritos antes de la ejecución de cualquier contrato, compromiso de consultoría u otra relación comercial que pueda implicar el intercambio de o acceso a información sensible. Los acuerdos pueden incluir un NDA, cláusulas contractuales, memorandos de comprensión u otros formatos. El acuerdo debe especificar el tipo de información a la que aplica, la identificación de las partes involucradas, el propósito del acuerdo y el período de tiempo por el cual seguirá siendo válido. En todos esos acuerdos se hará una referencia específica a la política de IAP y otras políticas, prácticas y procedimientos organizacionales relevantes.

Los individuos y entidades en una relación de confianza con nuestra organización deben ser advertidos de que sus obligaciones para proteger cierta información puede extenderse más allá del período de su relación con nosotros o del fin de un proyecto en particular. Además de nuestro acuerdo escrito, también aplicarán las leyes y reglamentos locales, estatales, federales o internacionales a la protección de la información y materias de no divulgación.

P. INFORMAR CUALQUIER ACTIVIDAD SOSPECHOSA O PRESUNTAS PÉRDIDAS O COMPROMISOS

Las personas deben notificar al gerente del programa de IAP o al departamento de seguridad acerca de (1) cualquier acercamiento inapropiado (en persona o electrónico) de individuos solicitando información sensible, (2) cualquier otra actividad sospechosa y (3) cualquier presunta pérdida o compromiso de información sensible. Estos asuntos pueden ser informados de la siguiente manera *[información de lista de contactos]*

Esta organización se rige por los derechos de autor, marca registrada, secreto comercial y derecho de patente.

Los empleados que violen esta política –ya sea en forma intencional o por negligencia- pueden estar sujetos a acciones disciplinarias, incluyendo el posible despido. Además, los empleados, individuos y entidades cubiertos bajo esta política pueden estar sujetos a acciones administrativas, procesos criminales o acciones civiles por violaciones.

ANEXO B

GUIA DE REFERENCIA RÁPIDA PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

Esta guía esta diseñada para ayudar a todos los empleados o asociados de confianza de una organización a determinar la apropiada clasificación del material y los procedimientos relevantes para el manejo de la información sensible. Se ha adaptado de la ASIS International *Information Asset Protection Guideline*, mayo 2007.

PASO 1 Este documento es una guía de referencia rápida para los propietarios y usuarios de activos de información. Para información más detallada sobre materias específicas, por favor ver la política, prácticas y manual de procedimientos disponible en_____.

A continuación se encuentran las cuatro categorías usadas para clasificar la información y una breve explicación de los procedimientos a seguir para cada clasificación. Toda la información debe ser clasificada bajo una de las siguientes cuatro categorías: Sin restricción, Uso Interno, Restringida o Altamente Restringida. Sólo se requiere que la información bajo las categorías de Uso Interno, Restringida y Altamente Restringida sea marcada. Para compartir o difundir esta información siga los procedimientos indicados a continuación para cada categoría. Si la información aún no ha sido clasificada, proceda al paso 2.

SIN RESTRICCIÓN	USO INTERNO	RESTRINGIDA	ALTAMENTE RESTRINGIDA
Esta información se puede compartir dentro y fuera de la organización	1. No tiene restricción de acceso de lectura dentro de la empresa. El control de las versiones y actualizaciones son administradas por el dueño del contenido. 2. Compartir externamente sin un acuerdo de no divulgación (NDA) requiere una clara comprensión entre las partes de que la información debe ser tratada como confidencial. 3. Esta información no es para ser compartida con el público.	1. Los dueños del contenido administran las listas de acceso y autorizan que sea compartida. 2. El acceso está limitado a ciertas organizaciones, grupos o personas en ciertos roles (i.e., legal, ingeniería, marketing, etc.) 3. La extensión y tipo de acceso a la información (v.gr. crear, sólo lectura, actualizar o borrar) está limitado y se basa en el rol y los requisitos de control de fraude 4. Un NDA firmado y una política establecida de "necesidad de saber" se requiere para compartir esta información con la empresa ampliada *	1. Los dueños del contenido administran las listas de acceso para los tipos de acceso e intercambio autorizado. 2. El acceso está restringido a personas específicamente nombradas con una "necesidad de saber" establecida. 3. Autorizar un funcionario exige la verificación del estado del empleado y una clara comprensión de su uso. 4. Al autorizar el intercambio de información con una persona de la Empresa Ampliada, verificar que exista un NDA firmado y un acuerdo contractual adecuado. 5. Revisión trimestral de acceso continuado

* "Empresa Ampliada" consiste de individuos y entidades con acceso a los activos de información, personas e instalaciones.

PASO 2 ¿Usted creó o de alguna forma es dueño de la información?

NO, pero me gustaría compartirla. Comparta la información siguiendo la guía proporcionada en la tabla del PASO 1. Si usted tiene una fuerte sensación de que información no marcada debería estar marcada, porque tiene un valor para los competidores o puede tener un valor para el propietario, contacte al dueño de la información para compartir su preocupación. Es responsabilidad del dueño o creador de la información marcarla inicialmente y actualizar las clasificaciones de la información.

SÍ, necesito determinar la clasificación y tener la autoridad para clasificar mi información. Yo determinaré la clasificación de la información utilizando las siguientes preguntas. La columna con la mayoría de las selecciones sugiere la clasificación de protección. Advertencias: (1) use un buen juicio de negocios cuando comparta cualquier información comercial; y (2) comparta los documentos sólo en forma de lectura.

	SIN RESTRICCIÓN	USO INTERNO	RESTRINGIDA	ALTAMENTE RESTRINGIDA
1. ¿Qué ventaja competitiva provee la información?	Ninguna	Posible ventaja	Ventaja definitiva	Ventaja significativa
2. ¿Probabilidad de que el competidor busque esta información?	Ninguna	Alguna	Existe la probabilidad	Alta probabilidad
4. Si esta información fuera divulgada, perdida o cambiada:				
• ¿Posible daño a las operaciones de la organización?	Ninguno	Algún daño	Daño moderado	Daño severo
• ¿Posible daño para una persona?	Ninguno	Algún daño	Daño moderado	Daño severo
• ¿Posible daño para la reputación o imagen de la organización?	Ninguno	Algún daño	Daño moderado	Daño severo
• ¿Pérdida de la confianza de clientes, accionistas o socios	Ninguno	Alguna oportunidad	Buena oportunidad	Oportunidad definitiva
• ¿Pérdida del secreto comercial o protección de la patente?	Ninguno	Alguna oportunidad	Buena oportunidad	Oportunidad definitiva
• ¿Pérdida de la capacidad para ser primero en el mercado?	Ninguno	Alguna oportunidad	Buena oportunidad	Oportunidad definitiva
• ¿Pérdida de la participación de mercado?	Ninguno	Alguna oportunidad	Buena oportunidad	Oportunidad definitiva
• ¿Efecto sobre el valor de la acción o del capital de riesgo de la compañía?	Ninguno	Poco efecto	Moderado efecto y a corto plazo	Severo efecto y a largo plazo

Ejemplos:

SIN RESTRICCIÓN	USO INTERNO	RESTRINGIDA	ALTAMENTE RESTRINGIDA
• Información fáctica contenida en la publicidad de la organización y en su sitio Web	• Organigrama de la organización • Directorio de Empleados • Mapas de las instalaciones	• Datos previo a la patente • Datos de seguridad • Informes de iniciativa de productos • Datos de clientes • Consumidores • Información del personal • Planes de Abastecimiento	• Fórmulas de desarrollo • Datos de Patente • Datos financieros consolidados • Acciones bursátiles • Información global del sistema financiero • Estrategia para la marca emblemática

Si la información no cumple los criterios mínimos para “Uso Interno” indicados anteriormente, podría ser considerada información pública, a menos que se encuadre bajo una categoría especial como datos restringidos por finanzas, salud o regulaciones de privacidad. Compruebe con su gerente del programa de IAP.

REQUISITOS DE PROTECCIÓN PARA COMPARTIR INFORMACIÓN DE DISTINTAS CLASIFICACIONES

A continuación se muestran algunos ejemplos y sugerencias de procedimientos a seguir para marcar y difundir documentos. Nota: las leyes o reglamentos internacionales, federales, estatales o locales pueden sustituir los requisitos de protección. Para todos los sistemas electrónicos, los empleados deben usar software, medios y herramientas de propiedad de la organización o aprobados por ella.

	USO INTERNO	RESTRINGIDA	ALTAMENTE RESTRINGIDA
Marcado de Documentos (Papel y Electrónico)	Sólo artículos con amplia circulación corporativa se marcan como "Uso interno" y estos se comparten en forma no editable.	Marcar "Restringida" en la primera página o marcar en la entrada a la Aplicación/sitio Web.	Marcar "Altamente Restringida" en cada página y cada pantalla en que se muestra o se proporcione acceso a datos altamente restringidos.
Correo/Envíos dentro de la compañía	Sobre de envío, sin marcas especiales.	Dos sobres sellados. En el sobre interior marcar "Restringida: para ser abierto sólo por el destinatario". Sin marcas de seguridad en el exterior del sobre.	Dos sobres sellados. En el sobre interior marcar "Altamente Restringido: para ser abierto sólo por el destinatario". Sin marcas de seguridad en el exterior del sobre.
Facsímil (FAX) dentro de la compañía	Sin requisitos especiales.	Confirmar número de fax y preguntar si la máquina está asegurada físicamente. Pedir al destinatario que esté presente mientras se recibe el fax.	Evitar el envío al extranjero, si es posible. Si se envía, neutralice o sanitise el contenido en un grado práctico.
Facsímil (FAX) sobre líneas externas	Notificar al destinatario y confirmar el número de fax.	Pedir al destinatario que esté presente mientras se recibe el fax.	Enviar por fax sólo si otros métodos de transferencia más seguros no están disponibles. 1.Neutralizar/ desinfectar los contenidos en un grado práctico. 2.Pedir al destinatario que esté presente durante la recepción 3.No llamar la atención sobre su sensibilidad marcando la portada.
E-mail/ Transferencia Electrónica dentro de la compañía (Intranet, vínculos encriptados,	Sin requisitos especiales.	Se recomienda la encriptación, pero no es requisito para las comunicaciones electrónicas internas.	1.Encriptar mensajes de e-mail o archivos, si es posible. 2.Usar tecnología de encriptación, si es posible. 3.Validar la necesidad

líneas dedicadas)			para el negocio y la identidad del receptor.
E-mail/ Transferencia Electrónica a través de redes externas (Internet)	1. Dirección a personas específicas. 2. No publicar en tableros de anuncios o enviar a foros públicos.	1. Usar tecnología de encriptación, si es posible. 2. Validar la necesidad para el negocio y la identidad del receptor.	
Almacenamiento dentro de la compañía	Usar protector de pantalla con una contraseña activada con tiempo de espera de menos de 15 minutos.	1. Encriptar los documentos electrónicos y el control de acceso. 2. Mantener el control del personal o usar almacenamiento bloqueado.	
Almacenamiento fuera de las instalaciones de la compañía	1. Mantenga la información bajo su control. 2. Usar protector de pantalla con contraseña activada con tiempo de espera menos de 15 minutos.		
Destrucción/ Eliminación	1. Cuando proceda, adherir a los límites de retención de la organización. 2. Hacer trizas la copia impresa o utilizar contenedores de reciclaje bloqueados. 3. Borrar la información electrónica. 4. Destruir los medios extraíbles (por ejemplo, disquetes, CD, cinta de cartuchos, discos comprimidos, etc.) antes de eliminarlos.		

ANEXO C

Este anexo contiene dos ejemplos de acuerdos de no divulgación. El primero protege los activos de información de sólo una parte, mientras que el segundo proporciona protección mutua. Para obtener mayor información, ver Daniel B. Hassett, "¿Is Your Model Non-Disclosure Agreement Adequate? Wireless Watch, Abril 2003, disponible en www.wileyrein.com/publication_newsletters.cfm?id=12&publication_ ID=10040.

MUESTRA 1: ACUERDO DE NO DIVULGACIÓN DE INFORMACIÓN QUE RIGE A UNA PARTE

(Fuente: Word Intellectual Property Association, septiembre 2003, disponible en http://www.wipo.int/expZort/sites/www/sme/en/documents /doc/model_nda.doc).

ESTE ACUERDO está fechado el_____, 20[ ] y elaborado

ENTRE

[1] [Nombre y dirección] ……..……..("Propietario") y

[2] [Nombre y dirección ……..……..…..("Destinatario")

CONSIDERANDO

(A) Que el propietario posee cierta información patentada que está dispuesto a revelar al destinatario en los términos que se establecen a continuación

(B) El destinatario está dispuesto a aceptar la información patentada en esos términos y usarla sólo para el propósito de……("el Propósito Permitido").

AHORA SE ACUERDA SEGÚN COMO SIGUE

1. "Información Confidencial" quiere decir cualquiera y toda la información, ya sea comercial o técnica, relacionada con el negocio del Propietario, incluyendo sin limitación, conocimientos, datos, procesos, diseños, fotografías, dibujos, especificaciones, programas de software y muestras, que están marcadas con un indicador como "Confidencial" o "Patentada", pero excluyendo la información que:

   1.1 es o entra en el dominio público, que no sea por divulgación o incumplimiento por parte del destinatario;

   1.2 era o es legalmente obtenida o disponible desde un tercer que estaba legalmente en posesión de la misma y libre de divulgarla; o

   1.3 ya era conocida por el destinatario como lo demuestra la constancia escrita antes de dicha divulgación.

2. Teniendo en cuenta que el Propietario revela información patentada, el Destinatario se compromete por un período de [cinco] años a partir de la fecha del presente Acuerdo

   2.1 a mantener el carácter confidencial de toda la información patentada que pueda adquirir de cualquier forma;

   2.2 a usar la información patentada exclusivamente para el Propósito Permitido y no usar la información patentada para propósitos o beneficio propio del Destinatario

   2.3 no divulgar esa Información Patentada a nadie, excepto a los empleados autorizados u otros agentes del Destinatario que necesiten tener acceso a la Información Patentada con el fin de realizar sus obligaciones en relación con el Propósito Permitido;

   2.4 a informar a todas las personas a las que se revela la Información Patentada que es confidencial y a obtener su compromiso para mantenerla confidencial en los mismos términos de este Acuerdo

   2.5 a mantener la seguridad de todos los dibujos, documentos, muestras o materiales proporcionados en préstamo por el Propietario, a no reproducir, desprenderse, modificar o interferir con esos elementos, a devolverlos inmediatamente en el momento que lo solicite el Propietario y espontáneamente en cualquier caso cuando ya no se necesiten para los propósitos del presente Acuerdo;

   2.6 a notificar al Propietario inmediatamente después de haber tenido conocimiento de cualquier violación a la confianza por alguien a quien el Destinatario haya revelado la Información, y a dar todo el apoyo necesario en relación a cualquier medida que el Propietario pueda desear tomar para prevenir, detener u obtener una indemnización por ese incumplimiento o amenaza de incumplimiento

3. Nada de lo dispuesto en este Acuerdo se considerará que concede al Destinatario una licencia expresa o por implicación bajo ninguna patente, derecho de autor u otro derecho de propiedad intelectual. Por el presente el destinatario reconoce y confirma que todos derechos de propiedad intelectual actuales y futuros que se relacionen con la Información Patentada son de exclusiva propiedad del Propietario. El Destinatario no solicitará u obtendrá ninguna protección de propiedad intelectual respecto a la Información Patentada. Todos los derechos de propiedad intelectual relativos a cualquier dibujo, documento y trabajo realizado por el Destinatario (ya sea pasado, presente o futuro) utilizando la Información Patentada pertenecerá y serán ejercidas por el Propietario. El destinatario desempeñará todas las actividades y ejecutará todos los documentos necesarios para permitir al Propietario obtener, defender o hacer valer sus derechos en esos dibujos, documentos o trabajo.

4. Este Acuerdo se regirá y se interpretará de acuerdo con la ley Inglesa y está sujeto a la jurisdicción no excluyente de los Tribunales Ingleses.

En nombre y por cuenta del Destinatario:

Firmado:_____

Nombre:_____

Cargo:_____

En nombre y por cuenta del Propietario:

Firmado:_____

Nombre:_____

Cargo:_____

MUESTRA 2: ACUERDO DE NO DIVULGACIÓN QUE RIGE LA INFORMACIÓN DE AMBAS PARTES

Fuente: Gene Quinn, "Mutual Non-Disclosure Agreement," enero 2008, disponible en http://www.ipwatchdog.com/tradesecret/mutual-confidentiality-agreement/

Queda entendido y convenido que las partes en el presente Acuerdo, cada una proporcionaría a la otra cierta información que pueda ser considerada como confidencial. Para asegurar la protección de esa información y en consideración al acuerdo para intercambiar la información indicada, las partes acuerdan lo siguiente:

1. La información confidencial a ser divulgada bajo este Acuerdo ("Información Confidencial") se puede describir como e incluye:

   Información técnica y comercial relacionada a ideas propias, ideas patentables y/o secretos comerciales, productos y servicios existentes y/o previstos, investigación y desarrollo, producción, costos, información de rentabilidad y margen, finanzas y proyecciones financieras, consumidores, clientes, marketing y planes de negocios actuales o futuros y modelo, independientemente de si esa información es señalada como "Información Confidencial" en el momento de su divulgación.

   Además de lo anterior, la Información Confidencial también incluirá, y que las partes tendrán el deber de proteger, cualquier otra información confidencial y/o sensible que es (a) revelada como tal por escrito y marcada como confidencial (o con otra denominación similar) en el momento de la divulgación; y/o (b) divulgada de cualquier otra forma y denominada como confidencial en el momento de la divulgación así como también resumida y denominada como confidencial en un memorando escrito entregado dentro de treinta (30) días a partir de la divulgación.

2. Las partes usarán la Información Confidencial sólo con el propósito de evaluar potenciales negocios, empleo y/o relaciones de inversión.

3. Las partes limitarán la divulgación de Información Confidencial dentro de su propia organización a sus directores, funcionarios, socios, miembros y/o otros empleados que tengan una necesidad de saber y no divulgarán la Información Confidencial a terceros (ya sea un individuo, corporación u otra entidad) sin el previo consentimiento por escrito. Las partes

cumplirán las obligaciones contraídas en virtud del presente párrafo si toman las medidas para asegurar el cumplimiento de estas obligaciones de confidencialidad por parte de sus empleados, agentes, consultores y otras personas a las que se les permita el acceso a o el uso de la Información Confidencial.

4. Este Acuerdo no impone ninguna obligación a las partes con respecto a cualquier Información Confidencial (a) que tenía antes de la recepción; (b) que es o se convierta en asunto de conocimiento público no por culpa de la parte receptora; (c) se reciba legítimamente de un tercero, que no tiene un deber de confidencialidad; (d) se divulgue sin una obligación de confidencialidad a un tercero mediante, o con la autorización de la parte que la revela; o (e) se desarrolla de manera independiente.
5. Las partes garantizan que tienen el derecho para hacer las divulgaciones en virtud del presente Acuerdo.
6. Este Acuerdo no se interpretará como creación, transmisión, transferencia, concesión u otorgamiento a cualquiera de las partes de ningún derecho, licencia o autoridad en o para la información intercambiada, excepto el derecho limitado a utilizar la Información Confidencial especificada en el párrafo 2. Aun más, y específicamente, ninguna licencia o transmisión de ningún derecho de propiedad intelectual es concedido o está implícito en este Acuerdo.
7. Ninguna de las partes tiene la obligación bajo los términos de este Acuerdo a la compra de ningún servicio, mercancía o intangible de la otra parte. Además, ambas partes reconocen y aceptan que el intercambio de información en virtud de este Acuerdo no confirma u obliga a ninguna de las partes a una relación contractual presente o futura (salvo en los casos en que esté expresamente indicado en este documento), ni tampoco el intercambio de información se entenderá como un incentivo para actuar o no actuar de una determinada manera.
8. Ninguna de las partes será responsable ante la otra en forma alguna por las decisiones, obligaciones, costos o gastos incurridos, cambios en las prácticas empresariales, planes, organización, productos, servicios o de otra manera, basado en la decisión de cualquiera de las partes de utilizar o confiar cualquier información intercambiada en virtud de este Acuerdo.
9. Si existiera un incumplimiento o amenaza de incumplimiento de cualquier disposición de este Acuerdo, se acepta y entiende que la parte que no incumplió no tendrá una compensación adecuada en dinero u otros daños y, en consecuencia, tendrá derecho a un desagravio por mandato judicial; a condición, sin embargo, de que ninguna especificación en el presente Acuerdo de algún recurso en particular sea interpretado como una renuncia o prohibición de cualquier otro recurso en el caso de un incumplimiento o amenaza de incumplimiento del presente Acuerdo.
10. Este acuerdo establece el acuerdo completo entre las partes sobre la divulgación de Información Confidencial y reemplaza cualquier acuerdo previo, entendimiento o representación con respecto al mismo. Cualquier adición o modificación a este Acuerdo debe ser hecha por escrito y firmada por representantes autorizados de ambas parte. Este Acuerdo se realiza bajo y será interpretado en conformidad a las leyes del estado de_____, U.S.A. En caso de que

este acuerdo, sea incumplido, cualquiera y todas las disputas deben ser resueltas en una corte de jurisdicción competente en el estado de_____, U.S.A.

11. Si cualquiera de las disposiciones de este Acuerdo se declara inejecutable, el resto se ejecutará en la medida de lo posible y la disposición inejecutable se considerará modificada en el grado necesario que permita la ejecución del Acuerdo en su conjunto.

POR TANTO, las partes reconocen que han leído y comprendido este Acuerdo y voluntariamente aceptan los deberes y obligaciones establecidas aquí.

Destinatario de la Información Confidencial:

Nombre (a máquina o letra imprenta):_____
Compañía:_____

Cargo:_____

Dirección:_____

Ciudad, Estado, Código postal:_____

Firma:_____

Fecha:_____

Destinatario de la Información Confidencial:

Nombre (a máquina o letra imprenta):_____

Compañía:_____

Cargo:_____

Dirección:_____

Ciudad, Estado, Código postal:_____

Firma:_____

Fecha:_____

ANEXO D

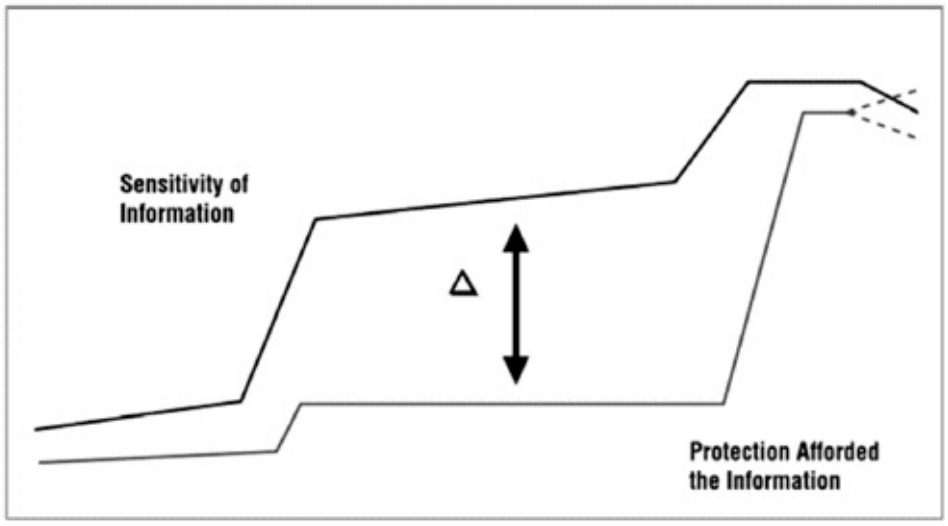
INFORMES TÉCNICOS Y CUADERNOS DE LABORATORIO

MANEJO DE INFORMES TÉCNICOS

Las empresas con instalaciones de investigación y desarrollo deben poner especial atención a los informes técnicos y cuadernos de laboratorio como parte de su estrategia de protección de activos de información (IAP). En primer lugar, es una buena práctica de negocios y, en segundo lugar, los procedimientos adecuados para el manejo de esos documentos asegurarán una sólida base legal en el evento de una demanda por secreto comercial o infracción de patente.

Los responsables de formular políticas a veces no consideran los pasos interdependientes que conducen a la producción de un informe técnico. Esto puede provocar una situación en la que cual hay un complejo sistema para la protección del producto terminado, pero relativamente poca preocupación para los numerosos pasos intermedios. *Sin embargo, a menudo es en las etapas intermedias donde se produce la mayor posibilidad de compromiso con la menor posibilidad de detección.* Esto, en parte, es la razón por la que se requiere un intenso y exhaustivo sistema de auditoría y elaboración de informes.

Como se indica en el gráfico, el período de mayor vulnerabilidad para la posible pérdida de información crítica es en las fases intermedias de un proyecto. Generalmente, la información disponible en los inicios de un proyecto, sobre todo un esfuerzo de investigación, está relacionada con las ciencias básicas y a menudo no se le considera altamente sensible. Las medidas de protección no son muy robustas en este punto, así que generalmente coinciden bastante bien con la sensibilidad de la información.



Durante la investigación de mercado y cerca del lanzamiento del producto, puede haber una gran cantidad de información sensible, pero generalmente hay una seguridad robusta en el lugar –nuevamente una buena coincidencia entre los niveles de sensibilidad y protección.

En las fases medias, sin embargo, la sensibilidad y cantidad de información relacionada con la iniciativa generalmente aumenta rápidamente, algunas veces de manera inesperada. Las medidas de protección de

la información pueden no ser una alta prioridad o pueden no estar a la altura de la cantidad o sensibilidad de la información. Del mismo modo, el personal clave puede no darse cuenta de la importancia o sensibilidad de la información en este punto. Por último, este período suele ser más largo que otras fases del proyecto, y los participantes pueden llegar a ser complacientes respecto a la protección de la información. Generalmente, por estas razones éste es el periodo cuando la información está más vulnerable, tanto a las amenazas intencionales como a las accidentales (Peterson, 2005).

Otro asunto que a menudo se pasa por alto es cómo se almacena y manipula la información una vez que se ha comercializado el producto o publicado el informe técnico. A menudo, la atención se ha desplazado a un nuevo producto en desarrollo, y el material es trasladado a un lugar de almacenamiento diferente, que puede estar bajo el control de empleados no familiarizados con la importancia de la información. Este es un ejemplo perfecto de por qué un programa de IAP eficaz debe incorporar la protección de la cuna a la tumba, incluyendo el control de la distribución secundaria de informes técnicos y acceso a los datos sin procesar. Esto es además de la protección del producto final o proceso, que generalmente es más sencillo.

Las consecuencias de una pérdida pueden ser dependientes del tiempo. En otras palabras, el compromiso de un secreto comercial en particular o una pequeña cantidad de información patentada puede tener un enorme impacto en un proyecto en la fase de investigación de las aplicaciones, pero sólo un impacto menor en la fase de comercialización. La oportunidad, dependencia del tiempo y fases del proyecto siempre deben considerarse al medir las posibles consecuencias de una pérdida de información.

Cronología de un Producto Comercial Basado en la Tecnología
(Peterson, 2005)

Los plazos involucrados en un proyecto de investigación o desarrollo pueden ser largos, lo que aumenta la complejidad del enfoque del IAP. La investigación inicial, los esfuerzos de desarrollo, los datos en bruto, los resultados de los ensayos, los prototipos, los resultados de pruebas intermedias y los datos técnicos deben ser considerados activos para ser protegidos, así como los productos terminados, informes y procesos.

PROCEDIMIENTOS PARA LOS CUADERNOS DE LABORATORIO

Las siguientes son directrices generales para manejar y proteger los cuadernos de laboratorio.

1. GENERAL

Mantener los cuadernos de laboratorio es parte de la responsabilidad profesional de científicos e ingenieros. Los cuadernos de laboratorio bien documentados son un importante activo para la

compañía, ya que, por ejemplo, ayudan a evitar la reiteración de trabajo experimental, permiten la reconstitución de pasos para aislar los aspectos críticos de un nuevo descubrimiento o invento, establecer legalmente importante documentación de un invento o descubrimiento y permitir la correcta decisión del inventor.

El requerimiento, desde el punto de vista legal, de mantener los documentos adecuados para las patentes es el más estricto. Por lo tanto, los cuadernos mantenidos apropiadamente con ese propósito normalmente serán suficiente para todos los demás efectos. Los requerimientos para registros de patente han sido establecidos a través de precedentes legales en los cuales los tribunales consideran el testimonio de un inventor como inadecuado para establecer la prueba de su propia invención. En todos los casos, los tribunales exigen que el testimonio del inventor sea corroborado por partes desinteresadas que tengan conocimiento de primera mano de la realización del invento.

2. PRINCIPIOS BÁSICOS LEGALES

Los procedimientos para la mantención de los cuadernos de laboratorio se basan en varios principios jurídicos básicos, que se resumen a continuación:

2.1. Un invento completo se compone de dos eventos:

- Concepción de la idea
- Reducción a la práctica[3] (demostrando la utilidad de los datos para el propósito previsto

2.2. El testimonio del inventor y los registros por sí mismos no son suficientes para establecer la concepción y reducción a la práctica. El testimonio debe ser corroborado en todos los sentidos por otros.

2.3. La concepción, estando totalmente dentro de la mente del inventor, puede ser probada sólo por su revelación a otros.

2.4. La concepción se prueba mejor a través de un documento escrito que revele el invento en forma completa, fechado, firmado por el inventor y en presencia de un testigo que entienda el invento

2.5. La reducción a la práctica (ejecución real del invento) debe ser probada (corroborada) por alguien más que pueda jurar que, ella o él, o bien

- vio al inventor realizar todos los aspectos importantes del invento o
- personalmente realizó el invento en nombre de o en la dirección del inventor.

2.6. Ni el testigo de la concepción ni el que corrobora la reducción a la práctica puede ser un coinventor. Donde participan dos o más inventores en conjunto, ninguno de ellos puede corroborar ningún otro invento conjunto. El testimonio de cada uno de ellos debe ser corroborado por alguien mas que no sea un de los inventores conjuntos.

2.7. Tanto el testigo de la concepción y el corroborador de la reducción a la práctica deben

entender el invento.

2.8. El testimonio del testigo y del corroborador debe ser apoyado por evidencias tangibles preparadas en el momento. Esa evidencia puede ser en forma de escritos, bocetos, croquis, planos, muestras, modelos, etc.

2.9. Documentos sin fecha o fechas anteriores no son evidencias admisibles.

3. REQUISITOS LEGALES MÍNIMOS DE MANTENCIÓN DE CUADERNOS PARA PROBAR LA CONCEPCIÓN Y REDUCCIÓN A LA PRÁCTICA

Teniendo en cuenta las reglas anteriores, la siguiente práctica debe ser seguida por cada empleado involucrado en el trabajo de laboratorio que implique investigación y desarrollo:

3.1. En la concepción de una idea origina, el inventor debe documentar inmediatamente esta idea en un cuaderno con los bocetos, dibujos y discusiones apropiadas, con el fin de un experto en el campo involucrado pueda comprenderlos. El registro en el cuaderno debe entonces estar fechado y firmado por el inventor. El registro en el cuaderno luego debe ser leído y comprendido por dos testigos que firmen la parte inferior de la siguiente forma:

"Visto, leído y comprendido por_____(nombre) en_____(fecha)".

3.2. La reducción a la práctica por el inventor pude ser probada solamente por el testimonio de alguien más que personalmente observó la reducción a la práctica y sabía lo que se hacía. La reducción a la práctica puede ser desarrollada por el inventor o por otra persona bajo la dirección del inventor. En el caso de una invención de proceso, el corroborador de la reducción a la práctica necesita observar sólo los pasos esenciales del proceso. La reducción a la práctica debe documentarse en un cuaderno de laboratorio. Pero, los planos, dibujos, órdenes de compra, etc., relacionados con la reducción a la práctica pueden ser incorporados por referencia en el cuaderno haciendo una clara y positiva identificación de estos documentos. La entrada relativa a la reducción a la práctica debe ser hecha por el inventor o la parte que hace la reducción en nombre del inventor en su cuaderno y luego firmado y fechado por el inventor. La entrada debe entonces ser leída y aceptada por dos personas que presenciaron, de primera mano, los aspectos esenciales de la reducción a la práctica.

Estos testigos corroboradores no pueden ser coinventores, pero deben ser personas competentes del campo científico implicado que estén trabajando en otros proyectos. Después de leer la entrada y aceptarla, los testigos corroboradores deben firmar directamente bajo la entrada de la siguiente manera:

"Visto, leído y entendido por_____(nombre)
en_____(fecha)".

Si una reducción a la práctica se lleva a cabo durante un largo período de tiempo, cada paso significativo debe ser ingresado en el cuaderno en la fecha que se hizo y atestiguado en la manera descrita anteriormente.

3.3. Se deben respetar los siguientes detalles administrativos en el uso y manejo de los cuadernos de laboratorio:

3.3.1. El cuaderno debe ser anillado y no hojas sueltas.

3.3.2. Cada entrada debe, en general, establecer por qué fue hecho el trabajo, qué se hizo, quién lo hizo, cuándo, con qué resultados y las conclusiones extraídas de los resultados.

3.3.3. Todas la entradas en el cuaderno deben ejecutarse consecutivamente sin espacios en blanco. Todas las partes no utilizadas deben ser bloqueadas, fechadas y firmadas.

3.3.4. No se debe usar terminología codificada a menos que el código esté plenamente definido en el cuaderno. Se permiten abreviaturas comúnmente aceptadas.

3.3.5. El registro no debe ser falsificado.

3.3.6. El registro no debe ser alterado. Cualquier error que se produzca no debe ser borrado o alterado. En su lugar, se debe dibujar un sola línea sobre el error y las correcciones se efectúan inmediatamente después. Las entradas anteriores pueden ser corregidas o revisadas por una nueva entrada, la cual hace referencia específica a la anterior.

3.3.7. Todas las entradas deben ser hecha con tinta o lápiz indeleble.

3.3.8. Las entradas no deben ser retroactivas.

3.3.9. Todos los registros deben mantenerse actuales, ya que cualquier demora en el registro de las materias de concepción o reducción a la práctica disminuye seriamente el valor de la entrada. La entrada hecha debe ser suficientemente completa de modo que un experto en la materia pueda comprender el invento. Cualquier crítica o punto óptimo debe ser establecido específicamente.

3.3.10. Asimismo, debe ingresarse cualquier esfuerzo fallido o que no funcione como se esperaba. Pero, se debe tener precaución para evitar demasiadas conclusiones negativas.

4. CONTROL DEL CUADERNO

4.1. Cada nuevo empleado involucrado en el trabajo de laboratorio de investigación y desarrollo debe adquirir un cuaderno de la biblioteca de investigación.

4.2. Todos los cuadernos serán numerados consecutivamente por el bibliotecario de investigación y serán registrado a nombre de la bibliotecaria y emitidos directamente a la persona que utilizará el cuaderno.

4.3. Un cuaderno totalmente lleno debe ser devuelto a la biblioteca de investigación, pero el cuaderno debe ser guardado en la oficina del autor para fines de referencia.

4.4. Al término, un empleado devolverá todos los cuaderno a la biblioteca de investigación. Cualquier otro empleado que vaya a continuar el trabajo puede tener el registro de los cuadernos transferidos a fin de que puedan ser guardados en su oficina para fines de referencia.

5. DIVULGACIÓN DE LOS INVENTOS

5.1. Después de realizar las entradas según lo establecido anteriormente, la revelación de un invento debe completarse como se establece en Standard Procedure.

5.2. Los empleados no divulgarán los datos de los cuadernos y la información relativa a los invento a nadie fuera de la compañía excepto en cumplimiento de los estándares de procedimientos de divulgación

6. DISPOSICIONES PARA LOS CUADERNOS DE LABORATORIO ELECTRÓNICOS

6.1. En el entorno actual, las organizaciones utilizan cada vez más cuadernos de laboratorio electrónicos en lugar de cuadernos de hojas impresas.

6.2. Cuando los cuadernos de laboratorio electrónicos están en uso, serán protegidos de manera acorde con los procedimientos descritos anteriormente y consistentes con las políticas sobre IAP y de seguridad de TI de la organización.

6.3. Deben existir controles para prohibir o manejar cuidadosamente la eliminación de los cuadernos de laboratorio electrónicos de las instalaciones donde normalmente se utilizan y almacenan. Con el predominio del robo de dispositivos electrónicos y la habilidad para transferir, copiar o modificar fácilmente enormes cantidades de datos, la integridad de los cuadernos de laboratorio es altamente vulnerable a ser comprometida.

ANEXO E

DESTRUCCIÓN Y ELIMINACIÓN DE INFORMACIÓN

Lo siguiente se base en material de la National Association for Information Destruction (www.naidonline.org) y es usado con autorización.

Toda empresa tiene información que requiere destrucción.

Las listas de clientes, las listas de precios, estadísticas de ventas, borradores de ofertas y correspondencia, e incluso memorandos que contienen información acerca de la actividad de la empresa que sería de interés para cualquier competidor. A todas las empresas también se le ha encomendado información que debe mantenerse en privado.

Sin la adecuada seguridad, la información termina en el basurero, donde queda fácilmente y legalmente disponible para cualquier persona. Cualquier establecimiento que simplemente descarta información privada y patentada se expone al riesgo de demandas criminales y civiles y a pérdidas de la empresa.

Los registros almacenados deben ser destruidos con una programación periódica.

Ningún registro debe mantenerse más tiempo de lo necesario para fines comerciales o de cumplimiento. Destruyendo rutinariamente los registros almacenados, una compañía puede evitar aparecer como sospechoso en el evento de un litigio o auditoría. La destrucción regular también limita la cantidad de material que la empresa debe proporcionar en procedimientos legales.

Los registros de la empresa desechados incidentalmente a diario deben ser protegidos.

La basura diaria de toda empresa contiene información que podría ser usada en su contra. Esos registros incluyen mensajes telefónicos, memos y borradores de ofertas y correspondencia.

El reciclaje no es una alternativa apropiada para la destrucción de información.

El reciclaje no es equivalente a destrucción segura. Los papeles son regalados o vendidos y no hay ninguna forma práctica de establecer dónde y cuando fue destruido un documento. Es mejor organizar el reciclaje después que los materiales se han destruido adecuadamente.

La Due Diligence es esencial.

Cualquier empresa que contrate un servicio de destrucción de la información debe exigir que le entreguen un testimonio firmado documentando la fecha en que los materiales fueron destruidos. El certificado de destrucción, es un importante registro legal. Esto, sin embargo, no transfiere la responsabilidad de la confidencialidad de los materiales al contratista.

Si surge información privada después que el contratista acepta, un tribunal puede preguntar por el proceso mediante el cual el contratista fue seleccionado. Cualquier empresa que no muestre debida diligencia en su selección de un contratista podría ser encontrado negligente. La Due Diligence

podría consistir de una revisión de las políticas y procedimientos del contratista y seguida de una auditoría del lugar.

La mayoría de las empresas de almacenamiento de registros no brindan ellas mismas servicios de trituración seguros.

Si la empresa de almacenamiento subcontrata sus servicios de destrucción, el cliente debe realizar una investigación de due diligence de la empresa de destrucción de documentos que usa.

REFERENCIAS

ASIS International. (2007). Information asset protection guideline. Alexandria. VA. Available: http://www.asisonline.org/guidelines/guidelinesinfoassetsfinal.pdf [2008, August 14].

ASIS International. (2007). Trends in proprietary information loss. Alexandria, VA. Available: http://www.asisonline.org/foundation/noframe/loss.pdf [2008, August 14].

ASIS International Information Asset Protection Council. (2005). IAP toolkit. Available: http://www.asisonline.org/councils/InfoToolkit.exe [2008, August 14].

Crowdy, T. (2006). The enemy within: A history of espionage. Westminster, MD: Osprey Publishing. Federal Bureau of Investigation. Focus on economic espionage. Available: www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage [2011, April 6].

Hassett, D. B. (2003, April). Is your model non-disclosure agreement adequate?, Wireless Watch. Available: www.wileyrein.com/publication_newsletters.cfm?id=12&publication_ID=10040 [2008, August 14].

Kramer, L. A., Heuer, R. J., Jr., & Crawford, K. S. (2005). Technological, social and economic trends that are increasing U.S. vulnerability to insider espionage. PERSEREC Technical Report 05-10. Monterey, CA: Defense Personnel Security Research Center.

Microsoft Corporation. (2006). Regulatory Compliance Planning Guide. Available: http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/default.mspx?mfr=true [2008, August 14].

Moberly, M. D. (2006). Positioning intellectual property, intangible assets and proprietary competitive advantages to beat the odds against counterfeiting and piracy. White paper. Memphis, TN: Knowledge Protection Strategies.

Moberly, M. D. (2007). Risk assessments and due diligence for business transactions. White paper. Memphis, TN: Knowledge Protection Strategies.

Peterson, K., CPP. (2005). A strategic approach to information protection for small businesses and organizations: Getting started. White paper. Herndon, VA: Innovative Protection Solutions.

Poteat, S. E. (2001, Winter). The attack on America's intellectual property: Espionage after the Cold War, The Bent of Tau Beta Pi.

Sun Tzu. (1983). The art of war. Ed. J. Clavell. New York, NY: Dell Publishing.

United States Department of Energy. Espionage and the Manhattan Project (1940-1945). Available: www.mbe.doe.gov/me70/Manhattan/espionage.htm [2008, August 14].

United States Department of Justice. (2006). Progress report of the Department of Justice's task force on intellectual property. Available: http://www.usdoj.gov/opa/documents/ipreport61-906.pdf [2008, August 14].

United States General Accountability Office. (2007, April 12). Intellectual property: National enforcement strategy needs stronger leadership and more accountability. Statement of Loren Yager, Director International Affairs and Trade.

United States Office of the National Counterintelligence Executive. (2006). Annual report to Congress on foreign economic collection and industrial espionage—2005. Available: http://www.fas.org/irp/ops/ci/docs/2005.pdf [2008, August 14].

United States Patent and Trademark Office. Inventor resources. Available: http://www.uspto.gov/web/offices/com/iip/index.htm [2008, August 14].

United States Secret Service and Carnegie Mellon Software Engineering Institute. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. Available: http://www.cert.org/archive/pdf/insidercross051105.pdf [2008, August 14].

Winkler, I. (2005). Spies among us. Hoboken, NJ: Wiley Publishing.

World Intellectual Property Organization. (2003). Non-disclosure agreement. Available: www.wipo.int/sme/en/documents/disclosing_inf.htm [2008, August 14].

CAPÍTULO 2
LA CRECIENTE IMPORTANCIA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

En la película Ocean's Eleven[4], el dueño del casino Terry Benedict descubre que Danny Ocean ha puesto en peligro el sistema de vanguardia de video vigilancia que protege la bóveda de Benedict y sus millones en dinero efectivo. El ataque contra el supuestamente inquebrantable sistema de seguridad se basó en parte en el pirateo a los sistemas de información. La película describe a Benedict como alguien que toma muy seriamente la protección de su dinero y no le da una segunda oportunidad a su personal de seguridad. También en el mundo real, los cibercriminales[5] a diario se aprovechan de las debilidades de seguridad en los sistemas de información corporativos, robando, destruyendo, malversando o abusando de los activos corporativos.

El cibercrimen –uso de los sistemas de información para cometer delitos- es real. En mayo de 2009, el Presidente Obama dijo, "Se estima que sólo el año pasado los cibercriminales robaron propiedad intelectual de las empresas en todo el mundo por un valor de hasta 1 trillón de dólares" (Obama, 2009). A diferencia de lo que ocurre en el mundo físico, los sistemas de información están plagados de vulnerabilidades. Para hacer frente a los nunca-antes-vistos desafíos de la seguridad de los sistemas de información (ISS de ahora en adelante, por sus siglas en inglés), los profesionales de la seguridad deben aumentar su paradigma de seguridad física con un nuevo paradigma de seguridad lógica (Lam & Stahl, 2010).

En *The Structure of Scientific Revolutions* (1962), Thomas Kuhn revolucionó la manera de pensar de los filósofos respecto a la ciencia. Él introdujo la palabra *paradigma* como una herramienta teórica para comprender todo lo que se piensa cuando se considera una escuela de pensamiento científico u otra disciplina rigurosa, como la seguridad física o ISS. Desde esta perspectiva, el paradigma de la seguridad física es el marco que se utiliza en asuntos de procesamiento específicamente centrados en el ámbito de la seguridad física, tales como las cámaras, los autores, la protección de la vida humana y la seguridad de las instalaciones contra las pérdidas físicas. El marco que comprende el paradigma de la seguridad lógica trata con asuntos similares, pero las pérdidas ocurren en el espacio virtual, donde son invisibles desde una perspectiva física y por lo tanto requieren una comprensión diferente para contrarrestarlas.

El propósito de esta parte de *Protección de Activos* es para proporcionar al profesional de la seguridad ya con conocimientos en el paradigma de la seguridad física con una comprensión práctica de un nuevo paradigma de seguridad lógica.

2.1 EL DESAFÍO HUMANO: FALTA DE IMAGINACIÓN

El 11 de septiembre de 2001, los terroristas estrellaron aviones contra las torres gemelas del World Trade Center y en el Pentágono. Un cuarto avión se estrelló en Pennsylvania, en lugar de su objetivo previsto, sólo como resultado del heroico esfuerzo de los pasajeros. El FBI y otras agencias de inteligencia de Estados Unidos tuvieron todos los elementos que necesitaban para ver que el 11/9 venía. Si ellos hubieran conectado los puntos se podrían haber salvado más de 3.000 personas. ¿Por qué los puntos no estaban conectados? En el informe final de la Comisión 911 (National Commission on Terrorist Attacks, 2004, p.336), una respuesta dada fue "falta de imaginación".

Aquí hay otro ejemplo, mucho menos grave, de falta de imaginación. En la puerta de la piscina de un hotel, los huéspedes pueden insertar sus llaves de tarjeta en una ranura, abrir la puerta y entrar al área de la piscina. La seguridad parecía estar funcionando perfectamente, hasta que una joven caminó hasta la puerta, extendió su delgada mano a través de las barras por debajo del pestillo, lo alcanzó y abrió la puerta.

En la pantalla de ingreso en un sitio Web, los usuarios podrían haber esperado entrar su identificación de usuario y contraseña, lo mismo que en la piscina los huéspedes podrían esperar ingresar sus llaves de tarjeta en la ranura de la puerta. Sin embargo, un usuario podría ser capaz de acceder al sitio ingresando "' o 1=1 – " o incluso algo muy complicado como lo siguiente:[6]

http://www.sanitized.net/Communications/PhoneList/directory.asp?fieldValue0=1′
%20UNION%20ALL%20select%20″,name,″,″,″,″,″,″
%20from%20MASTER..SYSDATABASES&fieldName0=EE_ID&fieldType0=202&fieldValue1=&fieldN

Ataques como estos -con nombres arcanos, por ejemplo, *SQL- injection, cross-site scripting, content spoofing*, e *information leakage*- son como las delgadas muñecas de la joven que entró en la piscina sin una llave, proporcionando a los cibercriminales el acceso al back-end (lado interno) de los activos corporativos.[7]

Antes de que este tipo de ataques ocurriera, nadie se lo había imaginado. Incluso después de imaginado, muchos sitios Web siguen siendo vulnerables a esos ataques, entregando a los piratas acceso total a la información subyacente.

No hace mucho tiempo, un director corporativo de tecnología de la información (TI) escribió lo siguiente acerca de la susceptibilidad de su empleador a los fraudes bancarios en línea:

> Teresa tiene un dispositivo electrónico (fob) que genera códigos de contraseñas, el cual cambia cada 30 segundos. El dispositivo no está conectado a la computadora en modo alguno. Para completar la autorización de una transacción en la computadora, ella necesita ingresar

un código de contraseña de su dispositivo en un lapso de 30 segundos. **No puedo imaginar la forma en que un pirata informático podría manipular [hackear] eso**. [Énfasis añadido].

No obstante, dos semanas atrás, un artículo del *Washington Post* sobre el robo de US$ 447.000 de la cuenta bancaria de una compañía había dicho esto acerca de la seguridad de la autenticación multifactorial, como el dispositivo de Teresa (Krebs, 2009):

> Algunos tipos de malware (software maligno), especialmente un tipo de programa Troyano de robo de datos conocido como "Zeus", permite a los piratas informáticos cambiar la visualización de la página de acceso a un banco cuando la víctima está ingresando sus datos de identificación. Por ejemplo, cuando una víctima envía su contraseña temporal junto con sus datos de identificación, el malware puede forzar al navegador a volver a una página falsa (que sigue mostrando el nombre de dominio del banco en la barra de URL) indicando que el sitio del banco no está en activo por mantenimiento y que por favor intente volver en 15 minutos. Mientras tantos, esas credenciales no son enviadas al banco sino que a los piratas informáticos.
>
> Esta táctica es notablemente eficaz: Cuando un cliente involuntariamente espera las instrucciones, los ladrones usan esos datos de identificación para iniciar sesión como si fueran la víctima e iniciar transferencias no autorizadas desde esa cuenta.

La falta de imaginación es parte del ser humano. Después de experimentar una mala situación, una persona puede imaginar escenarios similares. El desafío radica en situaciones que una persona no ha experimentado antes.

2.2 ESTADO DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La revolución de la microcomputadora –y con ello el surgimiento de las redes de área local, redes de área amplia e Internet- cumplió 35 años en 2010.[8] La interconexión de computadoras y redes ha traído grandes beneficios de productividad y abrió emocionantes nuevos campos de entretención e información. Acercó al mundo. Sin embargo, estas virtudes no están exentas de consecuencias imprevistas y, a veces, no deseadas.

El 01 de julio de 2003, entró en vigencia la California Senate Bill 1386, la primera ley de incumplimiento de divulgación de la nación. La ley exige que cualquier organización que realice negocios en California notifique a los residentes afectados si la organización tiene razones para creer que información personal no encriptada de los residentes de California ha sido adquirida por una persona no autorizada.[9] La mayoría de los estados ha seguido a California con sus propias leyes de incumplimiento de divulgación, y es probable una ley nacional.

En poco más de seis años desde que la ley de California entró en vigencia, la Privacy Rights Clearinghouse (2009) ha identificado más de 340 millones de registros de consumidores que han sido violados. Aquí hay sólo unas pocas de las muchas compañías que han reconocido que sufrieron violaciones de su información:

Choicepoint
Sam's Club
MCI
Bank of America

T.J. Maxx
Citi Financial
Kodak
Time Warner
Ernst & Young
Ralph Lauren
Motorola
Ford Motor
JP Morgan
DSW
Deloitte
Hanover

La cifra de 340 millones incluye sólo violaciones reportadas. No incluye las violaciones descubiertas, pero no reportadas, las violaciones no descubiertas u otras pérdidas de información –tales como robo en la banca en línea- que legalmente no es necesario que sea revelada.

Los 340 millones de registros de datos violados representan sólo la punta del iceberg. Ellos también demuestran cómo el cibercrimen ha cambiado en los últimos años. En el pasado, las grandes amenazas de los sistemas de información eran internas. Existían pocos piratas informáticos; de esos que lo hicieron, la mayoría era para su propio ego; y el máximo daño que causaban se limitaba al robo de los recursos informáticos y a la negación del servicio producto de ataques con virus.

Los piratas informáticos que usaban la piratería por placer o para hacer crecer su reputación, ahora están en eso por dinero (Herley & Florencio, 2009). Ellos son cada vez más sofisticados y aprenden a burlar las defensas. Una fuente informa que "los chicos malos están adaptando sus actuales estrategias de protección e inventando nuevas maneras para alcanzar los datos que ellos valoran" (Verizon Business RISK Team, 2009, p.47).

En julio de 2009, los cibercriminales se dirigieron a las cuentas de los titulares de YouTube con ataques de phishing[10] (Harwood, Junio 2009). El 17 de agosto de 2009, tres hombres fueron acusados de robar más de 130 millones de números de tarjetas de crédito. Ellos eran capaces de obtenerlas explorando las vulnerabilidades de los sitios Web corporativos (Trotta, 2009). También en agosto de 2009, el sitio de la red social Twitter fue deshabilitada por piratas informáticos que intentaron tomar represalias en contra de un solo usuario, pero derribó todo el sitio (Acohido, 2009). Por cierto, tomó casi 100.000 bots[11] (software de aplicaciones que ejecutan tareas automatizadas) bajo el control de los piratas informáticos para derribar el sitio. Costó alrededor de US$ 5.000 arrendar esos bots. Además, continúan descubriéndose nuevas formas de acceder a las redes inalámbricas, en detrimento de las empresas (Mills, 2009).

En testimonio ante el Congreso, un experto en seguridad informática señaló lo siguiente acerca de los ataques de piratas informáticos (kellerman, 2009):

los ciberataques se han convertido en un fenómeno totalmente generalizado, que se basa en parte en:

- el aumento de la conectividad y disponibilidad de las redes atacables y de las vulnerabilidades de sistemas y aplicaciones
- la capacidad de los cibercriminales para obtener importantes recompensas financieras a través de ataques exitosos
- las federaciones mundiales entre las distintas clases de cibercriminales y desarrolladores de malware
- el Estado-Nación, terrorista y políticamente dirigido a impulsar los esfuerzos del cibercrimen
- la carencia de aplicación de una ley cohesiva alrededor del mundo

La extorsión cibernética ha empezado a levantar su fea cabeza y ahora es un problema para las empresas en Estados Unidos (Wagley, 2009). Los cibercriminales han descubierto que no necesitan cambiar su malware tan pronto, sino que pueden implementarlo en más sitios (Harwood, agosto 2009). Además, utilizan técnicas automatizadas que continuamente ponen en peligro sitios Web legítimos, aumentando la oportunidad de que los usuarios finalmente sean redirigidos a un sitio ilegítimo. Más aun, los criminales están cambiando el código de malware por lo que no es detectado por los sistemas antivirus tradicionales.

Tal vez, el desafío más serio es la reciente seguidilla de robos de banco en línea. Según el FBI (2009), los ladrones cibernéticos pirateando la empresas se pequeño y mediano tamaño han robado alrededor de US$ 100 millones de cuentas bancarias estadounidenses. Algunos de estos ataques son lo suficientemente sofisticados para derrotar los sistemas de autenticación de dos factores.

El Computer Security Institute (CSI) Computer Crime and Security Survey (Richardson, 2008) descubrió que el fraude informático financiero promedio cuesta a la empresa víctima US$ 500.000 y un ataque bot promedio –un ataque a través de las computadoras cuya seguridad está en peligro, a veces cientos de miles- cuesta US$ 350.000. Esos ataques pueden tener serios impactos. Un caso afectó las operaciones de un hospital de Seattle (U.S. Attorney's Office, 2006). El informe del CSI también señala que el 27 por ciento de los ataques en 2008 fueron los ataques en los cuales una parche de malware fue escrito directamente para atacar una compañía específica.

La investigación de Verizon de 500 violaciones descubrió que durante el curso de estas violaciones, fueron robados 285 millones de registros (Verizon Business RISK Team, 2009). El estudio concluyó que el 74 por ciento de los registros fueron robados por fuentes externas. Kellerman (2009) corrobora la opinión de que los internos ya no son la causa de la mayoría de las pérdidas.

Además, el informe del CSI señala que los ataques de menor importancia siguen siendo un problema. Mischele Kwon, ex director del United States Computer Emergency Readiness Team (US-CERT) llama a esos ataques un "problema de higiene" (Kwon, 2009), es decir, un problema conocido que puede ser solucionado con due diligence. Sin embargo, es el ataque más sofisticado que está obteniendo la mayor parte de los registros robados (Verizon Business RISK Team, 2009).

El informe de Verizon señala que el profesionalismo del crimen informático está aumentando. La amenaza ya no viene de los "script kiddies"[12], sino de consorcios del crimen organizado, el cual tiene los fondos para realizar ataques más sofisticados. De hecho, Verizon concluyó que el 91 por ciento de los registros robados en 2008 fueron hechos por grupos del crimen organizado. CSI señala que los programas cortafuegos y antivirus son "fundamentalmente imperfectos", y que el malware y otros ataques pueden eludir controles basados en la firma. Además, Verizon afirma que en la mayoría de las violaciones exitosas, alguien fue capaz de tomar ventaja de un error cometido por la víctima e instaló el malware para obtener ventaja de ello.

Las noticias no son tan malas. Aparentemente, hay un exceso de oferta en el mercado del inframundo para los números de tarjetas de crédito, por lo que ahora los números de identificación personal (PIN) son los objetos de interés (Verizon Business RISK Team, 2009, p.7):

> El valor potencial de participación en el cibercrimen no existiría sin un mercado para el robo de información. Como con cualquier sistema de mercado legítimo, el valor unitario de bienes y servicios fluctúa con la oferta y demanda…Los criminales han rediseñado sus procesos y desarrollado nuevas herramientas –como el memory-scraping malware[13]- para robar este valioso producto. Esto ha llevado a la exitosa ejecución de las complejas estrategias de ataque que antes se pensaba que sólo eran posibles teóricamente.

Más aun, el malware personalizado va en aumento. Verizon estima que el 8 por ciento de los 285 millones de registros violados fueron tomados con malware personalizado creado específicamente para el ataque.

Los criminales también están ocultando su trabajo, creando desafíos para quienes tienen que capturarlos o investigar las consecuencias de los crímenes. Los investigadores descubrieron "anti-forenses" –intentos de ocultar sus pistas- en más de un tercio de los casos en la investigación de Verizon.

También está aumentando el uso del ciberespacio por entidades gubernamentales. Por ejemplo, en el 2008, "el estado-nación de Georgia fue atacado por piratas informáticos, presumiblemente desde Rusia" (Wilson, agosto 2009). Wilson también escribe acerca de los ataques contra Estonia y del uso de la guerra cibernética en los enfrentamientos entre Israel y Hamas. En julio de 2009, sitios Web de Corea del Sur también fueron atacados presuntamente por Corea del Norte (Kim, 2009).

Rogueware, el software que pretende ser un software de seguridad, pero que realmente pone en peligro una computadora, también va en aumento. Se estima que los cibercriminales están haciendo US$ 34 millones al mes logrando que los usuarios descarguen este software malicioso (Correll, 2009).

Ahora, incluso los teléfonos no son seguros. El malware móvil es un centro de beneficios prometedor para los criminales (Dunham, 2009). Los usuarios de teléfonos podrían estar comprometidos antes de que incluso comiencen a realizar actividades bancarias en el teléfono.

Stewart Baker, ex secretario adjunto de seguridad nacional de Estados Unidos, ofrece este resumen (2009):

> En quince años, las redes descentralizadas se han trasladado de usos novedosos como el monitoreo de máquinas de café comunitarias a la gestión de activos financieros, telecomunicaciones, y la red eléctrica. Eso es bueno y malo, porque esta revolucionaria nueva tecnología representa riesgos reales. Confiamos mucho más de nuestros activos críticos a las redes TI de lo que alguna vez lo hicimos, y las

vulnerabilidades de seguridad que pueden haber sido tolerables hace quince años pueden tener devastadoras consecuencias hoy en día.

Un informe de IBM concluye que "todo sitio Web debe ser visto como sospechoso y todo usuario es un riesgo" (IBM Global Technology Services, 2009).

El crimen y las situaciones descritas en esta sección afectan sistemas que los profesionales de seguridad usan en su trabajo cotidiano y que ellos están encargados de proteger. Los profesionales de la seguridad deben instruirse ellos mismos en las formas de la seguridad de la información –y también mantenerse al tanto de los cambios que se están produciendo.

2.3 ECONOMÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Los incidentes de seguridad de la información cuestan dinero. Por ejemplo, un virus informático produce la pérdida en productividad del personal de una organización además del tiempo y los gastos para que el personal de TI elimine el virus y restaure la disponibilidad. Por lo general, la pérdida de productividad es más costosa que el costo de la limpieza del ataque de virus. En un caso, eliminar el virus de la red de un bufete de abogados requirió tres días de trabajo por dos personas de TI y dos consultores, costando a la oficina aproximadamente US$2.400 en tiempo del personal y otros $10.000 en honorarios de los consultores. Mientras tanto, el bufete estimó que la productividad de sus 100 abogados se redujo en un 20 por ciento. El costo en pérdidas de facturación excedió los US$ 25.000, más del doble del costo de limpieza del ataque de virus.

El costo del robo de un secreto comercial por un ladrón cibernético es el valor del secreto comercial de la compañía. Las compañías deben preguntarse qué les costaría a ellos si un competidor tuviera la propiedad intelectual como sus listas de clientes, información de precios, estructura de costos, planes estratégicos o procesos patentados.

El costo del robo de los números de seguridad social de los clientes incluye el costo de notificar a los clientes además de los servicios de robo de identidad proporcionado para proteger a los clientes y los gastos legales, si se presentan demandas, más la pérdida de la buena disposición. El promedio de costo para cumplir con las leyes de violación de divulgación ahora excede los US$ 200 por registro (Claborn, 2009). Esto se traduce en los costos del incumplimiento de divulgación de más US$ 2 millones por un incumplimiento de una base de datos relativamente pequeña de 10.000 personas.

La implementación de la seguridad también tiene costos. Los cortafuegos y otras tecnologías ISS se llevan el capital lejos de otros usos. ¿Una compañía debería invertir en un nuevo sistema de gestión de ventas o aumentar su actual sistema de antivirus basado en la firma con un sistema moderno de prevención contra intrusos basado en el comportamiento?

El personal de seguridad de los sistemas de información (ISS) está a expensas del personal que puede contribuir más directamente al balance final. Un nuevo vendedor podría contribuir US$1 millón o más en

nuevas ventas. ¿Qué contribuye un analista de seguridad de la información al balance final?

Cada hora que la gerencia pasa en reuniones de seguridad, o que el personal pasa en entrenamiento de conciencia de seguridad, es una hora que podría contribuir también al balance final.

En la gestión básica de riesgos, cuánto se debe gastar para prevenir un incidente de ISS es igual a la probabilidad del incidente multiplicado por su costo (Gordon & Loeb, 2006). En relación con la gestión de riesgos, es un deber legal de la empresa tomar medidas para asegurar sus activos de información. Este aspecto fue precisado más de 60 años atrás por el Juez Learned Hand en el caso *Estados Unidos v. Carroll Towing Co.* (1947), en el cual Hand escribió que una parte es negligente si el costo (B) de tomar medidas adecuadas para prevenir el daño es menor que la pérdida monetaria (L) multiplicado por la probabilidad (P) de su ocurrencia ($B < PL$).

Un incidente de ISS crece en número y el costo de la recuperación sube, las compañías deben estar preparadas para invertir más recursos en prevención. Usando los recursos corporativos eficientemente para proteger la información sensible y los sistemas, es uno de los objetivos clave de un programa de ISS (Braun & Stahl, 2005). Dicho programa consiste en todas las actividades y gastos que la organización necesita para proteger la información sensible. El programa puede ser formal, con un ejecutivo específico encargado de la responsabilidad de la gestión (recomendado), o informal, con las actividades y gastos efectuados según sea necesario. En cualquier caso, el objetivo del programa debe ser manejar prudentemente y en forma rentable el riesgo de que la información crítica pueda

- ser comprometida
- ser cambiada sin autorización, o
- no estar disponible

2.4 FACTORES CRÍTICOS DE ÉXITO

Tres dominios que co-evolucionan definen si el programa de ISS de una compañía cumple con el estándar de seguridad del debido cuidado:

- la legislación y regulación en cuanto a la obligación de quienes poseen la información para proteger la información privada de los demás en sus sistemas informáticos
- el derecho contractual y responsabilidad extracontractual sobre la seguridad de la información y los activos de información
- las prácticas de seguridad recomendadas por la comunidad profesional de ISS

En *An Emerging Information Security Minimum Standard of Due Care* (2005), Braun and Stahl analizan esos tres dominios e identifican siete factores críticos de éxito que un estándar de cuidado de la seguridad de la información debe cumplir:

- **Responsabilidad de la dirección ejecutiva**. Alguien de la alta gerencia tiene la responsabilidad de la gestión del programa de seguridad de la información de la empresa, la cual es gestionada de acuerdo con sus políticas de seguridad de la información.
- **Políticas de seguridad de la información**. La empresa ha documentado su enfoque de gestión para la seguridad de la información de manera que cumpla con sus responsabilidades y deberes para proteger la información.
- **Educación y entrenamiento de la conciencia del usuario**. Los usuarios reciben educación y entrenamiento en las políticas de seguridad de la información y de sus responsabilidades personales para proteger la información.
- **Seguridad de redes y computadoras**. El personal de TI está gestionando de forma segura la infraestructura de tecnología de una manera definida y documentada que adhiere a las prácticas efectivas de ISS.
- **Garantía de terceros de la seguridad de la información.** La compañía comparte información con terceros sólo cuando se tiene la seguridad de que esos terceros protegen la información al menos con el mismo estándar de cuidado con que la empresa lo hace.
- **Seguridad física y personal**. La empresa proporciona protección física adecuada a la información, investiga los candidatos al empleo e incorpora la seguridad de la información en las responsabilidades del cargo.
- **Evaluación de riesgos periódica.** La empresa realiza una evaluación o revisión de su programa de ISS, preferiblemente a través de un tercero, abarcando la tecnología y la gestión, al menos una vez al año.

Un octavo factor –la clasificación y control de la información sensible- generalmente es parte del marco de recomendaciones de la política de seguridad de la información (como en ISO 27001 y 27002). Este factor llama a la empresa a comprender las leyes, regulaciones y contratos que le impone las obligaciones de seguridad de la información; identifica su propiedad intelectual que requiere protección; hace un inventario de la información sensible e implementa las medidas de seguridad apropiadas para protegerla; distingue la información como pública, para uso interno, o restringida; y asigna a los propietarios de la información la responsabilidad de definir quién necesita acceso a qué información. El personal que no pertenece al ISS obtiene una mayor comprensión del ISS cuando este octavo factor está incluido.

2.5 IMPLICACIONES PARA LA SEGURIDAD FÍSICA EN UN MUNDO CONVERGENTE

La convergencia de la seguridad física y de la información tiene numerosas definiciones. La Alliance for Enterprise Security Risk Management ofrece esta definición básica (Booz Allen Hamilton, 2005, p.3):

la identificación de los riesgos de seguridad y las interdependencias entre las funciones empresariales y los procesos dentro de la empresa

y el desarrollo de soluciones de procesos de negocios gestionados para abordar esos riesgos e interdependencias.

Aquí hay una definición más detallada (Tyson, 2007, p.4):

> La convergencia de la seguridad es la integración, de manera formal, colaborativa y estratégica, de los recursos acumulativos de seguridad de la organización con el fin de brindar beneficios a toda la empresa a través de una mayor mitigación del riesgo, aumento de la eficacia y eficiencia operacional, y el ahorro de costos.

La convergencia permite que los dispositivos de seguridad física interactúen a través de una red para beneficio sustancial de la organización. Al mismo tiempo, crean un riesgo adicional para la organización debido a que los dispositivos de seguridad física ahora son accesibles desde cualquier parte en la red. En el antiguo paradigma, las cámaras de video, grabadoras de video, sistemas de detección de intrusiones y cuentas bancarias no eran accesibles a menos que una persona físicamente se acercara a ellos. Actualmente son potencialmente accesibles desde cualquier lugar del mundo.

Un buen resumen de estos asuntos proviene de un testimonio ante el congreso del director de Sandia National Latoratories' Information Operations Center (Varnado, 2005):

> Hoy en día, los sistemas heredados están siendo reemplazados gradualmente por los nuevos sistemas SCADA (supervisión del control y adquisición de datos) que usa Internet como la columna vertebral del control. Este cambio se está implementando para reducir costos y aumentar la eficiencia de la operación. Sin embargo, esta tendencia aumenta sustancialmente la posibilidad de disrupciones debido a (1) el número de personas que tienen acceso al sistema es significativamente mayor, (2) las disrupciones pueden ser causadas por piratas informáticas que no tienen formación en ingeniería de sistemas de control y, (3) el uso de Internet expone los sistemas SCADA a todas las vulnerabilidades inherentes a las redes informáticas conectadas entre sí que están siendo explotadas actualmente por piratas informáticos, el crimen organizado, organizaciones terroristas, y Estado-naciones. Los gusanos, virus, network flooding (inundación de la red), ataques imprevistos a través de routers (enrutadores) comprometidos, spyware (programas espía), ataques internos, extracción de datos por externos que obtienen privilegios internos (phishing), y ataques distribuidos de denegación de servicio son todos habituales. El combate eficaz a estos ataques requiere el aumento de la sensibilización, nuevas tecnologías y mejores respuestas y capacidad de recuperación.

Este paradigma es virtualmente idéntico a la actual situación en el campo de la seguridad física.

La Figura 2-1 muestra un sistema de video vigilancia, en el cual se necesitaría el acceso físico al sistema para comprometerlo. El acceso físico al sistema podría ser evitado con una barrera, un oficial de seguridad u otras medidas.

Figura 2-1
Diseño Video-a-Grabador

La Figura 2-2 muestra un diseño moderno de video vigilancia.

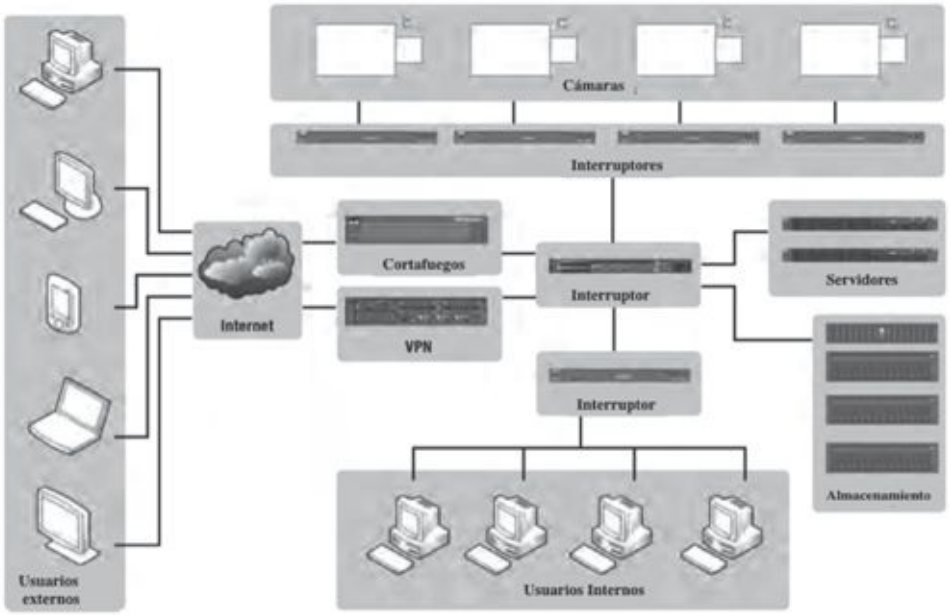


Figura 2-2
Infraestructura de Video

Múltiples computadoras en la red son capaces de acceder a un servidor que ahora almacena datos de video. Las cámaras en la red están poniendo esos datos de video en ese mismo servidor.

La seguridad física puede usar distintos modos de comunicación. En primer lugar, puede haber una conexión propia entre un dispositivo y otro. En segundo lugar, puede haber una conexión estándar de la industria entre dos dispositivos, tales como el protocolo Weigand entre un lector de tarjeta y un controlador. Y en tercer lugar, los dispositivos de la red generalmente conversan a través de TCP/IP (protocolo de control de transmisión/protocolo de Internet), el estándar mundial de Internet para la comunicación.

Los dispositivos pueden ser divididos en dos tipos de sistemas, integrados y basados en host (anfitrión). Los sistemas integrados (también conocidos como sistemas especiales) generalmente son programados por el fabricante y operan en sistemas operativos propios o no estándar. Estos pueden incluir cámaras de video, lector de tarjetas, controladores de acceso, paneles de control de detección de intrusión (alarma), convertidores de video análogo a digital, y así sucesivamente. Los sistemas basados en host operan en sistemas operativos más estándar, generalmente un sistema operativo Windows o Linux (Macintosh OS opera en una versión de UNIX, hermana del sistema operativo Linux). Los sistemas integrados son mucho más difíciles de cambiar que los sistemas operativos Windows, pero todos esos sistemas pueden ser comprometidos.

Dado que cualquier sistema que se comunica con algo más está potencialmente expuesto a un peligro, los profesionales de la seguridad física necesitan tomar decisiones informadas sobre qué sistemas pueden ir dónde. Por ejemplo, Underwriters Laboratories (UL) tiene reglas estrictas sobre cómo se deben implementar los sistemas de incendio, especialmente considerando los problemas de seguridad de la vida que surgen de esos sistemas. ¿Qué pasa si el servidor de un sistema de seguridad física de detección de intrusión fuera tomado e inutilizado por personas empeñadas en acceder al sitio?

La video vigilancia IP proporciona muchas ventajas sobre los anteriores sistemas, pero también es vulnerable. Los profesionales de la seguridad deberían hacerse estas preguntas:

- ¿Qué pasa si alguien tomó una cámara?
- ¿Qué pasa si alguien colocó una secuencia de video grabada anteriormente en lugar de la secuencia original?
- ¿El fabricante del equipo puso en práctica algún control para hacer esto difícil o imposible?
- ¿Qué pasa si los terroristas estuvieran viendo la secuencia de video?
- ¿Qué pasa si los ladrones apagaron el interruptor que trae el video en el sistema?
- ¿Qué pasa si alguien borró la evidencia de video?
- ¿Qué pasa si alguien apagó el video analítico por lo que no se enviaron las alarmas al oficial de seguridad?
- ¿Qué pasa si un ladrón cambió la función del video analítico de modo que repetidamente cause falsas alarmas?

Asimismo, el control de acceso electrónico proporciona muchos beneficios de seguridad, no obstante, también es vulnerable. Los sistemas de control de acceso generalmente contienen tres grandes componentes y hasta dos medios de transporte diferentes. El lector de tarjeta por lo general es la parte que ve el usuario, y presenta una tarjeta para, ya sea un mecanismo de contacto o un método sin contacto, a veces llamado tarjeta “prox” (proximidad). El lector de tarjetas se comunica a través de algún medio, ya sea por cable o inalámbrico, a un controlador que decide si la puerta se debe abrir o algo más debiera suceder (aunque esos dos sistemas pueden estar integrados). Finalmente, el controlador generalmente conversa con un servidor o una aplicación desde la cual obtiene instrucciones sobre qué hacer y qué información de la tarjeta almacenar localmente.

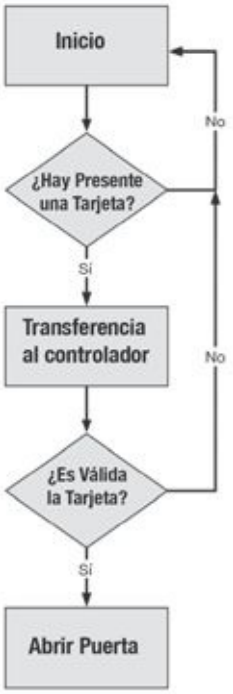


Figura 2-3
Flujo Básico de Tarjeta de Control de Acceso

Los sistemas tradicionales de control de acceso han sido comprometidos en una serie de maneras fuera de la red. En primer lugar, la mayoría de las tarjetas de control de acceso no requiere autenticación mutua antes de dar el número secreto a la tarjeta. Una tarjeta heredada HID (dispositivo de identificación Hughes) tiene dos componentes: el número secreto de la instalación, el cual no está impreso en la tarjeta, pero puede ser conocido por el propietario de la instalación, y un número de identificación que está impreso en la tarjeta. Cuando un lector de tarjetas solicita este número, una combinación del número secreto y el impreso, la tarjeta simplemente lo suministra. Si fuera tan fácil conseguir la llave de la casa de alguien como llegar a caminar en un pie de una persona con un escáner en la mochila o bolso y así obtener la información de la tarjeta, uno estaría muy preocupado. No obstante, muchas compañías aún están utilizando y comprando sistemas basados en esta modalidad.

La segunda gran vulnerabilidad que se aplica a los sistemas de control de acceso que no son accesibles desde Internet o cualquier otra red gira en torno a un protocolo denominado Wiegand. Muchos de los actuales sistemas de control de acceso se basan en este protocolo, desarrollado a fines de la década de los ochenta, el cual utiliza un mecanismo de texto plano para pasar las credenciales entre el lector y el panel de control.

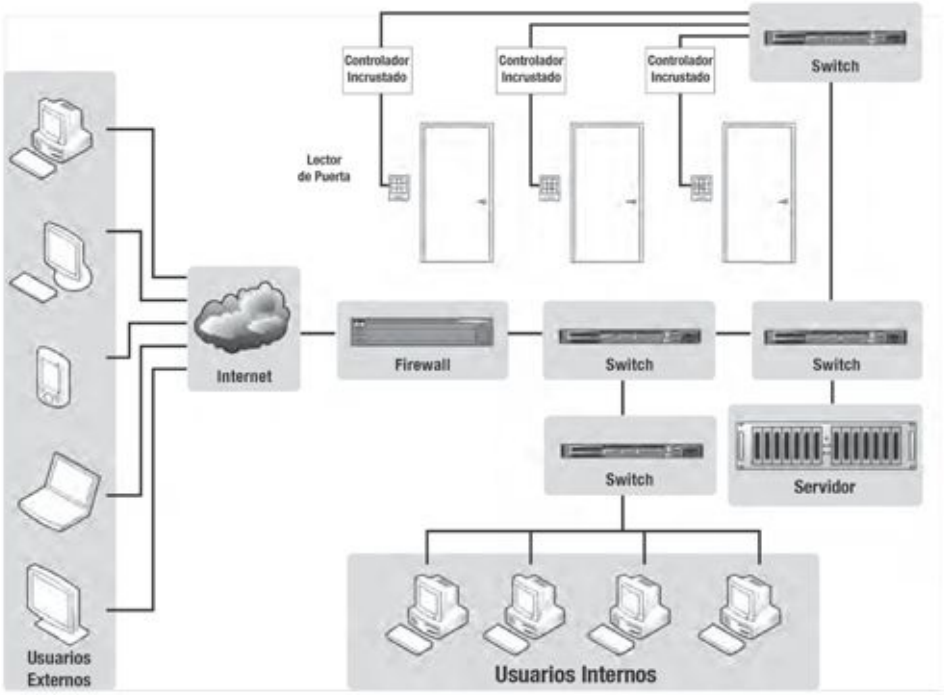


Figura 2-4
Flujo Básico de Wiegand

Desafortunadamente, dado que la información en texto plano no está codificada, cualquiera que puede obtener acceso al cable puede obtener acceso a la información. Una herramienta denominado gecko, la cual puede ser construida por US$ 10 por pieza, puede dar a un intruso un completo control sobre una puerta. Está claro que es importante informarse sobre los posibles riesgos asociados con cualquier dispositivo, incluso si los elementos de seguridad física no convergen con las redes.

En la típica implementación de control de acceso en red, los sistemas de control de acceso operan directamente en la red. Por lo general, la red está hecha de dos piezas: la conexión de sistemas integrados entre un lector y un controlador y luego una red TCP/IP en la cual los controladores conversan con los servidores y los usuarios conversan con los servidores.

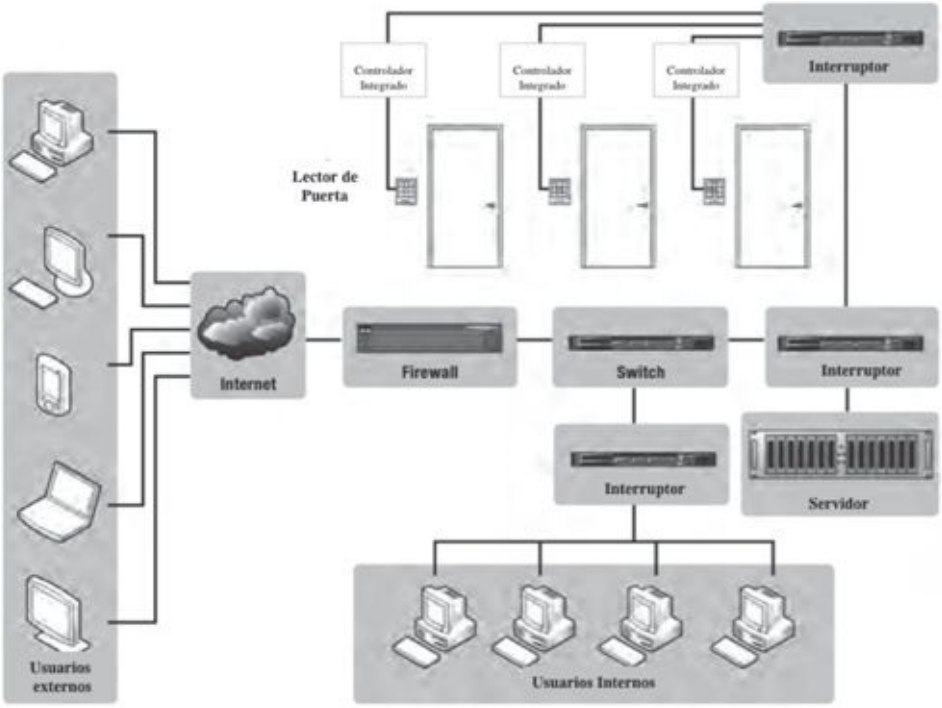


Figura 2-5
Sistema de Control de Acceso de Red

Casi todos los sistemas de control de acceso en uso hoy en día funcionan con una base de datos en una computadora. La base de datos determina cuando alguien puede entrar, cuáles son las reglas para ese acceso, y si una tarjeta está habilitada o deshabilitada. Una persona que puede controlar la computadora puede hacer esos cambios.

Se presentan dos peligros. Primero, un administrador válido podría añadir una tarjeta adicional o backdoor (puerta trasera). Por lo tanto, es esencial emplear metodologías de evaluación de riesgos de seguridad de la información para asegurarse de aplicar adecuadamente las reglas del sistema. Incluso los administradores autorizados no deberían ser capaces de cometer errores fácilmente, y si de todos modos se equivocan, una pista de auditoría debe mostrar los que sucedió.

Segundo, el sistema puede ser accesible a Internet. Un servidor puede ser accesible solamente desde algunas otras máquinas, pero una de esas máquinas podría ser tomada por un individuo malicioso. Si eso sucediera, todo el sistema de control de acceso de una compañía podría estar en manos de una persona desconocida.

Los profesionales de la seguridad deben usar tanto la inteligencia como la imaginación para tomar buenas decisiones cuando implementan sus sistemas. Ningún sistema es impermeable a ser cambiado, detenido o modificado externamente si está conectado a una red TCP/IP o computadora.

2.6 CIBERCRIMEN: UN DESAFÍO NACIONAL

El discurso del Presidente Obama sobre la seguridad de la infraestructura cibernética de la nación ofrece varias observaciones útiles. Los siguientes son extractos de ese discurso; después de cada uno hay un

comentario que aplica las observaciones del presidente a las preocupaciones del profesional de la seguridad (Obama, 2009):

> *Es la gran ironía de nuestra Era de la Información –las tecnologías que nos dan poder para crear y construir, también empoderan a aquellos que interrumpen y destruyen. Y esta paradoja –visible e invisible- es algo que experimentamos todos los días.*

La tecnología permite a los expertos en seguridad gestionar los riesgos de las organizaciones más que nunca antes. Sin embargo, también es necesario entender y aplicar un paradigma de seguridad lógico para proteger eficazmente los activos.

> *Es acerca de la privacidad y la seguridad económica de las familias estadounidenses. Confiamos en Internet para pagar nuestras cuentas, las actividades bancarias, comprar y presentar nuestros impuestos. Pero, hemos tenido que aprender todo un nuevo vocabulario tan sólo para adelantarnos a los cibercriminales que nos harían daño - spyware, malware, spoofings[14], phishing and botnets[15]- Según una encuesta, sólo en los dos últimos años el cibercrimen ha costado a los estadounidenses más de 8 billones.*

El cibercrimen está costando a los ciudadanos y a las empresas una gran cantidad de dinero. Los riesgos son altos.

> *Esta es una materia, también de competitividad económica de Estados Unidos. La pequeña empresa de una mujer en St. Louis, el operador de bonos en la Bolsa de Valores de New York, los trabajadores de una empresa naviera mundial en Memphis, el joven emprendedor en Silicon Valley- todos ellos necesita las redes para hacer la próxima nómina de pago, el próximo negocio, el próximo envío, el próximo gran avance. El E-commerce (comercio electrónico) sólo el año pasado representó alrededor de US$ 132 billones en ventas al por menor (retail).*

El problema afecta no sólo a la propia empresa, sino también a los socios de la empresa.

> *Pero, diariamente vemos olas de robos cibernéticos buscando información sensible –el empleado descontento al interior de la empresa, el pirata informático solitario a miles de kilómetros de distancia, el crimen organizado, el espionaje industrial y, cada día más, los servicios de inteligencia extranjeros. El año pasado, en un acto descarado, ladrones usaron la información de una tarjeta de crédito robada para robar millones de dólares de 130 cajeros automáticos (ATM) en 49 ciudades alrededor del mundo- y lo hicieron en sólo 30 minutos. Un solo empleado de una empresa estadounidense fue declarado culpable del robo de propiedad intelectual supuestamente de US$ 400 millones. Se estima que el año pasado solamente los cibercriminales robaron propiedad intelectual de empresas de todo el mundo por US$ 1 trillón.*

La amenaza proviene de múltiples vectores de amenazas, que los profesionales de la seguridad están en posición de detener.

> *En breve, la prosperidad económica de Estados Unidos en el siglo XXI dependerá de la seguridad cibernética.*

El éxito o fracaso de cada organización puede depender de las acciones de los profesionales de la seguridad.

> *Nuestra ventaja tecnológica es la clave del predominio militar de Estados Unidos. Pero, nuestra defensa y redes militares están bajo constante ataque. Al Qaeda y otros grupos terroristas han hablado de su deseo de lanzar un ataque cibernético en nuestro país –ataques que son difíciles de detectar y difíciles para defenderse. De hecho, en el mundo actual, los actos de terror podrían venir no sólo de unos pocos extremistas con chalecos suicidas, sino de unos pocos golpes de teclas en la computadora- un arma de disrupción masiva…*
>
> *Por todas esta razones, queda claro que esta amenaza cibernética es una de los desafíos económicos y de seguridad nacional más graves que enfrentamos como nación.*

En 1937, Alan Turing creo la Máquina Turing, antecesora de lo que se convertiría finalmente en la

microcomputadora. Su máquina creó un nuevo mundo, un nuevo paradigma en el cual los responsables de la protección de las personas y activos ahora deben comprender. La amenaza es real y los ataques ya están en marcha.

REFERENCIAS

Acohido, B. (2009, August 9). Twitter troubles show fragility of social network. USA Today.

Baker, S. (2009, April 28).Testimony before the U.S. Senate Committee on Homeland Security and Governmental Affairs. Available: http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=98c47739-98ac-43d5-a161-0fa82e2f5243[2010, December 5].

Booz Allen Hamilton. (2005). Convergence of enterprise security organizations. Arlington, VA: Alliance for Enterprise Security Risk Management.

Braun, R., & Stahl, S. (2005). An emerging information security minimum standard of due care. In H. Tipton and M. Krause (Eds.), Information security management handbook (6th ed.). Boca Raton, FL: Auerbach Publications.

Claborn, T. (2009, February 3). Data loss costing companies $6.6 million per breach. Information Week.

Correll, S. (2009, September). Rogueware on an explosive trend. ISSA Journal.

Dunham, K. (2009, August). Mobile malcode threats. ISSA Journal.

FBI. (2009, November 3). Press release: Fraudulent automated clearing house (ACH) transfers connected to malware and work-at-home scams. Available: http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm [2010, December 5].

Gladwell, M. (2008). Outliers: The story of success. New York, NY: Little, Brown and Company.

Gordon, L., & Loeb, M. (2006). Managing cyber-security resources: A cost-benefit analysis. New York, NY: McGraw-Hill.

Harwood, M. (2009, August). Cybercriminals keep malware alive longer. Security Management.

Harwood, M. (2009, June). YouTube account holders target of phishing scam. Security Management.

Herley, C., & Florencio, D. (2009). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. Microsoft research. Available: http://research.microsoft.com/pubs/80034/nobodysellsgoldforthepriceofsilver.pdf [2010, December 5].

IBM Global Technology Services. (2009). IBM Internet Security Systems X-Force 2009 mid-year trend and risk report. Available: http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=68843&ssid=66&sf=1 [2010, December 5].

ISO 27001. (2005). Information technology—security techniques— information security management systems—requirements. Geneva, Switzerland: International Organization for Standardization.

Kellerman, T. (2009, April 28). Testimony before the United States Senate Homeland Security and Government Affairs Committee. Available: http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=fd18b89f-b540-4e9a-9c52-823013751b9b [2010, December 5].

Kim, H. (2009, July 9). Official says seven South Korean websites attacked again. USA Today.

Krebs, B. (2009, September 9). Cyber thieves steal $447,000 from wrecking firm. Washington Post. Available: http://voices.washingtonpost.com/securityfix/2009/09/cyber_theives_steal_447000_fro.html#more [2010, December 5].

Kuhn, T. (1962). The structure of scientific revolutions. Chicago, IL: University of Chicago Press.

Kwon, M. (2009, September 20). Speech to the ISSA gala 25 year anniversary event.

Lam, D., & Stahl, S. (2010, January). Convergence, paradigm shifts and reaching the village. ISSA Journal.

Lemos, R. (2009, September 18). Real-time hackers foil two-factor security. Technology Review (MIT). Available: http://www.technologyreview.com/computing/23488/?a=f.

Mills, E. (2009, August 24). Cisco wireless LANs at risk of attack, 'skyjacking.' CNET News. Available: http://news.cnet.com/8301-27080_3-10316870-245.html [2010, December 5].

National Commission on Terrorist Attacks. (2004). The 9/11 commission report: Final report of the National Commission on Terrorist Attacks upon the United States. New York: W.W. Norton.

Obama, B. (2009, May 29). Remarks by the President on securing our nation's cyber infrastructure. Available: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [2010, December 4].

Privacy Rights Clearinghouse. (2009). Chronology of data breaches. Available: http://www.privacyrights.org/data-breach [2010, December 4].

Richardson, R. (2008). CSI computer crime & security survey. Available: http://www.cse.msstate.edu/~cse6243/readings/CSIsurvey2008.pdf [2010, December 5].

Symantec Corporation. (2008). Symantec internet security threat report: Trends for July-December 2007. Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf [2010, December

5].

Trotta, D. (2009, August 17). Three indicted in largest US identity theft scheme. Reuters. Available: http://www.reuters.com/article/idUSTRE57G4GC20090817 [2010, December 5].

Tyson, D. (2007). Security convergence: Managing enterprise security risk. Burlington, MA: Butterworth-Heinemann.

United States v. Carroll Towing Co., 159 F.2d 169, 173-74 (2d Cir. 1947).

U.S. Attorney's Office, Western District of Washington. (2006, August 25). Press release: California man sentenced for "botnet" attack that impacted millions. Available: http://www.usdoj.gov/usao/waw/press/2006/aug/maxwell.html [2010, December 5].

Varnado, S. (2005, October 18). Statement to U.S. House of Representatives Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cyber Security and the Subcommittee on Emergency Preparedness, Science, and Technology. Available: http://www.sandia.gov/news/resources/testimony/pdf/051018.pdf

Verizon Business RISK Team. (2009). 2009 Data Breach Investigations Report. Available: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

Wagley, J. (2009, August). Preparing for cyber extortion. Security Management. Available: http://www.securitymanagement.com/article/preparing-cyber-extortion-005952 [2010, December 5].

Willson, D. (2009, August). A global problem: Cyberspace threats demand an international approach. ISSA Journal.

CAPÍTULO 3
BASE DE CONOCIMIENTOS DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

El objetivo de un programa de seguridad de los sistemas de información (ISS) de una organización es manejar prudente y rentablemente el riesgo de que la información crítica pudiera

- ser comprometida
- ser cambiada sin autorización, o
- no estar disponible

En otras palabras, el profesional de la seguridad se esfuerza para proteger la confidencialidad, integridad y disponibilidad de la información (a veces llamado CIA[16] en este contexto). El esfuerzo es importante ya que el riesgo de los sistemas de información conduce a otros riesgos, como los siguientes:

- pérdida de dinero a través del robo, fraude y malversación
- costos de recuperación del incidente
- costos por pérdida de la productividad
- pérdida de propiedad intelectual
- abogados y otros gastos legales
- pérdida de valor de la marca

Esta parte de Protección de Activos presenta una visión general del cuerpo de conocimiento de la ISS, incluyendo los riesgos de la ISS y numerosos desafíos técnicos, legales y de gestión de la ISS.

3.1 LOS ELEMENTOS DE RIESGO DE LA ISS

3.1.1 TÉRMINOS DE LA ISS

El lenguaje básico de la ISS puede ya ser familiar para el profesional de seguridad tradicional:

- **Amenaza de los sistemas de información:** cualquier circunstancia, capacidad, acción o acontecimiento con el potencial para impactar adversamente un sistema de información a través del acceso no autorizado, destrucción, divulgación, modificación de datos y/o denegación del servicio.[17]
- **Vulnerabilidad de los sistemas de información:** un defecto o debilidad en el diseño, implementación u operación y gestión de un sistema de información, incluyendo políticas, procedimientos, procesos y controles internos que podrían ser explotados para violar la política de seguridad del sistema.[18]
- **Riesgos de los sistemas de información**: producto del nivel de amenaza y nivel de vulnerabilidad.[19]
- **Contramedidas de los Sistemas de Información:** una acción, dispositivo, procedimiento, técnica u otra medida que reduce una amenaza, una vulnerabilidad o un ataque eliminándolo o evitándolo, mediante la minimización del daño que puede causar o descubriéndolo e informándolo de modo que se pueda tomar una acción correctiva.[20]
- **Riesgo de amenaza residual:** por cada amenaza, el potencial riesgo que queda después de que todas las contramedidas de ISS son aplicadas.[21]
- **Riesgo residual:** el restante potencial riesgo que queda después que todas las contramedidas de ISS son aplicadas para todas las amenazas.[22]

3.1.2 ECUACIÓN FUNDAMENTAL DE ISS

Los conceptos de riesgo antes mencionados conectan en la ecuación fundamental de ISS (Quigley & Stahl, 1987):

$$Riesgo\ Residual = \frac{Amenazas * Vulnerabilidades}{Contramedidas}$$

Esta ecuación pretende ser cualitativa, no cuantitativa. Se dice que el riesgo residual aumenta a medida que aumenta la amenaza y a medida que aumenta la vulnerabilidad. El riesgo residual disminuye en la medida que se apliquen las contramedidas. Si todo lo demás sigue siendo igual (*ceteris paribus*), mientras más vulnerabilidades se tienen, más alto es el riesgo residual. Asimismo, cuanto más cuidadosamente se planifique y administre el sistema de contramedidas, más bajo es el riesgo residual.

3.1.3 AMENAZAS DEL SISTEMA DE INFORMACIÓN

Las amenazas son llevadas a cabo por factores de amenaza. Las primeras dos categorías de factores de amenaza ya son conocidas para los profesionales de la seguridad física. La tercera categoría demuestra la necesidad de un paradigma de seguridad lógica (en contraposición a la física). Las categorías son:

Naturaleza:

- terremotos
- huracanes
- otros desastres naturales

Personas:

- empleados y otras personas con acceso legítimo que desea aprovechar las oportunidades
- cibercriminales y otras personas con legítimo acceso
  - ladrones de banco a través de sistemas informáticos (online)
  - botnet herders (recolectores de botnet)
  - ladrones que se dedican al fraude de tarjetas de crédito y robo de identidad
  - espías corporativos
  - gobiernos extranjeros que participan en la guerra cibernética
  - personas enojadas, hostiles o trastornadas o grupos que participan en el ciberterrorismo

Amenaza Virtual:

- un programa informático o script instalado ilegítimamente en una estación de trabajo, servidor, router u otro dispositivo de sistemas de información y capaz de alguno o todos los siguientes:
  - enviar información desde el dispositivo el cual es instalado para el propietario del programa (su control)
  - recibir instrucciones de mando y control desde su control y ajustar su comportamiento en consecuencia
  - ejecutar comandos en el dispositivo en el cual está instalado

Un factor de amenaza virtual es el equivalente a un fantasma en la red, un fantasma que ni siquiera se sabe que está presente hasta que, actuando en nombre de su verdadero dueño, roba, cambia o destruye la información de una organización o hace mal uso de su sistema.

Las amenazas no existen en el mundo real. Para robar la bóveda real de un banco, uno debe ir al banco. Un criminal no puede decirle a Scotty "Beam me up"[23] y esperar a ser transportado a la bóveda y luego volver a salir con el botín. Por contraste, el equivalente virtual de esto se hace diariamente en el ciberespacio. Más que nada, la capacidad del cibercriminal para "ir virtualmente" es lo que hace tan diferente el paradigma de seguridad lógica del paradigma de seguridad física.

Las amenazas virtuales aprovechan la propia lógica de los sistemas informáticos y de comunicaciones. Esos sistemas son tan complejos que su lógica es inherentemente defectuosa. Estos defectos son la fuente de una serie interminable de vulnerabilidades. Los cibercriminales y otras personas aprovechan estas vulnerabilidad –por lo general con la ayuda involuntaria de los seres humanos- para instalar y ejecutar

sus factores de amenaza virtuales en las plataformas de tecnología.

Antes de usar un factor de amenaza virtual, un cibercriminal u otro delincuente debe acceder a la computadora de destino. Los métodos incluyen acceso físico directo en la computadora (a través de la unidad de USB u otro periférico); pirateando el equipo en forma remota; colocando un malware en la computadora, quizás mientras el usuario está navegando en un sitio Web; y haciendo phishing (suplantar la identidad) y social engineering (ingeniería social)[24].

Algunas amenazas virtuales actuales a partir de la redacción de este documento incluyen estas:

- **marketing spyware** (programa espía para comercialización), recolecta información sobre los sitios Web visitados, envía la información a su propietario y muestra las ventanas emergentes.
- **Keyloggers** (registrador de teclas), graba las pulsaciones del teclado y envía los datos a su propietario
- **Koobface** (anagrama de Facebook), gusano informático que se dirige a las personas que usan sitios de las redes sociales
- **Zeus**, troyano para fraudes bancarios online

3.1.4 VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN

Las amenazas no pueden manifestarse sin una vulnerabilidad de la que aprovecharse. Las vulnerabilidades del ISS se encuadran en cinco grandes categorías:

- **vulnerabilidades de la infraestructura de los sistemas de información**, tales como links (vínculos) a redes sin protección, configuración incorrecta del sistema o estaciones de trabajo sin parches
- **vulnerabilidades de las personas que usan la infraestructura de los sistemas de información (usuarios),** significa que los usuarios permiten que otras personas, a través de la ingeniería social u otros medios, accedan a sus computadoras
- **vulnerabilidades en las personas que mantienen la infraestructura de los sistemas de información (custodios),** incluyendo demasiados permisos, inadecuada supervisión y registro de acciones de inicio de sesión e inadecuada capacitación
- **vulnerabilidades de los ejecutivos y la alta gerencia**, incluyendo la falta de responsabilidad, políticas y procedimientos inadecuados, falta de entrenamiento de conciencia de seguridad, inadecuada administración de terceros y vulnerabilidades físicas
- **vulnerabilidades en los procesos de gestión de los sistemas de información**, incluyendo una incorrecta gestión del control de la infraestructura de los sistemas de información, inadecuada gestión de parches, inadecuado control de cambios, inadecuada protección de redes y dispositivos, inadecuado desarrollo de software y metodologías del administrador de bases de datos e inadecuada planificación de la continuidad de la información

3.1.5 OBJETIVOS DE CONTROL DE LOS SISTEMAS DE INFORMACIÓN

Antes de esbozar la gama de contramedidas disponible para la gestión del riesgo residual de los sistemas de información, es importante especificar los objetivos de control del ISS que esas contramedidas deben cumplir.

Tal como en otras disciplinas de seguridad, no basta decir que uno protege los activos corporativos. Deben cumplirse otros tres objetivos de control: detección, recuperación y cumplimiento. Como se muestra en la Figura 3-1, para cada uno de los cuatro objetivos de control es necesario mantener la confidencialidad, integridad y disponibilidad de los datos de la organización.

	Protege los sistemas de información	Detecta los ataques al sistema, tanto los exitosos y los obstruidos	Recuperación de los ataques	Cumplimiento de leyes, reglamentos, obligaciones contractuales
Confidencialidad	✔	✔	✔	✔
Integridad	✔	✔	✔	✔
Disponibilidad	✔	✔	✔	✔

Figura 3-1
Objetivos Generales y Objetivos de Control del ISS

3.1.6 CONTRAMEDIDAS DE LOS SISTEMAS DE INFORMACIÓN

Como en otras disciplinas de seguridad, las contramedidas de los sistemas de información se pueden dividir en tres grandes clasificaciones:

controles administrativos: gestión, políticas, procedimientos, estándares, directrices, investigación del personal, entrenamiento de conciencia, etc.

controles técnicos: inicio de sesión en redes y contraseñas, cortafuegos, auditoría de inicios de sesión, encriptación, antivirus y filtros de spam (correo electrónico no deseado)

controles físicos: cierre de puertas, cámaras, controles del entorno, guardias, etc.

Además de la clasificación de las contramedidas por tipo, es muy útil clasificar las contramedidas por el lugar en el que están siendo implementadas:

- contramedidas en la infraestructura de los sistemas de información (técnica)

- contramedidas en la gestión de la infraestructura de los sistemas de información (administrativa, técnica, física)
- contramedidas de los ejecutivos y la alta dirección (administrativa, técnica, física)
- contramedidas basadas en la comunidad (administrativa, técnica, física)

Cada una de las anteriores se aborda a continuación.

Contramedidas de la Infraestructura

Las contramedidas de infraestructura son los controles ubicados en la infraestructura del sistema de información para prevenir la explotación de las amenazas. Tales contramedidas incluyen las siguientes:

- **perímetro de seguridad**, incluyendo dispositivos que crean o aseguran un perímetro, tales como los interruptores, cortafuegos, etc.
- **protección del dispositivo de seguridad**, incluyendo protección específica en dispositivos (antivirus, cortafuegos personal, discos duros encriptados, etc.)
- **control de acceso y autenticación**, incluye asegurarse que una persona está autorizada antes de que pueda hacer algo en un dispositivo (identificación de usuario, contraseñas, segundo factor para dispositivos electrónicos, etc.)

Contramedidas en la Gestión de la Infraestructura de los Sistemas de Información

Las contramedidas en esta categoría incluyen las reglas sistémicas para la protección de todo el sistema. Ellas incluyen las siguientes:

- **vulnerabilidad y gestión de parches,** para hacer frente a cualquier vulnerabilidad conocida en el sistema
- **supervisión del sistema y revisión de ingresos**, para saber qué está sucediendo en los sistemas y ser capaz hacer una investigación forense de cualquier cosa que ocurra
- **métricas de seguridad de los sistemas de información**, para garantizar que se puede medir el éxito de los esfuerzos
- **seguridad física de la infraestructura de los sistemas de información**, para asegurarse que las personas no pueden obtener acceso físico a los sistemas
- **capacitación al personal de TI en seguridad de la información**, para asegurarse que aquellos en los que la organización confía sus sistemas estén capacitados apropiadamente.

Contramedidas de los Ejecutivos y la Alta Dirección

Quizás lo más importante en seguridad de la información, así como en seguridad física, es tener el compromiso de la gerencia ejecutiva en el apoyo a las iniciativas de seguridad. Las contramedidas de la gerencia incluye las siguientes:

- un sistema de gestión de ISS explícito con responsabilidad, autoridad y rendición de cuentas

(accountability) otorgada a toda la organización; un liderazgo ejercido desde arriba; y responsabilidades claras para todos los gerentes y empleados

- las políticas y procedimientos de seguridad de la información que incorporan el ISS a través de toda la organización, incluyendo la gerencia ejecutiva
- programas de sensibilización y educación del ISS para todos los usuarios
- incorporación de las materias de seguridad de los sistemas de información en los planes de continuidad del negocio, contingencia y emergencia.
- gestión de la seguridad de la información incorporada en todos los acuerdos para compartir información e implementaciones

Contramedidas Basadas en la Comunidad

En cierto sentido, se necesita una aldea para asegurar una aldea. Las vulnerabilidades generalizadas a través de los sistemas informáticos en todo el mundo los pone a todos en un riesgo cibernético mayor. Autores que escriben en el *ISS Journal* señalan (Lam, Pease, Stahl & Takamine, 2007):

> En el mundo actual, todo el mundo está expuesto al riesgo del cibercrimen. Y, nos corresponderá a todos disminuir el riesgo a niveles aceptables. La seguridad de la información ya no involucra simplemente a aquellos que trabajan profesionalmente en el campo. En el mundo actual, todos debemos participar en la disminución del riesgo. Todo gerente de TI, proveedor de TI, CIO, CTO, CFO, COO, CSO y CEO; cada miembro de la Junta de Directores, cada empleado, ya sea en TI, adquisiciones, auditoría, ventas o recursos humanos debe ser una parte de la solución de la seguridad de la información. Todo usuario de computadora tiene un rol que cumplir en la disminución del riesgo de la información de la comunidad. Nosotros los profesionales de la seguridad no podemos asegurar nuestras organizaciones por nosotros mismos.

Todo el mundo en los negocios (incluyendo los ejecutivos, personal de primera línea, y gerentes de seguridad) y en las organizaciones comunitarias es responsable de la seguridad de la información. Una sola máquina que quede sin parche puede ser la plataforma de lanzamiento de una serie de ataques sobre todas las demás.

3.2 CAYENDO POR LA MADRIGUERA DEL CONEJO: LÓGICA INFORMÁTICA, COMPLEJIDAD DEL SISTEMA Y VULNERABILIDAD INHERENTE

En 1936, un joven matemático británico, Alan Turing, publicó un documento que puede ser considerado el comienzo de la era informática moderna. En él exploró matemáticamente lo que significa que un número sea computable, es decir, para que sus sucesivos decimales sean calculables por medios finitos. El resultado fue que el marco matemático que él creó hoy es conocido como la Máquina Turing, una máquina para calcular los decimales de los números. Matemáticamente, una computadora no es nada más que una Máquina de Turing finita, un dispositivo increíblemente sofisticado para desarrollar lo que esencialmente son operaciones lógicas muy simples.

Todos los niños en la escuela, por ejemplo, aprenden a calcular los decimales de fracciones simples

como ½, ¾, 7/8, etc., En la medida que se avanza en la escuela, uno aprende algoritmos para calcular decimales de raíces cuadradas y la expansión decimal de números como Pi.

Lo que Turing hizo en su monumental documento de 1936 fue investigar explícitamente el carácter matemático deL aparentemente simple concepto de contabilizar. Haciendo eso, él descubrió que el concepto no era nada de simple; en 75 años transcurridos desde su documento, la teoría de la computabilidad ha llegado a ser una parte rica y profunda de las matemáticas, quedando en el corazón de los fundamentos lógicos de las matemáticas.

Tres años después de la publicación de su documento y con el estallido de la II Guerra Mundial, Turing empezó a aplicar sus matemáticas al desafío de descifrar las señales alemanas. De esta manera, él y sus colegas diseñaron y construyeron la primera computadora moderna del mundo. Irónicamente, esta primera computadora puede ser pensada como una herramienta de pirateo informático usada para descifrar la información alemana altamente sensible y confidencial!

Central para el trabajo de Turing –y para la comprensión de los desafíos de seguridad de los sistemas informáticos modernos- es el concepto de un algoritmo. Un algoritmo es un método preciso para resolver un problema utilizando una secuencia finita de instrucciones precisas.

Los programas computacionales son extremadamente grandes, algoritmos extremadamente complejos. Debido a su tamaño y complejidad, los programas computacionales contienen errores o fallas (bugs). Estos errores a veces son el resultado de no ser lo suficientemente preciso en la definición del problema a resolver, las instrucciones a seguir, o el orden en el cual se procesan las instrucciones. Estos errores pueden ocasionar vulnerabilidades para la seguridad de la información. Para comprender el paradigma de la seguridad lógica y lo que significa para la seguridad de los sistemas de información, es importante entender algunos de los desafíos de escribir buenos algoritmos, es decir, software que contiene relativamente pocos (y relativamente poco dañinos) errores.

3.2.1 CÓMO FUNCIONAN LOS SISTEMAS INFORMÁTICOS

Las primeras computadoras digitales construidas durante la II Guerra Mundial por Turing y otras personas, fueron diseñadas para hacer una cosa, ejecutar un programa. En los años 70 o más o menos a partir de entonces, las computadoras han evolucionado en tamaño, velocidad y complejidad. En 1968, cuando Intel fue fundada por Robert Noyce y Gordon Moore, en realidad nadie tenía idea de lo que estaba por venir. En la medida que Intel creció, Moore desarrolló la hipótesis, ahora conocida como la Ley de Moore, de que el poder de procesamiento en cualquier línea de computadoras se duplicaría cada 18 meses. Para algunos investigadores en la frontera entre la antropología y la ciencia informática, la Ley de Moore caracteriza el crecimiento exponencial de las tecnologías humanas que se remonta a más de 100.000 años.[25]

¿Por qué esto es relevante para el profesional de la seguridad física? El poder de procesamiento de un Smartphone BlackBerry o iPhone de Apple es mayor que el de la primera computadora lanzada por IBM

en 1981. Una consecuencia del trabajo de Turing es que una mayor complejidad, permitida por más poder de procesamiento, conduce a una mayor posibilidad de error. No sólo eso, sino que estos dispositivos están conectados entre sí de maneras ni siquiera imaginables cuando Intel fue fundada.

En la medida en que las computadoras son usadas en nuevas e innovadoras maneras, y se vuelven más interconectadas, se han vuelto más vulnerables. Los sistemas de seguridad física que hoy se ejecutan como parte de tecnologías de convergencia en redes de TI alrededor del mundo ilustran esto perfectamente. Lo que anteriormente se entendía como un activo físico, ahora presenta un nuevo tipo de riesgo porque es un activo virtual. Debido a que es campo del profesional de la seguridad física proteger esos sistemas, ya sean cámaras o alarmas, y si existen físicamente, virtualmente, o ambas, ahora es necesario que el profesional de la seguridad física comprenda cómo se interrelacionan estos dispositivos y cuáles son los riesgos adicionales que podrían representar para la organización.

Como en otros lugares del mundo virtual, existe una pequeña pero vital sutileza aquí: un programa puede hacer lo que está programado que haga y aún tener vulnerabilidades. La razón es que la seguridad está especificada inadecuadamente. Por ejemplo, una especificación de seguridad puede decir que la interfaz del usuario a una base de datos back-end [26] sensible requiere un nombre de usuario y una contraseña. El sistema de base de datos es construido de acuerdo con esta especificación, pero permite que cualquier persona con un acceso directo a la base de datos back-end lea los datos. Lo que la especificación debiera haber dicho es que no se permite el acceso a los datos sin que el usuario sea autenticado en el momento del acceso. Ahora el fondo ya no puede asumir que el usuario ya ha sido autenticado en el front-end.

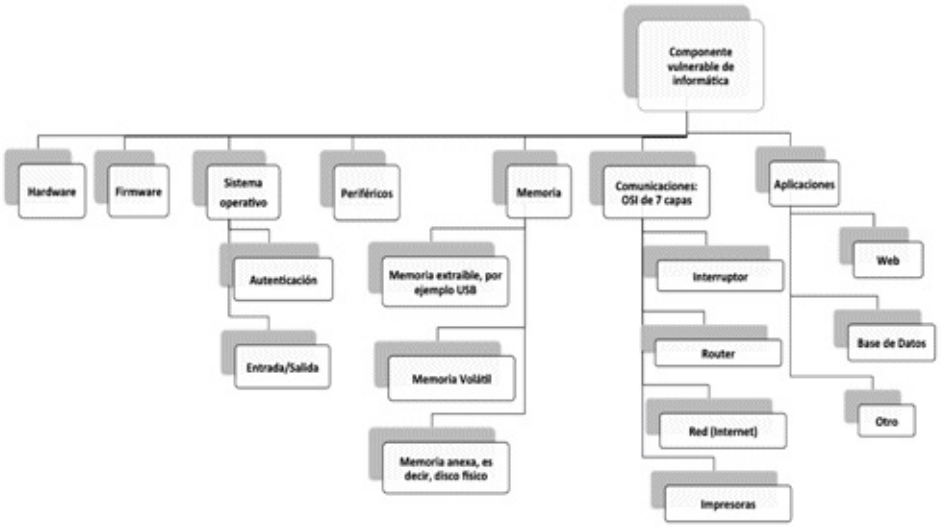


Figura 3-2
Componentes Básicos de una Operación Computacional

La Figura 3-2 muestra los aspectos básicos del funcionamiento de una computadora. Al comenzar el proceso de encendido del equipo, las instrucciones básicas de cómo se pone en marcha están almacenadas en su hardware. Tiene una serie de instrucciones sobre qué hacer cuando se enciende por primera vez. Este proceso se conoce como booting up (arranque o inicio), que es una referencia al concepto de una computadora que se levanta mediante su propio esfuerzo.

A continuación la computadora empieza a leer las instrucciones sobre qué hacer. Las instrucciones pueden estar almacenadas en distintos lugares, pero en pro de la discusión, el área de almacenamiento de las instrucciones puede ser llamada firmware. El firmware permite que las instrucciones de la computadora sean actualizadas periódicamente.

Después de leer esas instrucciones, la computadora pasa al sistema operativo. El sistema operativo, como Microsoft Windows, Linux o Mac OS, contiene millones de líneas de instrucciones necesarias para hacer funcionar una computadora moderna. Entre otras cosas, un sistema operativo se ocupa del input (entrada) y output (salida). Eso significa que un usuario u otro agente puede ingresar instrucciones y recibir a cambio un resultado. Además, los sistemas operativos por lo general son responsables de la autenticación del usuario –el proceso de verificación (autenticación) de que la persona accediendo al dispositivo es quién dice ser.

El siguiente nivel de la arquitectura de un sistema informático tiene relación con los periféricos, elementos dentro de la computadora o conectados a ella. Un ejemplo es el disco duro. Generalmente, el sistema operativo se carga en el disco duro y esas instrucciones son cargadas por la computadora cuando se enciende. Otro periférico es un lector de CD-ROM. Durante la secuencia de inicio, una computadora puede tomar instrucciones del CD-ROM y actuar sobre él. En una serie de situaciones de piratería informática, los hackers (piratas informáticos) colocaron en los lugares del almuerzo CD-ROM especialmente diseñados con títulos tentadores como “datos de nómina de pago”. Un usuario al poner el CD-ROM en su computadora ha comprometido su PC, ya que el CD-ROM ejecuta su programa de inicio.

Es importante señalar que una computadora funciona en dos modos principales: como un dispositivo de computación independiente (stand-alone) y como un dispositivo que puede comunicarse con otras computadoras. Una computadora opera como dispositivo independiente almacenando y manipulando información en su memoria. La memoria puede contener información que sólo está disponible cuando la computadora está encendida (memoria volátil) o información que está disponible sin energía aplicada al sistema (memoria estática).

Los cambios de los datos y las manipulaciones se llaman cálculos, lo cual ocurre en el procesador de la computadora. En el modo stand-alone, una computadora sigue un conjunto de instrucciones para manipular los datos, generalmente a través de la entrada en un teclado, desde la memoria, o desde un periférico. Luego, la computadora actúa sobre los datos, desarrollando un cálculo básico o escribiendo datos en la memoria. Este es el modelo básico de Turing de un algoritmo.

Una PC original de IBM en 1981 no necesariamente habría sido conectada a otra computadora. Por lo que uno tendría dificultad para añadir o eliminar algo de la computadora sin acceder a ella físicamente. En esa era, la seguridad de las PC era más fácil que hoy. A medida que avanzaron los ochenta, las computadoras empezaron a hablar entre ellas. No obstante, incluso entonces, la mayor parte del trabajo de la ISS consistía en asegurar los mainframes (macro-computadora o computadora central) al interior de los centros de datos.

Con respecto a las comunicaciones informáticas, las computadoras en Internet se comunican a través de

un protocolo llamado Protocolo de Internet (IP de ahora en adelante, por sus siglas en inglés) el cual también se conoce como TCP/IP (Protocolo de Control de Transporte/Protocolo de Internet). Casi todas las comunicaciones modernas vía computadora siguen un modelo llamado Interconexión de Sistemas Abiertos (OSI) Modelo de Red de Siete Capas, desarrollado por la International Organization for Standardization. El modelo (Reed, 2003)

> Describe siete capas de interacción para un sistema de información que se comunica a través de una red, presentando una pila de capas que representan la principales áreas de funciones que generalmente son necesarias o útiles para la comunicación de datos entre nodos en un entorno distribuido.

Las siete capas del modelo OSI son las siguientes:

Generalmente, la lista se lee de abajo hacia arriba.

Capa 1

En la capa física, las computadoras se comunican, ya sea enviando impulsos eléctricos, o no. Este nivel define el voltaje real y las interfaces que una computadora utiliza para comunicarse.

Capa 2

En el nivel de enlace de datos, las computadoras realmente se están comunicando lógicamente. En la comunicación de la capa 2, las computadoras sólo pueden hablar entre sí cuando pueden conectarse directamente entre ellas. Para que una máquina converse con otra, las dos deben estar conectadas. En la forma más simple, esto puede ocurrir cuando dos máquinas están conectadas con un cable. En una red moderna, los cables van desde una computadora a una ubicación centralizada, generalmente conocida como una instalación de distribución intermedia (IDF por sus siglas en inglés). En cada una de estas instalaciones, por lo general hay un switch (interruptor). El switch es análogo a un conmutador de teléfono, en el cual múltiples teléfonos se conectan y por el cual un teléfono puede conversar con otro. En términos simples, cada computadora directamente conectada a un switch puede hablar con cualquier otra computadora directamente conectada al mismo switch. En esta capa, las comunicaciones ocurren

automáticamente sin una configuración adicional.

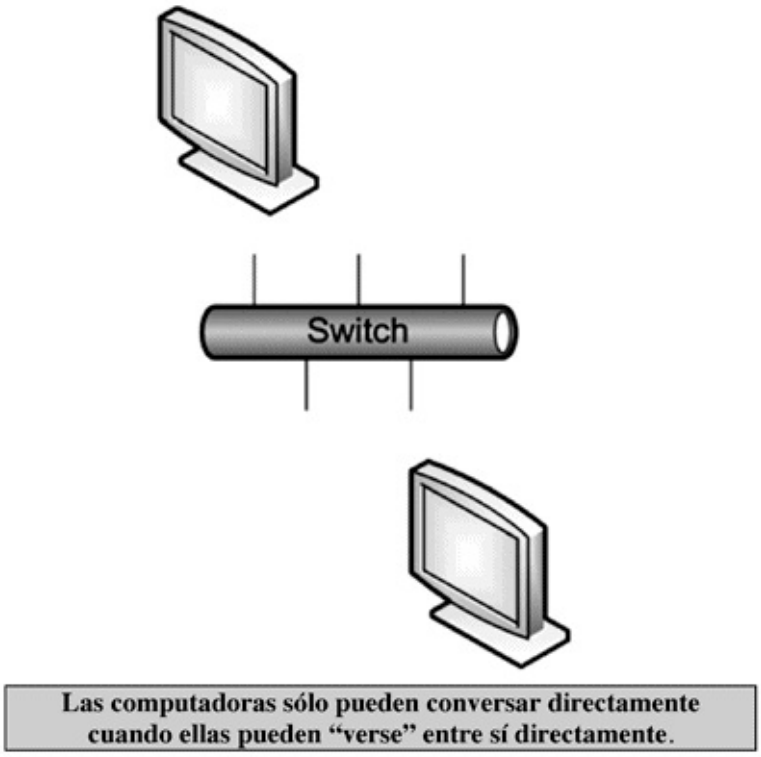


Figura 3-3
Comunicación Directa

Una persona en una habitación con varias otras personas, por lo general, puede conversar directamente con esas personas. Es fácil hablar alrededor de una mesa en una sala de reuniones, porque uno puede ver a las otras personas en la habitación. Esto se parece a las computadoras conectadas el mismo switch o un conjunto de switches. Una computadora es capaz de conversar con otra computadora simplemente diciendo su nombre.

Los switches proporcionan un poco de privacidad, análogos a una conversación susurrada entre dos personas que se sienta una al lado de la otra en una mesa de reuniones. Aunque una conversación susurrada se supone que es privada, existe una gran cantidad de maneras de escucharla. Una podría pararse cerca de las personas que están conversando o usar un micrófono especial. Del mismo modo, en el mundo virtual, los hackers pueden meterse en medio de una conversación de la que se supone ellos no son parte. Ciertamente, esto aplica a la comunicación a través de un switch local. Un switch no sólo es un dispositivo de back-end que conecta computadoras, sino también es un host (anfitrión) que se puede configurar. Ejecuta programas, lo que significa que puede ser comprometido (por ejemplo, si un cibercriminal obtiene acceso a la configuración del programa).

Capa 3

En la capa de red, las computadoras son capaces de verse unas a otras directamente. Esto también es conocido como la comunicación de capa 3. Esta capa fue creada de modo que las máquinas que no pudieran verse inmediatamente entre ellas puedan seguir comunicándose.

Para que esto ocurra, es necesario tener un intermediario que permita la comunicación a través de muchos

intermediarios en el proceso. En el mundo físico, las oficinas de correos y las compañías de teléfonos saben cómo entregar información de un lugar a otro basado en algún tipo de código de enrutamiento. El dispositivo informático que permite que esto suceda se llama router (enrutador). Un router sabe cómo llegar de un lado a otro de modo que las computadoras puedan conversar entre sí. Los routers también conversan entre sí, de modo que cada router en un camino crítico sepa como llegar a otro router en otro lugar.

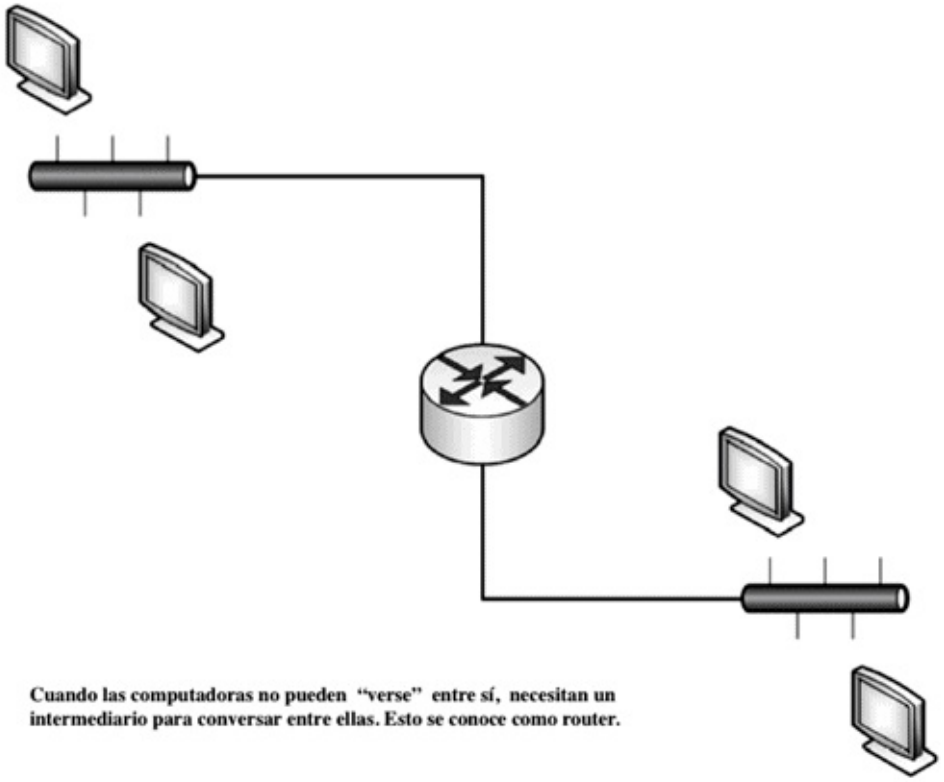


Figura 3-4
Comunicaciones mediante Router

Capas Restantes

Las otras cuatro capas del modelo OSI también son importantes para la comprensión de la forma en que las computadoras interactúan. Por ejemplo, la cuarta capa, la de transporte, determina el mecanismo de cómo las computadoras van a transportar la información entre dos computadoras ahora que ellas pueden conversar. Las últimas tres capas –sesión, presentación y aplicación- dirigen cómo las computadoras organizan los datos en flujos, estandarizan los datos y realizan funciones que no pertenecen directamente al funcionamiento de la red.

También son importantes las aplicaciones que se ejecutan en una computadora que realizan tareas específicas. Estas pueden ser cosas como servidores de Web que permiten a los usuarios obtener acceso a los datos, las bases de datos que realmente mantienen los datos o algo tan simple como Microsoft Word. Estas aplicaciones pueden acceder a los datos, y es importante pensar acerca de cómo ellas podrían ser mal usadas.

Desafíos del Ingreso de Datos (Input)

Hay varios mecanismos por los cuales alguien pueden acceder o manipular información en una

computadora.

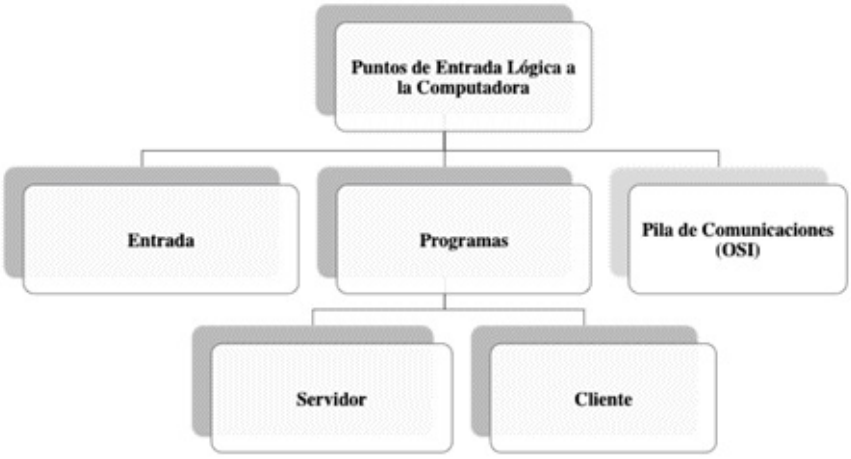


Figura 3-5
Puntos de Entrada Lógica a la Computadora

Una computadora normalmente tiene tres puntos de entrada lógica para conseguir hacer algo: entrada, programas y gran cantidad de comunicaciones. La entrada es el medio más fácil para hacer llegar información a una computadora –se escribe en un teclado o se usa otro dispositivo de entrada. Los programas, también, son capaces de pedirle a la computadora que haga algo. La parte peligrosa es la gran cantidad de comunicaciones, a través de la cual una computadora puede enviar entradas o pedirle a un programa que haga algo desde cualquier parte del mundo.

Las entradas vienen en muchas formas. Puede consistir en escribir texto en un procesador de texto desde el teclado; podría ser un usuario ingresando su nombre de usuario y contraseña; o podría ser el programa de la computadora controlando la entrada/salida del sistema enviando un registro de acceso al programa de la computadora evitando que los usuarios que no se encuentra en el edificio de acceso a un servidor que contiene información sensible.

Un modo de ataque mediante la entrada es para ingresar un texto inusual en un campo de inicio de sesión en una página Web, por ejemplo “o 1=1-”. Si la computadora no está preparada para enfrentar adecuadamente esta entrada, la computadora podría devolver información que el usuario no debería ver.

Otra categoría de ataque se llama desbordamiento de búfer (buffer overflow). En esta instancia, un usuario malintencionado o un programa puede dar más información al programa de la computadora que lo que está esperando. Las palabras o caracteres extras pueden producir un estado de desbordamiento de búfer, dando instrucciones a la computadora para que haga algo no planeado.

Los errores lógicos pueden tener similares consecuencias. Si el programador no escribe el código correctamente, un usuario mal intencionado realmente pude conseguir que haga algo. Además, si la computadora asume que algo sucederá en una secuencia determinada, pero la secuencia es interrumpida debido a que un programa o la red está lenta, entonces algo puede burlar la computadora y provocar un evento malicioso.

Hosts: Es una Parte

Una computadora host almacena información y permite manipularla o comunicarse con otra computadora. Un host necesita un mecanismo para aceptar un comando de un usuario y la manipulación de la información dentro de ella. Esto generalmente se conoce como la plataforma de la computadora. En la mayoría de los casos, la plataforma es una de un limitado número de sistemas operativos.

En cada una de estas plataformas, pueden ejecutarse uno o más programas de aplicaciones. Una aplicación podría ser Microsoft Word. Otra podría ser un navegador de Internet como Safari o Internet Explorer. Estas aplicaciones contienen millones de líneas de instrucciones. Aunque cada instrucción por lo general es muy simple, la complejidad lógica asociada a cómo interactúan estas instrucciones se convierte en un caldo de cultivo para los errores.[27]

Cualquier sistema que es una computadora host tiene un peligro potencial de un modo u otro, incluyendo los siguientes sistemas:

- **Servidores**. Esto por lo general son máquinas que sirven a más de una persona en su aplicación específica. En algunos casos, cuando la gente se refiere a un host, se están refiriendo a un servidor, aunque técnicamente esto no es correcto. Los servidores son de mayor preocupación debido a que suelen servir a más de una persona y como resultado, generalmente son un repositorio de datos o algún mecanismo de acceso a los datos.
- **Estaciones/Puestos de trabajo**. Estos generalmente son máquinas que ejecutan un sistema operativo estándar y en el cual los usuarios ejecutan múltiples programas. Estas clases de máquinas incluyen a las computadoras de escritorio y las computadoras con dispositivos de CPU aparte. Lo más notable, es que estas máquinas no son portables. *Estación/Puesto de trabajo* también puede significar una computadora de escritorio high-end (gama alta), pero aquí el término se refiere a una computadora que no se puede mover fácilmente.
- **Computadora Portátil**. Estas generalmente son idénticas en función a las estaciones de trabajo, pero son portables. Ellas pueden tener más problemas simplemente porque se pueden mover.

Los asistentes personales digitales (PDA por sus siglas en inglés), como un iPod Touch, pueden contener tanta información como una computadora de los noventa. Los teléfonos inteligentes, como el iPhone o la BlackBerry, también son computadoras potentes. Otros dispositivos, tales como las unidades USB o flash, pueden carecer de inteligencia pero aún así llevan datos de un lugar a otro. Los reproductores MP3 y las cámaras digitales también pueden transferir una inmensa cantidad de datos.

Cualquier cosa conectada o que se pueda conectar a una red está en riesgo. Eso ahora incluye teléfonos, cámaras e impresoras.

Ya que cualquier dispositivo que pueda comunicarse con otra computadora y tenga memoria se conoce como un host, un host también podría ser una impresora, la que por lo general tiene un servidor Web como parte de su sistema operativo.

Normalmente, cuando un usuario inicia sesión en un host, necesita ser identificado y autorizado para tener acceso. Esto es lo mismo que ir a un oficial de seguridad y mostrarle la identificación. El oficial revisa la identificación y la cara de la persona para determinar que es quién dice ser. Una computadora generalmente identifica una persona solicitando su nombre de usuario y contraseña.

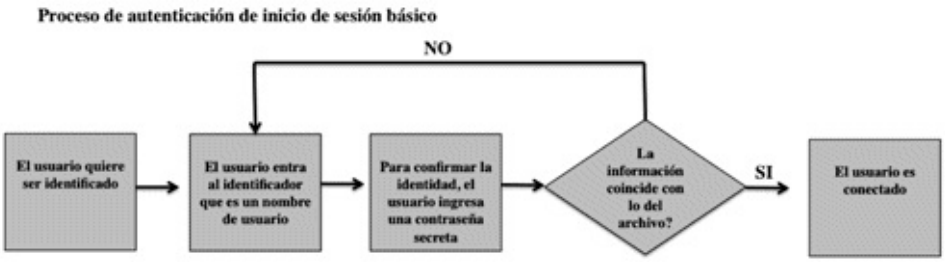


Figura 3-6
Autenticación

Después de la identificación del usuario, la computadora revisa una base de datos para ver qué tipo de autorización tiene ese usuario en particular. Las cosas que un usuario tiene permitido hacer se llaman derechos, permisos y privilegios.

Este proceso de autenticación y autorización es parte de lo que se conoce como la tríada AAA[28]. La tercera parte de esta tríada es la auditoría/responsabilidad, la cual es una parte esencial de asegurar de que lo que se supone que debería estar sucediendo, realmente está sucediendo.

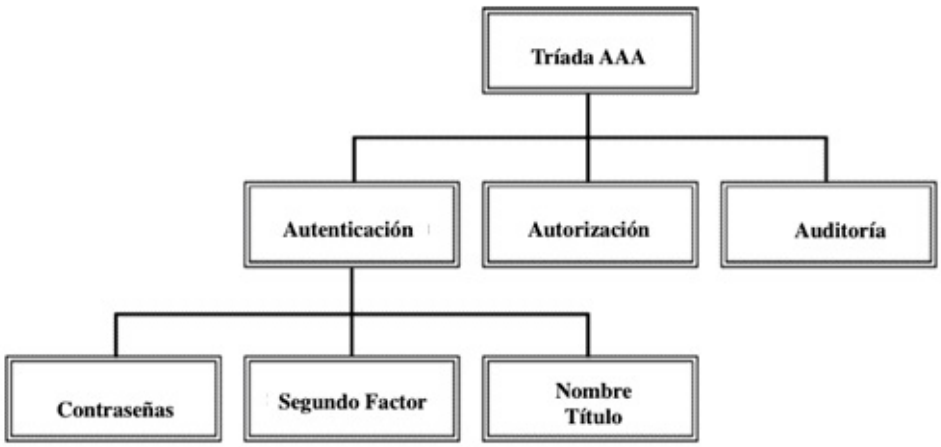


Figura 3-7
Tríada AAA

Entre los muchos programas que operan simultáneamente en una computadora están los programas que simplemente mantienen la computadora funcionando. Llamados servicios, estos programas se ejecutan como usuarios privilegiados, capaces de hacer muchas cosas en la computadora. Esto crea un problema si alguien puede obtener esos servicios para hacer algo no deseado.

El concepto de la tríada CIA (por sus siglas en inglés; confidencialidad, integridad y disponibilidad) aclara los tipos de temas relevantes en la seguridad de la información. La Figura 3-8 amplía la tríada CIA.

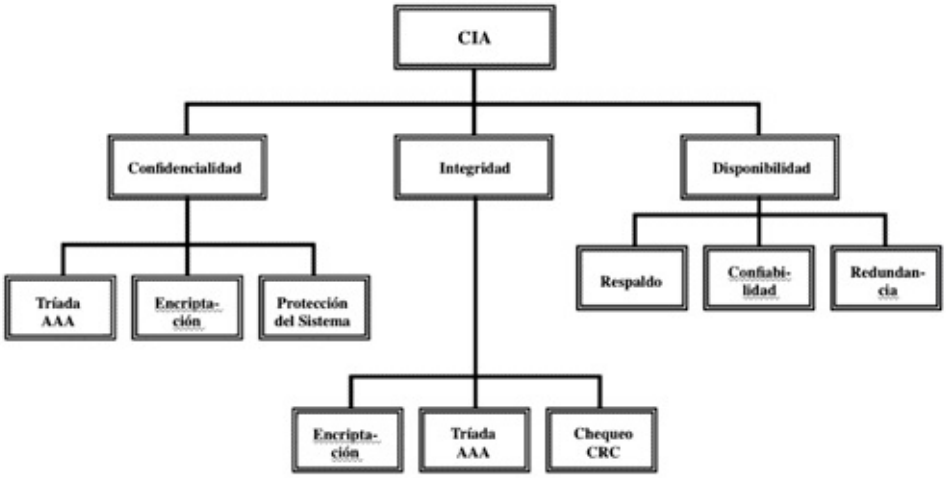


Figura 3-8
Tríada CIA ampliada

Confidencialidad

La autenticación del usuario es fundamental para asegurarse que las personas no consigan datos a los cuales no tienen derecho a acceder. Un mecanismo para aumentar la seguridad es usar un factor de autenticación adicional más allá del nombre de usuario y contraseña.

Las contraseñas pueden ser descubiertas, pero otros mecanismos de autenticación son mucho más difíciles de descubrir o copiar. Un ejemplo es la autenticación biométrica, como los escáneres de huellas digitales, escáneres de la geometría de la mano o escáner del iris. Otro mecanismo para un segundo factor de autenticación es el token (señal) de contraseña de un solo uso (OTP por sus siglas en inglés) que cambia cuando una persona presiona un botón en un dispositivo o después de un período de tiempo, generalmente cada un minuto más o menos.

Otro mecanismo para garantizar la confidencialidad es la encriptación. A menos que una persona sepa cómo descifrar los datos, no puede llegar a ellos. La encriptación tiene muchas formas y ha sido usada por miles de años. Uno de los primeros métodos conocidos de encriptación se denomina cifrado César, en el cual las personas usan una cuadrícula en cada extremo del método de encriptación permitiéndoles mover una letra un determinado número de posiciones más adelante del mensaje real. Por ejemplo, cada instancia de la letra A podría ser reemplazada con la letra M. Las tecnologías modernas de encriptación son mucho más sofisticadas que esta. No obstante, a lo largo del tiempo los mecanismos de encriptación son descifrados y es necesario aumentar la intensidad de la encriptación en forma repetida.

Integridad

La encriptación también puede ayudar a la integridad, debido a que es muy difícil de modificar algo que uno no puede leer. Otra herramienta para mantener la integridad es la comprobación de la redundancia cíclica (CRC por sus siglas en inglés), la cual muestra si los datos han sido manipulados.

Quizás los archivos más importantes cuya integridad debe ser conservada son los archivos que contienen los nombres de usuarios y contraseñas, y los roles permitidos (derechos, permisos y privilegios) para todos los usuarios. Una organización quedaría a merced de cualquier cibercriminal capaz de cambiar

tales archivos.

Disponibilidad

Si los usuarios no pueden obtener sus datos, no es de mucha utilidad. Un viejo chiste de TI dice que hay dos tipos de usuarios de computadoras: aquellos que sus discos duros han fallado y aquellos cuyos discos duros fallarán. Si la información desaparece, no está disponible. También puede desaparecer al ser robada. Un principio básico en informática es respaldar la información fuera del sitio, de preferencia en una bóveda adecuada de almacenamiento de información. De lo contrario, si una computadora falla, la oficina se incendia u otra tragedia, podrían dejar a la organización sin información.

La confiabilidad es una preocupación relacionada. Si un servicio adquirido no es altamente confiable, los usuarios podrían no ser capaces de acceder al servicio cuando lo necesitan. Si una determinada conexión a Internet se cae todo el tiempo, los trabajadores no podrán hacer sus trabajos.

La redundancia ayuda al esfuerzo de asegurar la disponibilidad de los datos. Las computadoras, meras máquinas, sí se rompen. Cuando se diseña un sistema de información, es importante incluir sistemas redundantes para garantizar la continuidad. Por ejemplo, si un servidor de grabador de video se cae, debe estar disponible otro servidor de grabación de video. La redundancia también requiere tener una batería de respaldo y un generador de energía en el evento que no haya suministro eléctrico. Dependiendo de la criticidad del sistema informático, uno puede necesitar sólo la suficiente energía para apagar el sistema o suficiente para mantener el sistema funcionando. Esta última situación puede requerir un generador.

3.2.2 GESTIÓN DE LA INFRAESTRUCTURA DE TI

Después de comprender los principios básicos de cómo funcionan y se comunican las computadoras, es importante comprender cómo se gestionan. Los profesionales de la seguridad son responsables de los activos de las empresas, incluyendo los activos entrelazados con la red informática. Por lo tanto, ellos deben asegurarse que TI está sirviendo a las necesidades de la organización.

Uno de los mecanismos que los profesionales de TI utilizan para la gestión de su trabajo es la Biblioteca de Infraestructura de Tecnologías de Información (ITIL por sus siglas en inglés). Este es un marco desarrollado por la British Office of Government Commerce en la década de los ochenta. Ha sido adoptada como un estándar internacional para la gestión de TI. El estándar aborda el concepto de un acuerdo de nivel de servicio (SLA por sus siglas en inglés). Esta es la forma que se negocia con los profesionales de TI para los servicios que una organización requiere haber entregado.

Todo lo que una organización desea, desde servicios regulares a servicios de emergencia, debe ser codificado de esta forma. De lo contrario, cuando algo no está funcionando, los profesionales de TI puede que no sean capaces de cumplir las necesidades de la organización. Por ejemplo, si una organización no especifica la cantidad apropiada de ancho de banda necesaria tanto para situaciones normales como de emergencia, el departamento de TI no puede crear la configuración adecuada en sus equipos para que cumplan esas necesidades. En una situación en que participa un francotirador activo,

cinco personas podrían necesitar acceso al servidor de video al mismo tiempo. Si esta necesidad no ha sido abordada por adelantado, los recursos necesarios podrían no estar disponibles cuando llegue el momento.

Los requerimientos de las instalaciones también son importantes desde la perspectiva del profesional de TI. Los profesionales de TI requieren seguridad física así como controles ambientales adecuados para asegurarse de que sus sistemas trabajan apropiadamente. La humedad, las vibraciones y el aire acondicionado son consideraciones importantes para el profesional de TI. Además, los profesionales de seguridad física deberían consultar con los profesionales de TI para asegurarse que existen sistemas adecuados de detección de intrusión, control de acceso y video vigilancia para proteger el espacio físico alrededor de la infraestructura basada en computadoras.

Esta preocupación incluye cada lugar en el cual los usuarios puedan conectarse a la red o tener acceso a los servidores. Si una persona obtiene acceso físicamente a una computadora o servidor, generalmente puede obtener acceso a los datos que hay en ellos. Los profesionales de seguridad física deben asumir que si alguien puede obtener acceso al switch físico, está cerca de obtener otros recursos de la red. Todas estas áreas deben ser aseguradas en forma apropiada.

3.2.3 SISTEMAS INFORMÁTICOS DEL MUNDO REAL

El tipo más común de conexión de red es Internet, y desde un punto de vista lógico, es lo mismo si uno se conecta a Internet desde su casa o una empresa. Una vez que el tráfico entra en Internet abierta, es imposible saber quién, si es que hay alguien, está protegiendo los datos.

Las empresas han abordado esto de múltiples maneras. En algunos casos, las empresas pagan proveedores de telecomunicaciones para redes privadas en las cuales sólo sus datos viajan. Muchos niveles de privacidad están disponibles, pero sigue habiendo riesgos.

Uno no debería confiar en los sistemas que no están bajo nuestro control, por lo que es prudente colocar un dispositivo entre Internet y los sistemas que uno necesita proteger: un firewall (cortafuego). Los firewall para las computadoras son como los firewall en los automóviles. La intención es mantener el fuego lejos de los ocupantes del compartimento para pasajeros del automóvil en el evento que el motor se incendie. Sin embargo, los incendios incluso pueden a veces abrirse camino a través de un firewall.

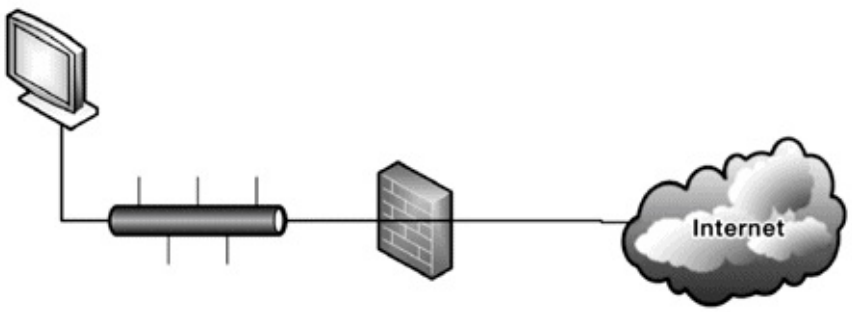


Figura 3-9
Firewall

Los firewall para computadoras permiten que sólo cierto tráfico fluya desde una red no confiable, como la de Internet, a una red interna (donde normalmente se almacenan los datos). Ellos debieran ser considerados sólo una herramientas del arsenal de defensa en profundidad.

Si una empresa está verdaderamente preocupada de la seguridad de su información, en Internet abierta o dentro de una red más privada, puede usar una tecnología denominada red privada virtual (VPN por sus siglas en inglés), la cual cifra los datos desde un punto a otro. Para que los datos sean comprometidos, asumiendo el uso de un algoritmo de encriptación adecuado, alguien tiene que conocer los secretos usados para encriptar los datos.

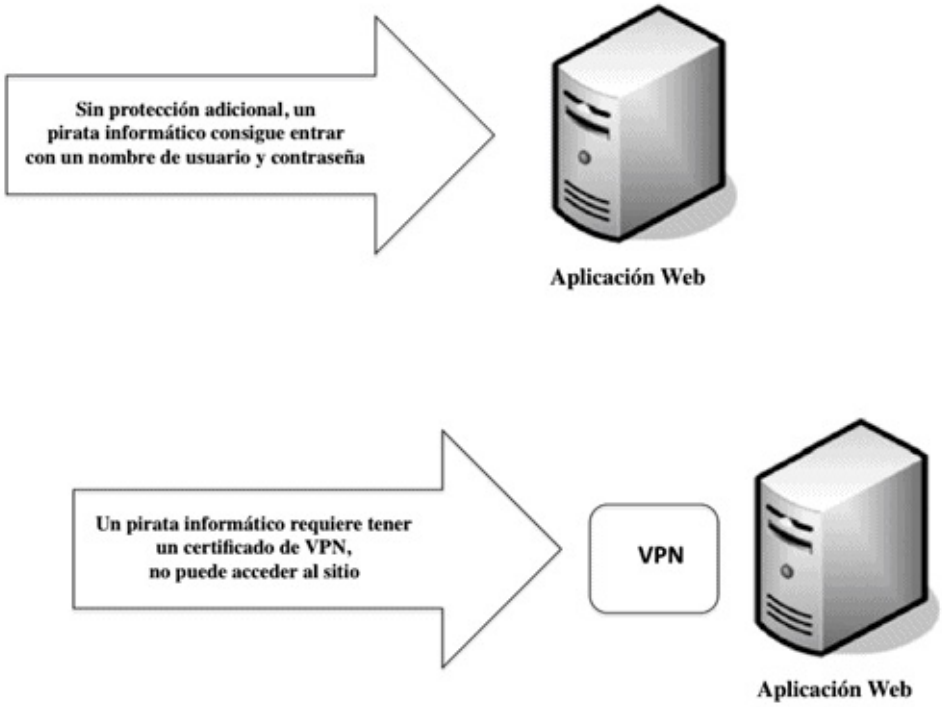


Figura 3-10
Red Virtual Privada

Un tema importante en la ISS es la nube informática, la cual permite a las empresas ofrecer servicios sin una inversión en infraestructura de tecnología. Un atractivo es que mucho de lo que concierne a TI es gestionado por otra persona. Lamentablemente, la nube informática también despierta inquietudes sobre la protección de datos.

Vulnerabilidades Reales: Un ejemplo de E-Mail

El e-mail (correo electrónico) se ha convertido en el mecanismo de comunicación estándar de facto en el ámbito empresarial. Lo que es sumamente interesante es que el e-mail está directamente disponible en Internet. Alguien pueden enviar un e-mail directamente al servidor de correos de otra persona, y ese servidor de correos entregarlo a la segunda persona. En general, esto es bueno; a la gente le gusta tener e-mail porque la conecta a otra gente en forma eficiente.

Sin embargo, para hacer su trabajo, el software de correos debe tener un cierta cantidad de permisos en el servidor del destinatario. Un e-mail especialmente diseñado puede hacer que el sistema de correos haga algo no deseado (al destinatario). Ese ataque de “escalada de privilegios” (escalation of privileges)

tiene éxito porque el programa de e-mail es engañado al ejecutar el e-mail como si fuera un programa más que procesarlo simplemente como texto.[29]

Este tipo de ataque en ninguna parte es más prevalente que en las aplicaciones Web. Tal como los profesionales de seguridad física, los profesionales de ISS aplican la defensa en profundidad para proteger los activos. Mientras más capas deba penetrar alguien para atacar a su objetivo, menos probabilidad de tener éxito en el ataque.

Generalmente, las aplicaciones Web hacen que esos ataques sean mucho más fáciles. Los usuarios de Internet anuncian su presencia, haciendo que los datos estén disponibles. Esto está bien cuando el usuario correcto está en el sitio Web de su banco. Sin embargo, abundan los riesgos.

Los nombres de usuario y contraseñas sólo son buenas si son secretas y no se pueden adivinar. La primera cosa que puede buscar un hacker es el nombre de usuario de alguien. A menudos es predecible, quizás una dirección de correo electrónico. Es una tarea un poco más difícil adivinar la contraseña o usar un programa llamado ataque de contraseña por fuerza bruta (brute force password hack) para repasar todas las combinaciones de contraseñas. Uno debe suponer que un cibercriminal puede penetrar estas dos defensas, los nombres de usuario y contraseñas.

Las aplicaciones de oficina típicas como Microsoft Word o Apple Pages generalmente parecen benignas. Sin embargo, en algunos casos, las personas han sido capaces de enviar archivos que le indican a esos programas que hagan cosas que no debieran hacer. Un usuario hace clic en ese archivo en un e-mail o lo descarga vía página Web, con permiso o no, y se produce el ataque.

A algunas personas les gusta usar un servicio llamado protocolo de transferencia de archivos (FTP por sus siglas en inglés) para compartir archivos. Lamentablemente, este es otro mecanismo a través del cual se puede tener acceso a la computadora de otro. Los programas hacen lo que se les dice, en el mejor de los casos, y a menos que estén adecuadamente especificados e implementados –una tarea que implica un gran desafío- no distinguen entre lo correcto y lo incorrecto.

Periféricos Relacionados

Muchos periféricos computacionales son motivo de preocupación para los profesionales de seguridad física. Ya se mencionó los variados dispositivos portables que pueden almacenar información, tales como los discos duros externos, las unidades flash, los iphones, etc. Estos dispositivos pueden cargar software malintencionado y sacar datos que no deberían sacarse.

La impresora, tal vez la forma de comunicación más antigua que se conecta a una red informática, también es motivo de preocupación. Las impresoras son conectadas a la red, por lo que las comunicaciones hacia y desde ellas pueden ser interceptadas. Más aun, algunas impresoras tienen unidades de discos duros o memoria interna, los cuales deben borrarse cuando se imprime información confidencial. Por último, la copia que la impresora crea puede ser llevada de un lugar a otro. Es esencial asegurarse que las impresoras de la organización tienen la seguridad y ubicación apropiada.

Las copiadoras modernas ahora se conocen como dispositivos de multifunción, los que pueden faxear, escanear, imprimir y copiar. Los profesionales de la seguridad deben considerar si la información de estos dispositivos puede ser eliminada y utilizada para motivos incorrectos. El escáner es otra preocupación debido a que convierte las copias impresas en documentos de formato electrónico que puede ser enviado al través del mundo en segundos. Todo dispositivo conectado a la red puede tener un efecto adverso.

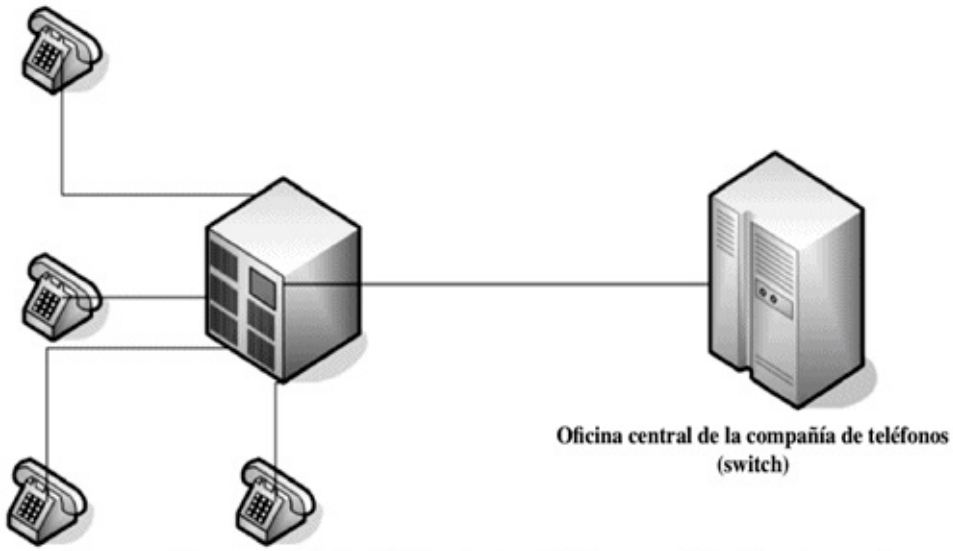
Telecomunicaciones

Los sistemas de telecomunicaciones son fundamentales para los negocios y la vida de las personas. Mientras que la mayoría de estos sistemas todavía están basados en tecnologías antiguas, las nuevas tecnologías han cambiado el panorama de las preocupaciones respecto a las telecomunicaciones.

Aunque considerados antiguos por los estándares modernos y denominados sistemas legacy (heredados) por los profesionales de TI, los sistemas de centrales telefónicas privadas (PBX private branch exchange) siguen siendo dispositivos de computación complejos que pueden verse comprometidos. Un PBX es el núcleo central de muchos sistemas telefónicos corporativos. Se debe entender una gran cantidad de funciones para asegurarse que están protegidos. Estos incluyen el correo de voz, las llamadas de larga distancia nacionales e internacionales, el desvío de llamadas, las conferencias telefónicas, control de llamadas y muchas otras funciones.

Además, algunos números, tales como los tradicionales números 976, cobran una tarifa cuando reciben la llamada, de modo que deben estar bloqueados. La compañía operadora de telefonía puede asegurarse de que esos números no puedan imputarse a la cuenta de la organización. Los sistemas PBX tradicionales se conectan al sistema telefónico internacional utilizando una o más tecnologías. Estas tecnologías son análogas a las conexiones de Internet que van a la oficina central. La oficina central actúa sobre comandos emitidos por el PBX. Este es otro lugar donde se puede ver comprometida la seguridad.

Los sistemas telefónicos son como cualquier otro sistema informático. Son simplemente sistemas operativos patentados que se ejecutan ya sea en un sistema integrado grabado en un hardware o en la parte superior de un servidor informático, como cualquier otra aplicación.



En un sistema PBX tradicional, los teléfonos están directamente conectados al PBX, el que está directamente conectado a la oficina central de la compañía de teléfonos.

Figura 3-11
Sistema PBX Tradicional

La mayoría de los sistemas telefónicos legacy no están realmente en la red. Los sistemas que unen un sistema legacy y un sistema moderno de voz sobre IP (VOIP por sus siglas en inglés) pueden estar en la red, pero son menos frecuentes. Esos sistemas suelen tener un mantenimiento remoto y una administración terminal (RMAT por sus siglas en inglés) que pueden utilizarse para marcar en el sistema y hacer cambios en su configuración. Además, los sistemas telefónicos legacy pueden activar una auditoría para ayudar al seguimiento de costos y detectar fraudes.

Cada teléfono en un sistema PBX legacy está conectado directamente al PBX. En la mayoría de los sistemas, esto se hace vía conexión digital, pero también puede ser a través del tradicional servicio de telefonía plana (POTS por sus siglas en inglés). Una línea telefónica POTS es una línea antigua, dos pares de líneas de teléfono que está conectado mediante cableado de cobre desde el teléfono a la oficina central (CO por sus siglas en inglés). Las líneas POTS también son conocidas como líneas análogas, las que son necesarias para los sistemas de incendio en la mayoría de las jurisdicciones, y son una buena idea para la intrusión en las conexiones de las alarmas de detección.

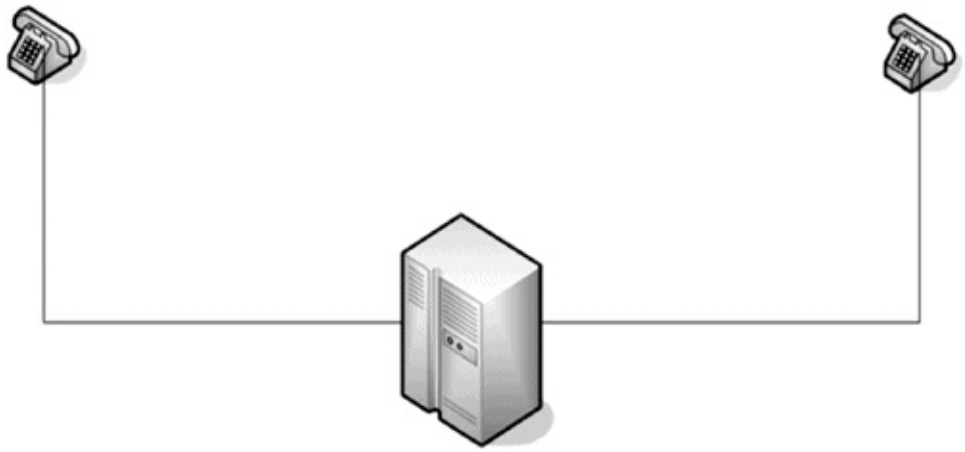


Figura 3-12
Oficina Central de la Compañía de Teléfonos

Las tarjetas para llamadas telefónicas también han disminuido considerablemente el costo en los últimos 20 años. Aún así, si se ven comprometidas, por ejemplo al ser vistas por encima del hombro del usuario, el usuario puede terminar con una cuenta más grande de lo esperado. Muchas compañías ahora están utilizando tarjetas de llamadas telefónicas de prepago para mitigar los riesgos de recibir grandes cuentas inesperadas.

El jugador más reciente es el sistema VOIP completamente automatizado. La convergencia de los teléfonos en la red tiene muchas ventajas: es menos cara debido a que el cableado es el mismo que el de una computadora; un teléfono se puede mover más fácilmente desde una ubicación a otra, porque se comporta como una computadora; y debido a que los sistemas se comportan como computadoras, el personal de TI es más capaz de administrarlos. Además, estos sistemas generalmente tienen funciones más avanzadas que los antiguos sistemas legacy. También pueden usar tecnologías avanzadas para reducir significativamente los costos telefónicos.

Sin embargo, los sistemas VOIP son totalmente accesibles en la red. Esto significa que cada teléfono y cada servidor que aloja información relacionada con un teléfono, incluyendo el correo de voz y las llamadas reales en curso, tienen el potencial de ser comprometidas.

El típico sistema telefónico moderno tiene un servidor que gestiona el proceso de obtener la voz del teléfono del que se habla, lo cual es realmente otro host, hacia el sistema telefónico tradicional y a otro teléfono. Como se muestra en la Figura 3-13, el tráfico de voz desde el teléfono a la oficina central de la compañía de teléfonos viaje en parte sobre una red.

En un sistema de voz sobre IP, cada uno de los teléfonos es un host, que es el dispositivo que controla el sistema telefónico. El tráfico fluye en la red del usuario y, posiblemente en Internet, antes de llegar a la compañía telefónica.

Figura 3-13
Sistema de voz sobre IP (VOIP)

Además, para ahorrar dinero algunas compañías conectan su oficina central vía Internet, lo que quiere decir que existe una exposición adicional del sistema a un compromiso potencial. Más aun, el mismo sistema telefónico, incluyendo los componentes adicionales, están disponibles en la red y podrían ser potencialmente comprometidos a través de distintos ataques basados en la red, incluyendo los ataques provenientes de Internet. Este riesgo afecta servicios como el correo de voz y la marcación mediante un software ejecutado en la computadora, así como la información de contacto. Todas estas preocupaciones deben ser consideradas en las políticas de ISS.

En un sistema telefónico tradicional, toda la energía viene del PBX hacia los teléfonos, y los teléfonos residenciales obtienen su energía de la compañía de teléfonos. Los profesionales de la seguridad deben asegurarse que, en el caso de un corte de la energía, las rutas fundamentales para la información del teléfono tengan una energía de respaldo de 12 horas o más, la expectativa típica de un sistema telefónico moderno.

También es necesario garantizar la redundancia a través de todos los componentes necesarios para mantener el sistema telefónico. Un PBX legacy por lo general está construido sólidamente con pocas partes móviles, tales como discos duros, ventiladores, etc. Un sistema telefónico VOIP generalmente se ejecuta en computadoras normales, las cuales son más propensas a los fallos que un simple dispositivo de estado sólido. Una instalación profesional de un VOIP por lo general tiene dos de estas máquinas en una configuración redundante de modo que si falla, la otra asuma el control.

La necesidad de redundancia se extiende a los routers que se conectan con el sistema telefónico, las líneas que conecta al sistema telefónico y los switches que conectan toda las redes. Los profesionales de seguridad física deben planificar para diferentes escenarios de emergencia. Por ejemplo, en un edificio que no permite el uso de teléfonos celulares, ¿qué pasaría si no hubiera ningún teléfono disponible para llamar al número telefónico policial para emergencias?

Varias de las nuevas tecnologías que vienen junto con los sistemas telefónicos modernos pueden mejorar

en gran medida la productividad y seguridad de los teléfonos de una organización. Por ejemplo, E911, puede decirle al equipo de respuesta a emergencias exactamente desde qué ubicación del edificio se llamó al número telefónico Policial para emergencias. Integrando esta tecnología con la seguridad del centro de operaciones de la organización puede ayudar al personal de seguridad del lugar a manejar mejor las emergencias. Otras características de los sistemas telefónicos modernos incluyen sistemas integrados de altavoces, sistemas automatizados para envío de mensajes, y la capacidad de acceder a otros sistemas a través del teléfono.

Otro tema relacionado con el teléfono es el fax. La seguridad tradicional del fax se centraba en quién estaba encargado de recibir el fax y si se dirigía a la persona adecuada. Por ejemplo, el envío de un fax a un área de recepción pública, como un hotel, hace que el fax ya no sea confidencial. No obstante, los sistemas modernos de fax vienen con otras preocupaciones. Primero, algunas maquinas de fax modernas tienen memoria para almacenar las imágenes de fax. Esa memoria puede o no ser borrada adecuadamente cuando el fax ha sido transmitido. Segundo, más y más sistemas pueden transmitir y recibir faxes electrónicamente, complicando la seguridad. Por ejemplo, en estados donde la información confidencial debe ser encriptada, los faxes confidenciales deben ser encriptados también. Además, los usuarios deben tomar precauciones especiales para proteger los faxes; antes simplemente se imprimían, ahora están disponibles electrónicamente.

Los teléfonos móviles y los PDA complican aún más la situación de las telecomunicaciones. Como dispositivos portables, presentan dos tipos de riesgos. Primero, alguien puede escuchar subrepticiamente la conversación. En el 2009, el algoritmo usado para encriptar la mayoría de los teléfonos de consumo fue descifrado (O'Brien, 2009). Los profesionales de seguridad física ciertamente deben preocuparse de la seguridad de las comunicaciones inalámbricas. Los Smartphones plantean preocupaciones aún más grandes. La enorme cantidad de información sensible, que solía estar contenida dentro del perímetro de la red de una compañía, puede ahora residir en un dispositivo pequeño, permanentemente móvil y fácil de perder.

3.2.4 CONCEPTOS ADICIONALES DE SEGURIDAD DE LA INFORMACIÓN

Calidad del Servicio

Otro concepto fundamental es la calidad del servicio (QoS por sus siglas en inglés). En una red de computadoras, muchos dispositivos diferentes compiten por la atención y la capacidad de comunicarse. La información sensible oportuna, como la información de las cámaras de video, debe ser capaz de pasar bajo cualquier circunstancia. Después que un profesional de seguridad identifica cuáles son los datos críticos en una red, los administradores de la red pueden decirle a la red para que le den la prioridad a los datos.

Revisión de Terceros

La revisión de terceros es un aspecto crítico de cualquier programa de seguridad de la información. Básicamente, una organización no es indemnizada por la externalización de ningún elemento en particular

de la seguridad de su información o los programas de tecnología de información. Cada organización es responsable por la gestión de sus proveedores y de asegurarse que ofrezcan un nivel específico, al menos el mismo que la organización contratante, en sus prácticas de seguridad de la información.

El Payment Card Industry Data Security Standard (PCI DSS)[30] señala lo siguiente (PCI Security Standards Council, 2010, p.11):

> Aquellas entidades que subcontratan a terceros prestadores de servicios para el almacenamiento, procesamiento o transmisión de los datos de los titulares de las tarjetas, [la entidad] deben documentar el rol de cada proveedor de servicio, identificando claramente cuáles requerimientos aplican a la entidad revisada y que aplican al proveedor del servicio. Hay dos opciones para validar el cumplimiento de los estándares de los proveedores de servicio: 1) ellos pueden someterse a una evaluación del PCI DSS por cuenta propia y entregar las pruebas a sus clientes para demostrar su cumplimiento, o 2) si ellos no se someten por cuenta propia a la evaluación del PCI DSS, será necesario que sean revisados durante el curso de cada una de las evaluaciones del PCI DSS de sus clientes.

En una plantilla de política de extranet (red externa) de SANS, una conocida autoridad en seguridad de la información, los siguientes son los cursos de acción apropiados cuando se permite el acceso de terceros a los datos de la organización (2006):

- una revisión de seguridad del tercero en cuestión por el departamento de seguridad de la información
- un análisis de viabilidad para tener el acceso a los datos
- una acuerdo de los requisitos para el acceso
- una nueva revisión de la seguridad en el sitio del tercero cuando se produzcan cambios

Adicionalmente, es prudente incluir revisiones periódicas de todos los accesos externos a la información, incluyendo el derecho a auditar al tercero.

3.2.5 TECNOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN

La siguiente es una breve reseña de tecnologías de seguridad de la información seleccionadas:[31]

Intrusion Detection Systems (IDS) (Sistema de Detección de Intrusión)

Un sistema de detección de intrusión supervisa la red e intenta descifrar vía comportamientos o patrones/firmas si alguien está tratando de atacar el sistema. Una variación del IDS es un sistema de prevención de intrusión (IPS por sus siglas en inglés), el cual es diseñado para detener automáticamente un ataque en curso. Sin embargo, un IPS puede detener un servicio válido, impidiendo innecesariamente que los usuarios accedan a la red.

Host Intrusion Protection System (HIPS) (Sistema de Protección de Intrusión Basado en Host)

Este es como un IDS excepto que funciona en un sistema host, como una computadora o servidor. El HIPS es una evolución de la protección del host de antivirus, debido a que es capaz de mirar tanto las firmas y los comportamientos para proteger una máquina. Cuando la gente afirma que un software antivirus está muerto, quieren decir que los programadores no pueden escribir las firmas lo suficientemente rápido para

identificar y mantener alejada la embestida de amenazas de virus, gusanos o troyanos y es necesaria esa protección basada en el comportamiento.

Certificates (Certificados)

Un certificado es un mecanismo a través del cual las personas que no se conocen entre ellas pueden garantizar una transacción segura. Los certificados son herramientas asimétricas que funcionan como una cerradura y la llave, permitiendo a las personas intercambiar información en forma segura a través de canales no confiables. Los certificados también son usados frecuentemente para permitir la encriptación, debido a que usando un par de certificados, es posible pasar un secreto compartido utilizado para descifrar la información. Debido a que los certificados generalmente son lentos al encriptar los datos, es preferible utilizar el certificado simplemente para intercambiar el secreto y luego usar un algoritmo mucho más rápido para intercambiar la información.

Security Information and Event Manager (SIEM) (Gestión de la Seguridad de la Información y de Eventos)

Un SIEM es un dispositivo que observa toda la actividad de registro en una red e intenta señalar lo que es más importante para facilitar la respuesta a las incursiones y otros problemas en la red. Ahora hay una clase de software para el campo de la seguridad física que hace lo mismo, llamado gestión de la información sobre la seguridad física (PSIM por sus siglas en inglés).

E-mail Gateway (Puerta de Enlace de Correo Electrónico)

Este es un dispositivo que observa la entrada y salida de correos para determinar si hay un riesgo de seguridad. Uno de los propósitos de un e-mail gateway es reducir la cantidad de correos spam (correo masivo), o los correos no deseados que ingresan a la red. Una gran cantidad de spam puede tener malware, y los sistemas gateway hacen lo posible para reducir la amenaza.

Web Gateway/Proxy Server (Puerta de Entrada a Sitio Web / Servidor Procurador).

Los web gateways y proxy servers filtran lo que puede ser descargado de la Web. Pueden impedir que los usuarios tengan acceso a sitios particulares, tales como los sitios pornográficos, o funcionan como un proxy, o intermediario, que elimina las páginas que podrían tener contenido malintencionado.

Data Loss Protection (DLP) (Protección de Pérdida de Datos)

Esta tecnología evita que la gente envíe cierta información, como los secretos comerciales u otra propiedad intelectual, fuera de la rede, ya sea involuntariamente o a propósito.

Web Application Firewall (WAF) (Cortafuego de Aplicaciones Web)

Un WAF es un dispositivo con un propósito especial que filtra el tráfico antes de que llegue al sitio Web de la organización. Los WAF son usados para evitar que los ataques malintencionados de código vulnerable logren alcanzar su objetivo, específicamente en un servidor Web.

Network Access Control (NAC) (Control de Acceso a la Red)

NAC es una tecnología mediante la cual las computadoras no son admitidas en una red a menos que estén autorizadas, no tengan un software malintencionado y cumplan lo estándares de la red.

802.1x

Este es un estándar del Institute of Electrical and Electronics Engineers (IEEE) que permite la autenticación específica antes de que una computadora pueda entrar en una red. Generalmente se usa con el control de acceso a la red.

Common Vulnerabilities and Exposures (CVE) (Vulnerabilidades y Exposiciones Comunes)

Este es un diccionario online de las vulnerabilidades y exposiciones de la seguridad de la información de conocimiento público. Forma la columna vertebral de la National Vulnerability Database y es una herramienta esencial en las disciplinas gemelas de gestión de las vulnerabilidades y gestión de parches. Está disponible en http://cve.mitre.org.

3.3 MARCO PARA LOS PROFESIONALES DE ISS

El ISS es suficientemente complejo como para requerir un marco sistemático si se quiere asegurar de que las contramedidas son adecuadas para manejar el riesgo. Un marco de seguridad organiza el cuerpo de conocimientos del ISS de una forma estratégicamente buena y focalizada, que apoya la planificación y la acción.

Existen varias perspectivas de los profesionales de ISS en uso. Han sido desarrolladas por diferentes organizaciones, y cada una tiende a reflejar un punto de vista diferente. Al exponerse a múltiples puntos de vista, el profesional de la seguridad es capaz de comprender mejor toda la gama de desafíos y soluciones en ISS.

Cada una de estas perspectivas se ocupa de un nivel abstracto del tema de los estándares para la protección de los activos de los sistemas de información. Sus puntos de vista son bastante diferentes, así como su historial.

- ISO/IEC 27001: 2005 e ISO/IEC 27002:2005 son extensiones de la ISO 17799, la cual se originó en Australia y Gran Bretaña antes de ser adoptada por la International Organization for Standardization.
- El Cuerpo Común de Conocimientos CISSP fue desarrollado para caracterizar el conjunto de conocimientos necesarios para la certificación como un profesional de ISS. Fue desarrollada por ISSA y es administrada por (ISC)^2 [32]
- La *Guidance for Boards of Directors and Executive Management* (Guía para la Junta de Directores y Gerencia Ejecutiva) fue desarrollada y publicada por la Information Systems Audit and Control Association.
- La “Generally Accepted Information System Security Practices” están siendo desarrolladas por un

consorcio internacional bajo el liderazgo de ISSA, con una mayoría de participantes que provienen de Estados Unidos.

3.3.1 ISO/IEC 27001:2005 e ISO/IEC 27002:2005

Estos dos estándares, conocidos informalmente como ISO 27001 y 27002, forman un estándar internacional emergente para la gestión de la seguridad de la información. Ellas son las primeras normas conocidas en todo el mundo para identificar un código de prácticas para la gestión de la seguridad de la información.

En conjunto los estándares identifican 11 prácticas específicas vitales de gestión de la seguridad de la información, integrándolas en un marco denominado sistema de gestión de la seguridad de la información (ISMS). La información de una organización está segura sólo en la medida en que estas 11 prácticas sean sistemáticamente gestionadas y reforzadas a través del ISMS. Las debilidades en una sola práctica o en el ISMS en sí mismo puede negar la fuerza combinada de otras prácticas.

La pieza central de la ISO 27001 es su concepto de un ISMS. Un ISMS de una organización es esa parte del sistema global de gestión de la organización (p.2)

> basado en un enfoque de los riesgos del negocio, para establecer, implementar, operar, supervisar, revisar y mejorar la seguridad de la información…El sistema de gestión incluye la estructura organizacional, las políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Las 11 prácticas de gestión de la seguridad de la información son las siguientes:

- política de seguridad
- organización de la seguridad de la información
- gestión de activos
- seguridad de recursos humanos
- seguridad física y ambiental
- gestión de comunicaciones y operaciones
- control de acceso
- adquisición de los sistemas de información, desarrollo y mantención
- gestión de incidentes de seguridad de la información
- gestión de la continuidad del negocio
- cumplimiento

3.3.2 CUERPO COMÚN DE CONOCIMIENTOS CISSP

Tal como la ISO 27001 y la ISO 27002 proporciona la directriz de certificación definitiva para una organización, el cuerpo de conocimientos del Certified Information Systems Security Professional (CISSP) proporciona los requerimientos de certificación definitiva apropiados al profesional de ISS individual. CISSP es el estándar de facto para la certificación ISS. El Common Body of Knowledge CISSP organiza las ISS en 10 dominios, enumerados a continuación, seguidos por una breve discusión de cada uno:

- **Control de acceso**. El control de acceso es definido por la tríada AAA autenticación, autorización y auditoría (responsabilidad). El hecho de que toda una sección esté dedicada al control de acceso indica la importancia de este principio básico de la seguridad de la información.
- **Seguridad del desarrollo de Aplicaciones**: un principio clave en seguridad de la información es la necesidad de escribir un código seguro. Esto significa que las instrucciones de programación dadas a la computadora deben hacer lo que se supone que deben hacer y no responder incorrectamente a los comandos.
- **Planificación de continuidad del negocio y recuperación de desastres**. Según Gregg (2009, p.280):

  > El dominio de plan de continuidad del negocio (BCP por sus siglas en inglés) y el plan de recuperación de desastres (DRP por sus siglas en inglés) aborda la necesidad de prepararse para y cómo responder a las ocasiones cuando las cosas van mal. Para que una empresa tenga éxito bajo la presión de una dificultad o catástrofe, debe planificar cómo mantener las operaciones del negocio ante estas grandes disrupciones.

- **Criptografía**. La criptografía es un aspecto importante de la seguridad de la información, ya que evita que las personas accedan a los datos reales (Gregg, 2009, p.118):

  > La criptografía se relaciona con las formas en las que la información puede ser cifrada o encriptada para evitar su divulgación. Está estrechamente vinculada a tres pilares básicos de seguridad: integridad, confidencialidad y no repudio.

- **Gestión de la seguridad de la información y gestión del riesgo**. La sección se ocupa de cómo una organización gestiona la seguridad de la información, identificando específicamente los riesgos y ocupándose de ellos a través de políticas, procedimientos y directrices.
- **Aspectos legales, regulaciones, investigaciones y cumplimiento**. Estas preocupaciones son una parte importante de la seguridad de la información. Además, es importante para el profesional de seguridad de la información conocer los elementos para conducir una investigación informática forense.
- **Seguridad de las operaciones**. Según Gregg (2009, p.450):

  > Los lectores que se preparan para el examen ISC2 Certified Information Systems Security Professional y aquellos que están repasando el dominio de seguridad operacional deben conocer los recursos que deberían ser protegidos; los principios de las mejores prácticas, los métodos de restricción de acceso, los potenciales abusos de acceso, la selección de los controles apropiados, y la respuesta a los ataques.

- **Seguridad física (ambiental):** obviamente, la seguridad física es una segunda naturaleza para los profesionales de la seguridad física. El objetivo es evitar que las personas accedan físicamente a los dispositivos electrónicos y mantener un entorno apropiada en el cual los sistemas puedan funcionar.

- **Diseño y arquitectura de seguridad**: esta sección se ocupa específicamente del hardware, software, controles de seguridad y la documentación. Es importante entender cómo funcionan los sistemas y para construirlos apropiadamente de modo que se comporten como se espera.
- **Seguridad de las telecomunicaciones y redes**. Esta sección es análoga a la discusión anterior sobre cómo se comunican las computadoras y cómo asegurar la red sobre la cual se comunican.

Para los profesionales de seguridad física interesados en aprender más acerca de la seguridad de la información, el CISSP es un excelente lugar para empezar. Proporciona una amplia base de conocimientos sobre los principios de la seguridad de la información.

3.3.3 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: GUÍA PARA LA JUNTA DE DIRECTORES Y GERENCIA EJECUTIVA

La tercera perspectiva, proporcionada en la *Gestión de la Seguridad de la Información: Guía para la Junta de Directores y Gerencia Ejecutiva* (ISACA, 2001), representa el punto de vista de los responsables de auditar el nivel de madurez del ISS de una organización.

El modelo ISACA fue elaborado en un marco de madurez de gestión de ingeniería de software que había sido desarrollado en los ochenta por el Software Engineering Institute, un centro nacional de tecnología en la Carnegie Mellon University. El modelo mide el grado en el que la seguridad de la información es formal y proactivamente gestionada a través de la organización.

Las organizaciones pueden aplicar el modelo de madurez de gestión ISACA a su propia organización como:

- una herramienta de evaluación “fotográfica” del momento, ayudando a la organización a identificar las fortalezas relativas a sus prácticas de gestión de la seguridad de la información,
- una herramienta para identificar el nivel apropiado de madurez de gestión de la seguridad, a la cual la organización puede evolucionar,
- un método para identificar la brecha entre su actual nivel de madurez de seguridad y el nivel deseado,
- una herramienta para planificar y gestionar un programa de mejora de la gestión de seguridad de la información en toda la organización, para mejorar sistemáticamente las capacidades de gestión de seguridad de la información de la organización, y
- una herramienta de planificación y gestión de proyectos específicos de mejora de la gestión de la seguridad de la información.

La Figura 3-14 proporciona una visión general de cada nivel de madurez de gestión de la seguridad de la información.

Nivel de Madurez de Gestión	Descripción
0	***Gestión de la seguridad Inexistente*** La organización no gestiona la seguridad de los activos de información
1	***Gestión Inicial de la seguridad ad hoc*** La gestión de la seguridad es ad hoc y no organizada; la responsabilidad de la gestión está fragmentada o no existe
2	***Gestión de la seguridad Repetible pero Intuitiva*** Las contramedidas y procesos básicos de seguridad están implementados; la responsabilidad de la gestión, autoridad y auditoría están asignadas
3	***Proceso Definido*** Los flujos de gestión de la seguridad de la estrategia organizacional y de una política de gestión del riesgo de toda la organización; los empleados reciben entrenamiento y educación regularmente
4	***Gestionada y Medible*** La gestión de la seguridad es supervisada y medida; se utiliza una retroalimentación regular para evaluar y mejora la eficacia de la gestión
5	***Gestión Optimizada de la seguridad*** Se siguen las directrices de configuración de la seguridad de la información

Figura 3-14
Nivel de Madurez de la Gestión de Seguridad de la Información

El mayor beneficio del marco ISACA es que permite niveles de madurez, haciendo posible medir qué tan bien lo está haciendo una organización comparado con qué tan bien podría hacerlo.

3.3.4 PRINCIPIOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN GENERALMENTE ACEPTADOS (GAISP)

La cuarta perspectiva proviene del proyecto de norma de los “Principios de Seguridad de los Sistemas de Información Generalmente Aceptados (GAISP de ahora en adelante, por sus siglas en inglés) en fase de desarrollo por la Information Systems Security Association (ISSA). Se distingue por la codificación de las prácticas reales de ISS que abarcan tanto la gestión, como la entrega de las capacidades del ISS.

GAISP es un proyecto en marcha para recolectar y documentar los principios de seguridad de la información que han sido probados en la práctica y aceptados por los profesionales. GAISP se basa en directrices y estándares de seguridad establecidos para crear una orientación integral, objetiva para los profesionales de la seguridad de la información, las organizaciones, gobiernos y usuarios. El uso de documentos y estándares existentes aceptados está diseñado para garantizar un alto nivel de aceptación para el producto final de GAISP.

3.4 EL NUEVO PANORAMA LEGAL, REGULADOR Y CONTRACTUAL RELACIONADO AL ISS

Además de comprender los marcos del profesional de ISS, los profesionales de la seguridad deben estar en conocimiento del conjunto de leyes y reglamentos de seguridad de la información que van apareciendo. El marco legal generalmente es diseñado para obligar a las organizaciones a proteger la información sensible a su cuidado que pertenece a otras personas. Esta sección examina los siguientes temas legales:

- Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)
- Health Care and Insurance Portability and Accountability Act (Ley de Portabilidad y Responsabilidad del Seguro de Salud)
- Ley de Gramm-Leach-Bliley
- Children's Online Privacy Protection Act (Ley de Protección de la Privacidad de Menores en Internet)
- Ley de Sarbanes-Oxley
- Red Flag Rules (Regla de las Banderas Rojas)
- Medidas de Cumplimiento de la FTC
- Incumplimiento de Divulgación y relacionados con ISS y las leyes de privacidad
- Directiva de Protección de Datos de la Unión Europea
- Nueva jurisprudencia

3.4.1 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

El Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago) es un estándar mundial definido por el Payment Card Industry Security Standards Council (2010). Con su origen en los distintos programas de ISS de Visa, MaterCard, American Express, Discover y JCB International, el estándar está diseñado para proporcionar un conjunto uniforme de estándares de ISS para proteger la información de las tarjetas de crédito. El estándar se aplica a todas las organizaciones que mantienen, procesan o intercambian información de los titulares de las tarjetas desde cualquier tarjeta marcada con el logo de una las empresas anteriores.

El estándar contiene 12 requisitos organizados en seis grandes categorías. Están incluidos los requisitos para la gestión de seguridad, las políticas y procedimientos. El PCI DSS está estructurado de la siguiente manera (pp.2-3):

Construir y Mantener una Red Segura

- Requisito 1: Instalar y mantener una configuración de cortafuegos (firewall) para proteger los datos de los titulares de las tarjetas.
- Requisito 2: No usar las contraseñas y otros parámetros de seguridad predeterminados por el proveedor

Proteger los Datos de los Titulares de las Tarjetas

- Requisito 3: Proteger los datos almacenados de los titulares de las tarjetas..
- Requisito 4: Encriptar los datos de los titulares de las tarjetas para la transmisión a través de redes abiertas, públicas.

Mantener un Programa de Gestión de Vulnerabilidades

- Requisito 5: Usar y actualizar regularmente los programas o software de antivirus.
- Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar Fuertes Medidas de Control de Acceso

- Requisito 7: Restringir el acceso a los datos de los titulares de las tarjetas por la necesidad de saber del negocio.
- Requisito 8: Asignar una identificación única a cada persona con acceso a una computadora.
- Requisito 9: Restringir el acceso físico a los datos de los titulares de las tarjetas.

Supervisar y Probar las Redes con Regularidad

- Requisito 10: Seguir y supervisar todo acceso a los recursos de la red y a los datos de los titulares de las tarjetas.
- Requisito 11: Probar regularmente los sistemas de seguridad y procesos.

Mantener una Política de Seguridad de la Información

- Requisito 12: Mantener una política que abarque la seguridad de la información para empleados y contratistas.

El incumplimiento de la norma trae graves consecuencias. En enero de 2010, Heartland Payment Systems acordó pagar 60 millones de dólares como parte de un acuerdo establecido con Visa. Anteriormente Heartland acordó con American Express 3,6 millones de dólares. Aún están por venir los acuerdos con MarterCard y Discover. Los pagos son el resultado de una vulnerabilidad en el 2008, cuando cibercriminales robaron la información de las tarjetas de crédito de millones de titulares de tarjetas de crédito (Cordeiro, 2010).

3.4.2 HEALTH CARE AND INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

La Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPPA por sus siglas en inglés) fue uno de los primeros intentos significativos de adoptar una norma para las transacciones electrónicas en el campo del cuidado de la salud. Si bien HIPPA aborda gran parte de los derechos de los pacientes según los planes de los seguros de salud, HIPPA también incluye disposiciones clave relacionadas con los derechos de privacidad de los pacientes. Las compañías de seguros, médicos, hospitales, laboratorios y empleadores que mantienen planes de salud de los empleados están sujetos a las disposiciones de HIPPA.

HIPPA se ha ampliado y modificado significativamente por la adopción, en el 2009, de la Ley de Tecnología de Información Económica y de Salud Clínica (Health Information Techology for Economic and Clinical Health - HITECH). Entre otras cosas, la ley HITECH exige que las empresas asociadas de las entidades cubiertas también adopten medidas de seguridad específicas.

El Department of Health and Human Services (HHS) de Estados Unidos ha emitido reglamentos que prevén la protección de la privacidad de "la información personal de salud" creada, recibida, o en posesión de las entidades cubiertas por HIPAA (45 CFR 160, 162, 164).

Las normas de seguridad de la información de HIPAA exige a las entidades cubiertas y empresas asociadas que hagan lo siguiente para proteger dicha información (45 CFR 162):

- Mantener un programa de gestión de la seguridad de la información orientado a los riesgos, basado en una combinación de controles administrativos, técnicos y físicos.
- Asegurar la confidencialidad, integridad y disponibilidad de toda la información electrónica de salud protegida que la entidad cubierta cree, reciba, mantenga o transmita.
- Proteger contra cualquier amenaza razonablemente esperada o riesgos de la seguridad o integridad de dicha información.
- Proteger contra cualquier uso o divulgación razonablemente esperada de dicha información que no esté autorizada o haya sido requerida.
- Asegurar el cumplimiento por su fuerza de trabajo.
- Asegurar el cumplimiento por terceros con los cuales se comparta la información.

HIPPA ilustra la tendencia general que requiere una organización para gestionar proactivamente la seguridad de la información que se le ha confiado.

La ley HITECH y las regulaciones asociadas publicadas por HHS y la Federal Trade Commission exige a las entidades cubiertas, empresas asociadas, y otras entidades que mantengan registros de atención de salud que informe a los pacientes –y agencias reguladoras- la ocurrencia de una violación de la seguridad que afecte la información de salud protegida en formato electrónico o en papel.

3.4.3 GRAMM-LEACH-BLILEY ACT (GLBA)

En 1999 el Congreso aprobó la ley Gramm-Leach-Bliley[33], la cual regula el uso y divulgación de información personal privada sobre las personas que obtienen productos o servicios financieros de instituciones financieras (15 USC 6801):

> Es política del Congreso que toda institución financiera tenga una obligación afirmativa y continua para respetar la privacidad de sus clientes y para proteger la seguridad y confidencialidad de la información personal no pública de esos clientes.
>
> En cumplimiento a la política …toda agencia o autoridad…establecerá estándares apropiados para las instituciones financieras sometidas a su jurisdicción con respecto a medidas de seguridad administrativas, técnicas y físicas
>
> (1) para garantizar la seguridad y confidencialidad de los registros de los clientes y la información;
>
> (2) para proteger contra cualquier amenaza o riesgo esperado para la seguridad o integridad de dichos registros; y
>
> (3) para proteger contra el acceso no autorizado o el uso de esos registros o información que podría resultar en un daño sustancial molestias para cualquier cliente

GLBA, en la superficie, aplica sólo a las instituciones financieras. Sin embargo, las definiciones amplias de GLBA implican que aplica no sólo a los bancos u otras instituciones financieras tradicionales, sino también a una amplia variedad de empresas e individuos que ayudan a efectuar las transacciones financieras. Estas incluyen corredores/agentes de bolsa, asesores de inversión, prestamistas hipotecarios, prestamistas en efectivo, compañías financieras, corredores hipotecarios, servicios de contabilidad, cambiadores de cheques, servicios de transferencias electrónica de fondos, agencias de viaje operadas en conexión con servicios financieros, agencias de cobranza, asesores de créditos y otros asesores de finanzas, empresas de preparación de impuestos, y cooperativas de créditos no aseguradas federalmente.

GLBA generalmente prohíbe a una institución financiera revelar información personal no pública a un tercero no afiliado, ya sea directamente o a través de una filial, a menos que la institución haya informado al cliente, de forma clara y manifiesta, que la información puede ser revelada a un tercero; le ha dado al cliente una oportunidad de disponer que la información no sea divulgada; y ha descrito la manera en la cual el cliente puede ejercer la opción de no divulgación.

Las instituciones financieras también deben preparar y promulgar las declaraciones de privacidad que describen las políticas de la institución respecto a la divulgación de información personal no pública a los terceros afiliados y no afiliados; la divulgación de información personal no pública de personas que han dejado de ser clientes de la institución; y las categorías de información personal no pública que la institución recopila. La institución está obligada a informar claramente y de forma manifiesta esas políticas y prácticas en el momento en que establece una relación con el cliente y, al menos una vez al año, durante al duración de la relación con el cliente. Eso ha dado lugar a una avalancha de papeles de los bancos, casas de corretaje, contadores, y otros que proporcionan servicios financieros.

GLBA también regula las medidas que una empresa debe tomar para evitar el intercambio involuntario de información personal no pública en sus sistemas informáticos. Toda agencia federal y estatal con jurisdicción GLBA tiene distintas regulaciones de protección de seguridad de la información.[34] Aunque no son idénticas, por lo general destacan lo siguiente:

- participación de la gerencia ejecutiva
- medidas dirigidas al riesgo y la vulnerabilidad, basadas en evaluaciones periódicas
- políticas escritas de seguridad de la información
- entrenamiento de los empleados
- control de terceros

Un efecto indirecto de la GLBA es un mayor cumplimiento de la actividad por la Federal Trade Commission. Además, muchas de las industrias directamente afectadas por la GLBA están empezando a aplicar los estándares que les han impuesto para sus clientes. Por ejemplo, las compañías de seguros están comenzando a revisar las declaraciones de privacidad y políticas de sus asegurados, y los bancos están empezando a considerar estos asuntos en sus decisiones de suscripción.

Numerosas regulaciones que tienen implicaciones de seguridad significativas aplican a las instituciones financieras. Por ejemplo, reglas especiales exigen a las instituciones financiera usar dos factores de autenticación con el fin de identificar los usuarios de sus servicios on line. Otras regulaciones definen las medidas que las instituciones financieras deben tomar en el evento de una violación a la seguridad.

3.4.4 CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA)

La Ley de Protección de la Privacidad de Menores en Internet (COPPA por sus siglas en inglés) (efectiva a partir del 21 de abril de 2000) aplica a cualquier operador on line que recopila información personal de niños menores de 13 años. Las normas adoptadas en virtud de COPPA explican lo que un operador de sitio Web debe incluir en una política de privacidad, cuándo y cómo buscar el consentimiento verificable de un padre, y qué responsabilidades tiene un operador para proteger la privacidad y seguridad on line de los niños. Además de crear desafíos para el diseño de los sitios Web –por ejemplo, muchos operadores Web han rediseñado sus sitios para hacerlos menos atractivos para los niños menores de 13 años- COPPA y las normas que implementa impone requisitos para los avisos de privacidad y crea procedimientos específicos que se deben seguir antes de que un operador pueda obtener información de los niños. COPPA ha sido la causante de que muchas empresas (y debería motivar a todas las empresas) a considerar sus políticas de privacidad tanto en la forma como en el fondo y a desarrollar guías prácticas.

La Federal Trade Commission (Comisión Federal de Comercio) hace cumplir COPPA. Algunas de las multas que ha impuesto incluyen las siguientes:[35]

- US$100.000 multa contra la Sra. Fields
- US$85.000 multa contra Hershey Foods
- US$1.000.000 multa contra el sitio de red social Xanga.com
- US$75.000 multa contra Bonzi Software
- US$130.000 multa contra el sitio de red social Imbee.com

- US$1.000.000 multa contra Sony BMG Music
- US$250.000 multa contra Iconix Brand

3.4.5 SARBANES-OXLEY ACT (SOX)

La ley Sarbanes-Oxley del 2002 (SOX por sus siglas en inglés) ha sido denominada la nueva ley de valores más importante desde que fue creada la Securities and Exchange Commission (Comisión de Bolsa y Valores, SEC) en 1934. SOX impone responsabilidades adicionales sustanciales a los funcionarios y directores de compañías públicas e impone sanciones criminales significantes a los directores ejecutivos (CEO por sus siglas en inglés), directores financieros (CFO por sus siglas en inglés), y otras personas que violen sus disposiciones.

Los nuevos requisitos de SOX transforma la manera en que todas las compañías públicas se gestionan de arriba hacia abajo. Incluso las corporaciones que no son públicas hoy, pero que esperan llegar a ser de propiedad pública o ser vendidas a una compañía pública en el futuro, necesitan estar en conocimiento de los requisitos básico para el funcionamiento de una compañía en cumplimiento a SOX, particularmente los requerimientos para el establecimiento, seguimiento y divulgación de controles y procedimientos internos. Los requisitos obligan a todas las compañías públicas a abordar sus procedimientos y prácticas de seguridad de la información de una manera muy pública.

La sección 404 de SOX exige a la gerencia de una compañía pública evaluar la efectividad del control interno de la compañía sobre los informes financieros. La sección 404 también exige a la gerencia incluir en el reporte anual de la compañía para los accionistas, las conclusiones de la gerencia respecto a esa evaluación. La sección 404 tiene la mayor relevancia para la seguridad de la información con su requerimiento de que la gerencia desarrolle, documente, pruebe y supervise sus controles internos y sus controles de divulgación y procedimientos.

La responsabilidad nueva más importante que afrontan el CEO y CFO de toda compañía pública es el requerimiento de certificación personal de los reportes anuales y trimestrales de la compañía. Para cumplir los requerimientos de certificación relacionados con los controles internos y los controles de divulgación, la SEC recomienda que toda compañía establezca un comité de divulgación conformado por el CFO, el contralor, los jefes de divisiones, y otras personas que tengan una responsabilidad significativa en las divisiones operativas principales de la compañía. El comité de divulgación debería revisar los controles internos existentes de la compañía, los controles de divulgación y los procedimientos, documentarlos, evaluar su adecuación, corregir cualquier debilidad material y crear procedimientos de supervisión y prueba que se usarán cada trimestre para evaluar continuamente los controles internos, los controles de divulgación y los procedimientos de la compañía.

Si bien la SOX fue adoptada en respuesta a las deficiencias y mal comportamiento de directores y funcionarios corporativos, su focalización en los sistemas y certificación de la adecuación de los esquemas de presentación de informes ha tenido un amplio efecto en el establecimiento de controles y estándares corporativos. Estos cambios no existen en el vacío; los principios del gobierno corporativo

que se aplicaron por primera vez a las corporaciones públicas ha menudo han sido extendidas a las compañías privadas, a veces a través de leyes y reglamentos estatales, otras veces a través de las fuerzas del mercado (por ejemplo, cuando los auditores y las compañías de seguros adoptan normas similares para compañías públicas y privadas).

3.4.6 RED FLAG RULES

La Regla de las Banderas Rojas pone en práctica las Secciones 114 y 315 de la Ley de Transacciones Crediticias Justas y Exactas (Fair and Accurate Credit Transaction – FACT). Diferentes versiones de la Regla de Banderas Rojas han sido adoptadas por las distintas agencias que regulan las instituciones financieras, así como la Federal Trade Commission (FTC). [36] Por ejemplo, la 16 CFR 681 (FTC) exige:

> a cada …acreedor que mantiene alguna cuenta de consumidor, u otra cuenta que represente un riesgo razonablemente previsible de robo de identidad, desarrollar e implementar un Programa de Prevención de Robo de Identidad (Programa) para combatir el robo de identidad.
>
> El programa debe incluir políticas y procedimientos razonables para detectar, prevenir, y mitigar el robo de identidad y permitir al… acreedor:

1. Identificar patrones relevantes, prácticas, y formas específicas de la actividad que son "banderas rojas" señalando un posible robo de identidad e incorporar esas banderas rojas en el Programa;
2. Detectar las banderas rojas que han sido incorporadas en el Programa;
3. Responder apropiadamente a cualquier bandera roja que sea detectada para prevenir y mitigar el robo de identidad; y
4. Asegurarse que el Programa es actualizado periódicamente para que refleje los cambios en los riesgos de robo de identidad.

El propósito del programa es la detección temprana y la prevención del robo de identidad.

Las "Cuentas Cubiertas" Requieren Protección

De acuerdo a las regulaciones de la FTC, una "cuenta cubierta" significa cualquiera de estas dos cosas:

> Una cuenta que una institución financiera o un acreedor ofrece o mantiene, principalmente para fines personales, familiares, o domésticos, que implica o se diseña para permitir múltiples pagos o transacciones, tales como cuenta de tarjeta de crédito, préstamo hipotecario, préstamo automotriz, cuenta de margen, cuenta de teléfono móvil, cuenta de servicios, cuenta de cheques, o cuenta de ahorros; y
>
> Cualquier otra cuenta que la institución financiera o acreedor ofrece o mantiene por la que hay un riesgo previsible razonable de robo de identidad para los clientes o para la seguridad y solidez de la institución o acreedor, incluyendo riesgos financieros, operacionales, de cumplimiento, reputación, o de litigios

Categorías de Bandera Roja

Las banderas rojas que deben ser identificadas, detectadas y respondidas, incluyen las siguientes:

- Alertas, notificaciones, o advertencias de una agencia de información del consumidor
- Documentos sospechosos

- Información de identificación personal sospechosa, como una dirección sospechosa
- Uso inusual de –o actividad sospechosa relacionada a- una cuenta cubierta
- Avisos de los clientes, víctimas de robo de identidad, autoridades competentes, o de otras empresas sobre posibles robos de identidad relacionado con las cuentas cubiertas

3.4.7 MEDIDAS DE CUMPLIMIENTO DE LA FTC

La Federal Trade Commission ha estado a la vanguardia de las normas de privacidad y seguridad de la información. En ese papel, ha adoptado una "regla de seguridad" bajo la GLBA, la cual exige que toda institución financiera dentro de su jurisdicción (16 CFR 314)

> desarrolle, implemente y mantenga un programa integral de seguridad de la información que esté escrito en una o más partes fácilmente accesibles y contenga medidas de seguridad administrativas, técnicas y física que sean apropiadas a su tamaña y complejidad, la naturaleza y alcance de sus actividades, y la sensibilidad de cualquier información del cliente en cuestión

Conforme a su autoridad para proteger a los consumidores, la FTC está en posición de adoptar normas que cruzan las fronteras de toda las industrias. También exige que toda empresa dentro de la jurisdicción de la FTC toma las determinaciones que sean consistentes con el tamaño y complejidad de la empresa y sus actividades, así como de la sensibilidad de la información del consumidor en cuestión. No proporciona reglas específicas; exige que las empresas se autorregulen. Por lo tanto, las empresas son forzadas a analizar sus operaciones, necesidades, y vulnerabilidades para cumplir con las reglas de seguridad de la FTC y GLBA.

Otra herramienta de la FTC para abordar la privacidad o violaciones de la seguridad ha sido la aplicación de la Sección 5 de la Ley de la FTC, que prohíbe las prácticas desleales y engañosas. Esta ley ha sido utilizada en las medidas de cumplimiento contra una amplia variedad de empresas, incluyendo Tower Records, DSW Wharehouse, Microsoft, Eli Lilly y VCS Caremark. Según la Ley FTC, la FTC está orientada a prevenir los métodos de competencia desleal y los actos o prácticas desleales o engañosas en o que afecten al comercio. En su sitio Web, la FTC destaca su intención de regular las privacidad online como parte de sus iniciativas de privacidad:[37]

> Una parte clave del programa de privacidad de la Comisión es asegurarse de que las compañías cumplan las promesas que hacen a los consumidores acerca de la privacidad y, en particular, las precauciones que toman para asegurar la información personal de los consumidores. Para responder a las preocupaciones de los consumidores sobre la privacidad, muchos sitios Web publican las políticas de privacidad que describen cómo la información personal de los consumidores se recopila, utiliza, comparte y asegura. De hecho, casi todos los 100 mejores sitios comerciales ahora publican sus políticas de privacidad. En uso de su autoridad según la Sección 5 de la Ley FTC, que prohíbe las prácticas desleales o engaños, la Comisión ha traído una serie de casos para hacer cumplir las promesas de las declaraciones de privacidad, incluyendo las promesas sobre la seguridad de la información personal de los consumidores.

Las Primeras Medidas de la FTC

La FTC has estado haciendo cumplir la Sección 5 de la Ley FTC al menos desde el caso GeoCities en 1998. Otras medidas tempranas de la FTC relacionadas con la privacidad online incluye las demandas con Eli Lilly y la Compañía (relacionadas con la información sensible recopilad de sus sitio Web Prozac); Microsoft Corp. (relacionado con la privacidad y seguridad de la información personal

recopilada de los consumidores a través de sus servicios Web “Pasaportes”); y Guess Incorporate (relacionada a la potencial divulgación de las tarjetas de crédito y otra información).[38]

Resoluciones de la FTC con TJX, Reed Elsevier (REI) y Seisint

En marzo de 2008, la FTC anunció una resolución con el distribuidor TJX que “falló al usar medidas de seguridad razonables y apropiadas para evitar el acceso no autorizado a la información personal en sus redes informáticas”. Según la FTC, un intruso

> Aprovechó estas fallas y obtuvo decenas de millones de tarjetas de pago de crédito y débito que los consumidores usaron en las tiendas TJX, así como la información persona de aproximadamente 455.000 consumidores que devolvieron las mercancías a las tiendas. Los bancos han afirmado que decenas de millones de dólares en cargos fraudulentos se han hecho en las tarjetas y millones de tarjetas han sido canceladas y vueltas a emitir.
>
> En concreto, la agencia denunció que TJX:
>
> - Creó un riesgo innecesario para la información personal almacenándola y transmitiéndola entre y dentro de sus diferentes redes informáticas en texto claro;
> - No usó las medidas de seguridad fácilmente disponibles para limitar el acceso inalámbrico a sus redes, permitiendo así que un intruso se conectara inalámbricamente a sus redes sin autorización;
> - No exigió a los administradores de la red y otras personas que usaran contraseñas robustas o que usaran diferentes contraseñas para acceder a los diferentes programas, computadoras y redes.
> - No utilizó medidas de seguridad fácilmente disponibles, como los cortafuegos, para limitar el acceso entre sus computadoras e Internet; y
> - No empleó medidas suficientes para detectar y prevenir el acceso no autorizado a las redes informáticas o para realizar investigaciones de seguridad, como los parches o la actualización de los software de antivirus.

En el mismo comunicado de prensa anunciando la resolución, la FTC anunció resoluciones similares contra los corredores Reed Elsevier (REI) y Seisint. La demanda de la FTC alega que los sistemas REI y Seisint contenían numerosas fallas de seguridad que fueron aprovechadas por ladrones de identidad para obtener acceso a la información sensible de al menos 316.000 consumidores de las bases de datos de Seisint. Los ladrones de identidad usaron la información para activar tarjetas de crédito y abrir nuevas cuentas, e hicieron compras fraudulentas con las tarjetas y las nuevas cuentas. La FTC explica:

> La resolución para TJX exige que establezca y mantenga un programa integral de seguridad razonablemente diseñado para proteger la seguridad, confiabilidad e integridad de la información personal que recopila de o sobre los consumidores. La resolución para REI y Seisint exige que establezcan y mantenga programas integrales de seguridad para proteger la información persona que es total o en parte información privada. Las resoluciones exigen que los programas contengan medidas de seguridad administrativas, técnicas y físicas apropiadas para el tamaño, naturaleza de sus actividades, y la sensibilidad de la información personal que recopila cada compañía. Específicamente, las compañías deben:
>
> - Designar un empleado o varios empleados para coordinar el programa de seguridad de la información;

- Identificar riesgos internos y externos para la seguridad y confidencialidad de la información personal y evaluar las medidas de seguridad existentes;
- Diseñar e implementar medidas de seguridad para controlar los riesgos identificados en la evaluación de riesgos y supervisar su efectividad;
- Desarrollar las medidas razonables para seleccionar y supervisar a los proveedores de servicios que manejan la información personal que reciben de las empresas; y
- Evaluar y ajustar sus programas de seguridad de la información para que reflejen los resultados de la supervisión, cualquier cambio material en sus operaciones, u otras circunstancias que puedan impactar la eficacia de sus programas de seguridad;

Las resoluciones requieren que las compañías mantengan auditores de seguridad independientes para evaluar sus programas de seguridad sobre una base bianual para los próximos 20 años. A los auditores se les exigirá certificar que los programas de seguridad de las empresas cumplen o exceden los requisitos de las órdenes de la FTC y están funcionando con la suficiente eficacia para proporcionar una seguridad razonable de que la información personal de los consumidores está siendo protegida.

Al anunciar estas resoluciones, la presidenta de la FTC, Deborah Platt Majoras dijo

Por ahora, el mensaje debe ser claro: las empresas que recopilan información sensible de los consumidores tienen la responsabilidad de mantenerla segura. Estos casos llevan a 20 el número de demandas en las cuales la FTC ha sancionado a las empresas por las deficiencias en la protección de la información sensible de los consumidores. La seguridad de la información es una prioridad para la FTC, como debiera ser para todas las empresas en Estados Unidos.

Resoluciones para la CVS Caremark

En febrero de 2009, CVS Caremark estableció que la FTC la acusa de que no tomó medidas de seguridad razonables y apropiadas para proteger la información financiera y médica de sus consumidores y empleados, en violación a la ley federal. [39] En un acuerdo separado pero relacionado, la cadena de farmacias de la compañía acuerda pagar 2.25 millones de dólares para resolver las demandas de HHS de que violaba HIPPA.

En el comunicado de prensa de la FTC, William E. Kovacic, Presidente de la Federal Trade Commission, dijo

Este es un caso que restaurará las protecciones de la privacidad apropiadas a decenas de millones de personas a lo largo del país… También envía un fuerte mensaje a otras organizaciones que poseen información personal protegida de los consumidores. Están obligados a asegurar la información privada de los consumidores.

Otras Resoluciones de la FTC por la Falta de Protección de la Información Sensible de los Consumidores

La FTC ha realizado numerosas acciones de cumplimiento contra las empresas. Aproximadamente 30 han dado lugar a una resolución pública. Entre ellas se encuentran las siguientes:[40]

- BJ’s Wholesale Club (minorista), 2005
- Life is Good (minorista de ropa), 2008
- Goal Financial, LLC (préstamos para estudiantes), 2008

- Choice Point (corredor de información del consumidor), 2006 y 2009
- Estas resoluciones de la FTC demuestran que las empresas que ignoran sus responsabilidades en la protección de sus activos de información tendrán que responder por sus actos.

3.4.8 DIVULGACIÓN DE INCUMPLIMIENTO ESTATAL Y LEYES RELACIONADAS CON LOS ISS Y LA PRIVACIDAD

Para complicar más aún el panorama legal están las numerosas leyes estatales relacionadas con la seguridad de la información. Debido a que son 50 estados, el volumen de leyes puede ser abrumador.

El 01 de julio de 2003, El Código Civil de California 1798.80-84 se convirtió en la primera ley estatal que exige que los consumidores sean notificados si una organización tiene razones para creer que ha sufrido una violación informática en la cual la información personal de los residentes de California hubiera sido comprometida.

En el momento de escribir este artículo, 46 otros estados, más el Distrito de Columbia, Puerto Rico y las Islas Vírgenes, han promulgado leyes que requieren la notificación de las violaciones a la seguridad que afecten la información.[41] El cumplimiento debe incluir todas estas leyes que aplican a la organización.

Los estados también han sido muy activos en la redacción de leyes de seguridad de la información y protección de la información privada (por ejemplo, California Civil Code 1798.81.5). Las Leyes de Massachusetts (201 CMR 17.00) proporcionan estándares mínimos para la protección de la información personal para cualquier empresa que posea o venda información personal de los residentes de Massachusetts. Las empresas que poseen ese tipo de datos están obligadas a desarrollar y supervisar un programa integral escrito de seguridad de la información, designar un empleado responsable del programa, implementar el entrenamiento, establecer políticas relacionadas con el acceso a la información, usar encriptación y exigir que los proveedores de servicios cumplan con estos requerimientos en todos los contratos escritos.

Minnesota, Nevada y Washington han promulgado leyes que permiten a los bancos recuperar los costos y daños de los minoristas y procesadores de tarjetas de crédito que sufran violaciones a la información después de no cumplir con los estándares actuales de la Industria de las Tarjetas de Pago (PCI).

El panorama va a complicarse más. El abogado de propiedad intelectual Stephen Wu señala (2010):

> Espero que los estados sigan probando la eficacia de la legislación relativamente modesta e incremental. No obstante, con el enorme costo de las violaciones de datos, pequeñas y grandes, es más importante que nunca que las empresas adopten programas de seguridad desde una perspectiva de gestión del riesgo, incluso si no tienen ningún requerimiento legal o reglamentario para hacerlo.

3.4.9 DIRECTIVA DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

En 1995, la Comisión Europea emitió la Directiva de Protección de Datos de la UE (Directiva 95/46/EC). La directiva está diseñada para armonizar las leyes nacionales de los estados miembros de la

UE que están dispuestas a proteger la privacidad y proteger toda la información personal recopilada sobre los ciudadanos de la UE. La directiva, la cual entró en vigencia en 1998, crea un marco estandarizado para los derechos de privacidad online, establece estándares mínimos que la legislación de protección de la información de todas las naciones miembro de la UE deben cumplir.

La directiva se complementa con la Directiva 2002/22/EC o ePrivacy Directive, que aborda la privacidad de las comunicaciones electrónicas y el uso de cookies y aclara las reglas que aplican a los mensajes comerciales no solicitados. Esa directiva ha sido modificada por la Directiva 2009/136/EC, en la que la UE exige a los estados miembros que modifiquen sus leyes nacionales acordadas en junio 2011.

US - EU Safe Harbor

La Directiva de Protección de Datos de la Unión Europea exige que las leyes nacionales de los estados miembros prohíban la transferencia de datos personales fuera de la UE excepto cuando el destinatario demuestre que proveerá un nivel adecuado de protección a la privacidad individual consistente con los estándares de la directiva.

Para proporcionar un medio ágil para que las organizaciones de Estados Unidos cumplan con la directiva y tengan en cuenta los diferentes enfoques de privacidad entre la Unión Europea y los Estados Unidos, el Departamento de Comercio de Estados Unidos en consulta con la Comisión Europea desarrolló un Puerto de Protocolo Seguro (safe harbor framework) a través del cual las organizaciones estadounidenses podrían demostrar que proveen un adecuado nivel de protección a la información personal de los ciudadanos de la UE.

El Departamento de Comercio de Estados Unidos (2000) ha documentado siete principios clave de privacidad que exige la Directiva de la UE 94/96 EC:

> **AVISO** (notice): Una organización debe informar a las personas acerca de los propósitos por los cuales recopila y utiliza información sobre ellos, cómo contactar a la organización ante cualquier pregunta o reclamo, los tipos de terceras partes a los que revela la información, y las opciones y medios que la organización ofrece a las personas para limitar su uso y divulgación…
>
> **OPCIÓN** (choice): Una organización debe ofrecer a las personas la oportunidad de elegir (opt ut) si su información personal va (a) a ser revelada a un tercero* o (b) a ser utilizada con un propósito que es incompatible con los propósitos para los cuales originalmente fue recopilada o subsecuentemente autorizada por la persona…
>
> **TRANSFERENCIA SUCESIVA** (onward transfer): para revelar la información a un tercero, las organizaciones deben aplicar los Principios de Aviso y Opción…
>
> **SEGURIDAD** (security): las organizaciones que crean, mantienen, usan o difunden información personal deben tomar precauciones razonables para protegerla de pérdidas, mal uso, acceso no autorizado, divulgación, alteración y destrucción.
>
> **INTEGRIDAD DE LA INFORMACIÓN** (data integrity): consistente con los Principios, la

información personal debe ser relevante para los propósitos para los cuales se va a utilizar…

ACCESO (access): las personas deben tener acceso a la información personal de ellas que una organización mantiene y tener la posibilidad de corregir, modificar, o borrar esa información cuándo sea inexacta…

CUMPLIMIENTO (enforcement): la protección eficiente de la privacidad debe incluir mecanismos para asegurar el cumplimiento de los Principios, el recurso para las personas con quienes se relacionan los datos afectados por el no cumplimiento de los Principios, y las consecuencias para la organización cuando los Principios no se cumplan…

* No es necesario avisar o dar a elegir cuando se hace la divulgación a un tercero que está actuado como un agente para realizar tareas en nombre de y bajo las instrucciones de la organización. El principio de transferencia, por el contrario, aplica a esas divulgaciones.

3.4.10 NUEVA JURISPRUDENCIA

Responsabilidad por el Robo Bancario Online

Era sólo cuestión de tiempo que los cibercriminales descubrieran que irrumpir en los sistemas informáticos de las empresas podría darles acceso a las credenciales bancarias online. Eso parece haber sucedido en gran escala en el tercer trimestre de 2009, cuando los cibercriminales robaron más bancos online que en el tradicional robo de bancos con ladrillo y mortero. Krebs (2010, "Cyber crooks") señala que en el tercer trimestre de 2009 los cibercriminales robaron más de 25 millones de dólares en robo a bancos online, mientras que los tradicionales ladrones de banco obtuvieron menos de 9,5 millones de dólares durante el mismo período.

Los cibercriminales son capaces de lanzar el ataque "man-in-the-middle" (hombre en el medio o ataque de suplantación de identidad) y otros sofisticados ataques contra las empresas aprovechando las vulnerabilidades técnicas de los sistemas informáticos junto con los ataques de ingeniería social dirigidos a las personas clave. Los cibercriminales también instalan software maliciosos en la computadora de la víctima para robar las credenciales de la banca en línea, y luego usar esas credenciales para desviar dinero desde las cuentas objetivo.

Debido a que estos ataques utilizan credenciales de banca en línea legítimas, los bancos reclaman que ellos no tienen la obligación legal de reembolsar a las empresas sus pérdidas, ya que el banco usa medidas de seguridad comercialmente razonables según se establece en el Uniform Commercial Code § 4A-202 (Authorized and Verified Payment Orders) (Órdenes de Pago Autorizadas y Verificadas).

Varias empresas víctimas han presentado demandas contra sus bancos en un intento de recuperar sus pérdidas:

- En septiembre de 2009, un tribunal del distrito de Illinois dio lugar a la demanda de una empresa contra su banco con el argumento de que puede haber fallado en asegurar suficientemente su cuenta, después que un hacker no identificado obtuvo un préstamo de 26.500 dólares en la cuenta usando el nombre de usuario y contraseña de los clientes (Zetter, 2009).

- En septiembre 2009, una empresa constructora en Maine demandó a un banco local después que ladrones cibernéticos robaron más de medio millón de dólares de la empresa en un sofisticado robo online (Citadel Information Group, 23 septiembre 2009).
- En diciembre 2009, una empresa de pruebas electrónicas en Lousiana demandó a su banco, Capital One, alegando que la institución financiera fue negligente al no detener una transferencia de los hackers de casi 100 mil dólares desde su cuenta (Citadel Information Group, 07 diciembre 2009).
- En marzo 2009, una empresa de tasaciones de bienes raíces en Hammond, Louisiana, perdió más de 27 mil dólares cuando se hicieron cuatro retiros automáticos no autorizados (ACH)[42] y se enviaron a personas en Estados Unidos. La empresa está demandando a su banco, también el Capital One, para recuperar sus pérdidas (Krebs, 2010, "Victim").

En un caso inusual, el banco PlainsCapital en Lubbock, Texas, está demandando a su cliente, Hillary Macinery Inc. El banco PlainsCapital citó una carta de Hillary que exigía el pago de una pérdida online, alegando que el banco no había empleado las medidas de seguridad comercial razonable. La demanda pide a la Corte del Distrito de Estados Unidos del Distrito Oriental de Texas, certificar que la seguridad de PlainsCapital era de hecho razonable, y que procesó las transferencias electrónicas de buena fe. En los documentos presentados a la corte, el banco alega que las transacciones fraudulentas fueron iniciadas utilizando las credenciales de banca online válidas del demandado (Krebs, 2010, "Texas").

Demandas Colectivas

No es extraño que se hayan presentado demandas colectivas en contra de las empresas que han perdido información sensible de los clientes. Una demanda colectiva de los accionistas contra Heartland Payment System por la violación de sus datos fue desestimada en diciembre de 2009. La demanda había sido presentada por lo accionista que alegaban que Heartland no protegió adecuadamente la información de los clientes comprometidos y no notificó a los clientes sobre de la violación de manera oportuna como lo exige la ley (Mills, 2009).

En una demanda colectiva de clientes por la misma violación de datos, Heartland Payment Systems acordó el pago de un mínimo de 1 millón de dólares y hasta un máximo de 2,4 millones a los miembros que presentaron solicitudes válidas de pérdidas como resultado de la intrusión. La empresa también será responsable de 1,5 millones de dólares por el costo de notificar los demandantes y USD$ 760.000 para cubrir los honorarios legales (Heartland, 2009).

En otra demanda colectiva de consumidores, en abril de 2010, la Corte de Distrito de Estados Unidos del distrito occidental de Kentucky comenzó alertando a los consumidores que proporcionaron su información personal o hicieron pagos hipotecarios a Countrywide sobre un acuerdo propuesto alcanzado en una demanda colectiva sobre el robo de información personal y financiera (Court, 2010). La demanda afirma que un alto asesor financiero que había sido empleado por Countrywide tomó la información confidencial de millones de registros de clientes y los vendió a terceros. La demanda alegaba que Countrywide no protegió adecuadamente la información personal y financiera de sus clientes. Bajo el acuerdo propuesto, Countrywide debe proporcionar la supervisión del crédito y el seguro de robo de

identidad de estos clientes; reembolsar en efectivo más de 6,5 millones de dólares a las víctimas de robo de identidad; y los honorarios del abogado demandante de 3.625 millones de dólares.

Obviamente, como los sistemas de información se convierten en omnipresentes, el panorama legal aún es incipiente. Como afirma Francoise Gilbert en su conferencia sobre aspectos de seguridad y privacidad de la información (2008):

> Hace un tiempo atrás, no hace mucho, cuando Internet era un mundo aparte. Distinguíamos e-commerce (comercio electrónico) y otras actividades en el "ciberespacio" de aquellos que han existido durante siglos en lo que hemos denominado el mundo de "ladrillo y mortero". Este ya no es el caso. Estos mundos han convergido.

Claramente hay un mayor sentido de responsabilidad por la seguridad de la información, un panorama legislativo complejo y un escenario legal que cambia rápidamente. El asesor legal debe participar no sólo durante el desarrollo de un programa de ISS de una organización, sino que también después, periódicamente, para asegurarse que el programa cumple con los cambios en las leyes y otras obligaciones legales.

3.5 TEMAS ESPECIALES DE LOS ISS

Esta sección examina tres temas adicionales:

1. Evaluación del riesgo y vulnerabilidad del ISS
2. Implementación de la política
3. Respuesta a incidentes

Después de este examen, el lector habrá sido expuesto a todos los elementos de la gestión de la seguridad de los sistemas de información (ISMS por sus siglas en inglés). La siguiente sección usa esos elementos para elaborar un marco integral para los ISMS conforme a lo requerido por la norma ISO 27001.

3.5.1 EVALUACIÓN DEL RIESGO Y VULNERABILIDAD DE LOS ISS

Todo estándar profesional y legal descrito aquí exige que una organización gestione el ISS utilizando un enfoque basado en el riesgo.

Generalmente, una evaluación del riesgo y vulnerabilidad se realiza para medir el cumplimiento de una norma específica. Por ejemplo, el Payment Card Industry Data Security Standard exige a las compañías que tienen tarjetas de crédito o débito que lleven a cabo una evaluación con respecto al actual PCI DSS. Una empresa que busca ser certificada en conformidad a la ISO 27001 deberá realizar una evaluación del riesgo y vulnerabilidad de acuerdo a los estándares de ISO 27001. Un tercero que reciba información de los pacientes desde un centro médico necesitará evaluar su capacidad para cumplir los requisitos de privacidad del HIPAA.

Una evaluación de ISS por lo general aborda los objetivos tradicionales del ISS: proteger los sistemas de información; detectar los ataques al sistema, tanto los exitosos como los bloqueados; y cumplir con las leyes, reglamentos y obligaciones contractuales – garantizando la confidencialidad, integridad y disponibilidad de los datos de la organización.

Una evaluación de riesgo y vulnerabilidad del ISS generalmente tiene componentes de gestión y técnicos. El componente de gestión puede ser desde muy formal a muy informal. En su modo más formal, el componente de gestión puede tener el rigor de una auditoría formal realizada para demostrar el cumplimiento con una norma documentada. En su modo más informal, el componente de gestión puede consistir en entrevistas estructuradas con personal y directivos seleccionados, junto con una revisión de la documentación disponible. El componente técnico de la evaluación del riesgo proporciona a la organización una evaluación formal del momento de la seguridad de su infraestructura de TI.

Independientemente de lo específico o general, de lo formal e informal, una evaluación del riesgo y vulnerabilidad del ISS puede responder las siguientes interrogantes:

- ¿Cuáles son las necesidades, obligaciones y oportunidades de la seguridad de la información de la organización?
  - obligaciones legales para proteger la información
  - obligaciones éticas para proteger la información de los clientes, socios comerciales y otras personas
  - riesgo de incidente de seguridad de la marca
  - responsabilidades fiduciarias
  - oportunidades competitivas
- ¿Qué tan efectiva es la organización en la gestión de la seguridad de sus activos de información críticos?
  - controles administrativos, técnicos y físicos
  - estructura de gestión
  - políticas de ISS
  - clasificación y control de la información
  - educación y entrenamiento de la conciencia del usuario
  - seguridad de computadoras y redes
  - seguridad física
  - seguridad del personal
  - garantía de terceros del ISS
- ¿Cuáles son las brechas entre sus necesidades y sus realidades?

  - brechas de gestión
  - brechas de tecnología
  - brechas culturales
- ¿Qué capacidad existe para subsanar la brecha?
  - Tiempo y recursos
  - Capacidad de atención
  - Cultura

Armada con esta información, ahora la organización puede hacer planes para subsanar metódicamente sus brechas del ISS.

3.5.2 IMPLEMENTACIÓN DE LA POLÍTICA DEL ISS

Según la norma ISO 27002, las políticas de seguridad de la información deben incluir, como mínimo, las siguientes directrices:

- una definición de seguridad de la información, sus objetivos generales, el alcance y la importancia de la seguridad como un mecanismo propicio para el intercambio de información
- una declaración de las intenciones de la gerencia, apoyando los objetivos y principios de seguridad de la información
- una breve explicación de las políticas, principios, estándares y requerimientos de cumplimiento de seguridad de particular importancia para la organización

El desafío más grande de la gerencia no radica en la escritura de las políticas específicas sino en el desarrollo ordenado y la implementación de las políticas. Una organización puede aumentar las posibilidades de que sus políticas de seguridad de la información influirán realmente en la seguridad mediante los siguientes pasos. Más aún, siguiendo una rigurosa metodología de desarrollo de las políticas de ISS prepara a una organización para la implementación de un sistema de gestión de la seguridad de la información.

Este proceso de ocho pasos ilustra una metodología:

Paso 1 Identificar los problemas organizacionales que afectan a la política de ISS

Paso 2 Identificar la información que necesita protección y la protección requerida

Paso 3 Identificar las distintas clases de usuarios de la política

Paso 4 Elaborar las políticas de ISS basándose en los pasos 1-3

Paso 5 Revisar las políticas elaboradas con la gerencia, los usuarios, y el asesor legal, y luego finalizarlas.

Paso 6 Capacitar a todo el personal en las políticas de ISS de la organización

Paso 7 Hacer cumplir las políticas de ISS

Paso 8 Revisar y modificar las políticas, según proceda, pero al menos anualmente.

3.5.3 RESPUESTA A INCIDENTES

La respuesta a incidentes de seguridad de la información es un conjunto de habilidades críticas para los inevitables problemas relacionados con la seguridad de la información. Esos problemas comprenden todos los tipos de incidentes ya descritos, incluyendo malware, hacking, y errores. De acuerdo a NIST (Scarfone, K., Grance,T., & Masone, K., 2008, p.ES-1):

> La respuesta a incidentes de seguridad de computadoras ha llegado a ser un componente importante de los programas de tecnología de la información (TI). Las amenazas relacionadas con la seguridad no sólo se han convertido en más numerosas y diversas, sino también en más dañinas y disruptivas. Los nuevos tipos de incidentes relacionados con la seguridad surgen frecuentemente. Las actividades preventivas basadas en los resultados de las evaluaciones de riesgo pueden disminuir el número de incidentes, pero no todos los incidentes pueden ser evitados. Una capacidad de respuesta a incidentes es, por lo tanto, necesaria para la rápida detección de incidentes, minimizar las pérdidas y destrucción, mitigar las debilidades que fueron aprovechadas y restaurar los servicios informáticos.

Según CERT, una conocida unidad de respuesta de seguridad de la información de la Carnegie Mellon University, existen 19 pasos para desarrollar un equipo de respuesta a seguridad de incidentes informáticos (CSIRT por sus siglas en inglés) (CERT, 2006):

1. Identificar las partes interesadas y los participantes.
2. Obtener el apoyo y patrocinio de la gerencia.
3. Desarrollar un plan de proyecto CSIRT.
4. Reunir información.
5. Identificar la circunscripción de CSIRT.
6. Definir la misión del CSIRT.
7. Asegurar los fondos para las operaciones del CSIRT.
8. Decidir el alcance y nivel de servicios que el CSIRT ofrecerá.
9. Determinar la estructura de presentación de informes del CSIRT, la autoridad y el modelo organizacional.
10. Identificar los recursos necesarios tales como personal, equipos e infraestructura..
11. Definir las interacciones e interfaces.
12. Definir roles, responsabilidades y la respectiva autoridad
13. Documentar el flujo de trabajo.
14. Desarrollar políticas y los procedimientos respectivos.
15. Crear una implementación del plan y solicitar la retroalimentación .

16. Anunciar el CSIRT cuando esté operacional.
17. Definir métodos para evaluar el rendimiento del CSIRT..
18. Tener un plan de respaldo para cada elemento del CSIRT
19. Ser flexible.

La creación de un equipo de respuesta a incidentes también es analizada por SANS, una notable autoridad en seguridad de la información (utilizando un nombre diferente para el equipo):

> Ninguna política de seguridad de la empresa debe ser considerada completa hasta que se apliquen los procedimientos que permiten el manejo y recuperación de incluso el más devastador de los incidentes. Una posible solución es la inclusión de un Equipo de Respuesta a Incidentes Informáticos (CIRT por sus siglas en inglés) dentro de los procedimientos de respuesta a incidentes de la empresa.

NIST, CERT y SANS tienen muchos documentos de ayuda para desarrollar planes de respuesta a incidentes de seguridad de la información. Uno de los elementos más críticos del plan es el documento de política. NIST define los elementos de la política de respuesta a incidentes para ser (Scarfone, K., Grance, T., & Masone, K., 2008, p.2-3):

- Declaración del compromiso de la gerencia
- Propósitos y objetivos de la política
- Alcance de la política (a quién y qué se aplica y bajo qué circunstancias)
- Definición de incidentes de seguridad informática y sus consecuencias dentro del contexto de la organización
- Estructura organizacional y delimitación de funciones, responsabilidades, y niveles de autoridad; debe incluir la autoridad del equipo de respuesta a incidentes para confiscar o desconectar equipos y para supervisar actividades sospechosas, y los requerimientos para informar cierto tipo de incidentes
- Priorización o calificación de la gravedad de los incidentes
- Medidas de funcionamiento
- Informes y formularios de contacto

El CSIRT o CIRT forman la capacidad esencial de respuesta para remediar un incidente. La seguridad física puede ser un elemento crítico de este equipo, especialmente debido a las similitudes en la respuesta a incidentes entre los paradigmas de seguridad física y de la información. Como bien saben los profesionales de seguridad física, estar preparados para responder a incidentes es un aspecto crítico de cualquier programa de seguridad.

3.6 GESTIÓN TOTAL DEL ISS

Los riesgos, amenazas, vulnerabilidades y contramedidas son todos cambiantes. Como los

ciberdelicuentes mejoran su oficio, los defensores deben mejorar los suyos. Asimismo, mientras mejores son los chicos malos, más probabilidad de que leyes, reglamentos y contratos serán fortalecidos para exigir una mejor seguridad de los sistemas de información. La carrera de armamentos resultante da lugar a lo que se conoce como Red Queen Effect[43] (Efecto Reina Roja).

En un sentido amplio, de acuerdo con otras mejores prácticas de gestión en constante evolución, el Efecto Reina Roja requiere que el programa de gestión de los sistemas de información de una organización sea mejorado continuamente.

Esto significa que la función de la gerencia no puede ser sólo proporcionar un nivel apropiado de seguridad de los sistemas de información hoy. La gerencia del ISS también debe aceptar la responsabilidad de hacer un mejor trabajo mañana. Este es el propósito del sistema de gestión de seguridad de la información (ISMS).

3.6.1 ISO 27001 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La pieza central de la norma ISO 27001 es el ISMS, la piedra angular para la mejora continua de la capacidad de la organización para gestionar eficientemente la seguridad de sus activos de información.

El ISMS de una organización es esa parte de la organización que corresponde al (ISO 27001, p.2)

> sistema general de gestión, basado en un enfoque de riesgo empresarial, para establecer, implementar, operar, supervisar, revisar y mejorar la seguridad de la información…El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Un ISMS se basa en una perspectiva de modelo de proceso de gestión de seguridad de la información (ISO 27001, p.v):

> El enfoque del proceso para la gestión de la seguridad de la información presentado en este Estándar Internacional estimula a sus usuarios a destacar la importancia de:
>
> a. Comprender los requerimientos de seguridad de la información de una organización y la necesidad de establecer políticas y objetivos para la seguridad de la información;
> b. Implementar controles de operación para manejar los riesgos de la seguridad de la información de una organización en el contexto de los riesgos empresariales globales de la organización
> c. Supervisar y revisar el funcionamiento y eficacia del ISMS; y
> d. La mejora continua basada en una medición objetiva

El siguiente diagrama basado en la ISO 27001 ilustra el modelo espiral planificar-hacer-verificar-actuar (PDCA por sus siglas en inglés).

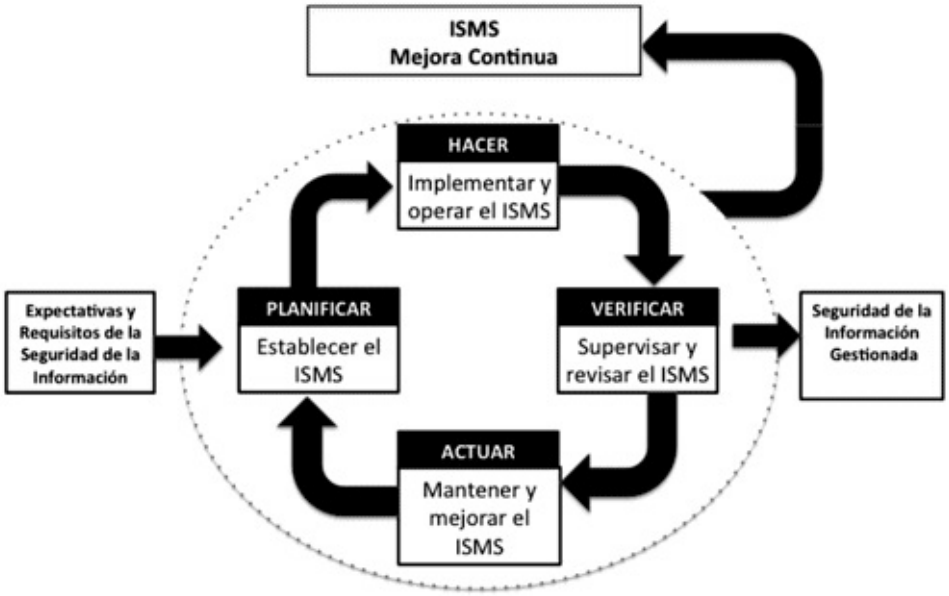


Figura 3-15
Modelo Planificar-Hacer-Verificar-Actuar
Aplicado a los Procesos ISMS

A la izquierda, como entrada continua al modelo PDCA, están los requerimientos y expectativas cambiantes de la seguridad de la información. A la derecha, como salida continua del modelo PDCA, está la constante capacidad de mejora para gestionar las necesidades de la organización. Un ISMS basado en la progresión continua de planificar-hacer-verificar-actuar puede generar la mejora continua.

La ISO 27001 define las cuatro fases del PDCA como sigue:

Planificar	**Establecer el ISMS** Establecer la política, objetivos, procesos y procedimientos relevante del ISMS para gestionar el riesgo y mejorar la seguridad de la información en alineación con las políticas globales y objetivos de la organización.
Hacer	**Implementar y Operar el ISMS** Implementar y operar la política, controles, procesos y procedimientos del ISMS
Verificar	**Supervisar y Revisar el ISMS** Evaluar y si es el caso medir el funcionamiento del proceso comparado con la política del ISMS, los objetivos, y la experiencia práctica; informando los resultados a la gerencia para la revisión.
Actuar	**Mantener y Mejorar el ISMS** Mejorar continuamente el ISMS tomando las medidas correctivas y preventivas sobre la base de los resultados de auditorías internas del ISMS, revisión de la gestión, y otra información relevante.

3.6.2 HACIENDO POSIBLE LA MEJORA CONTINUA

La idea fundamental detrás de un ISMS es la mejora continua, siempre logrando lo mejor, siempre la vara más alta. Muchos programas de mejora continua se han desarrollado, implementado y probado en los últimos 40 años. Se ha aprendido mucho sobre lo que funciona y lo que no funciona al implementar esos programas. Sin duda un factor clave es la cultura organizacional.[44]

Una Cultura de Conciencia del ISS

La efectividad de un programa de seguridad de la información depende finalmente del comportamiento de las personas [45] . El comportamiento, a su vez, depende de lo que las personas saben, de cómo se sienten y de lo que sus instintos les digan que hagan. Si bien un programa de entrenamiento de conciencia de ISS puede impartir conocimientos sobre seguridad de la información, rara vez tiene un impacto significativo en los más profundos instintos de seguridad de las personas. El resultado es una brecha entre lo que dictan las políticas de seguridad de la información y los comportamientos de las personas. A menos que los sentimientos e instintos de las personas sobre la seguridad de la información cambien, la brecha seguirá existiendo. Es función de la cultura eliminar esa brecha.

La cultura de una organización se puede definir de la siguiente manera (Shein, 1992):

> Un patrón de suposiciones compartidas básicas que el grupo aprendió como ello resolvió sus problemas de adaptación externa e integración interna, que ha funcionado lo suficientemente bien para ser considerado válido y, por lo tanto, ser enseñado a los miembros nuevos como el modo correcto de percibir, pensar y sentir en relación a esos problemas.

En la medida que una organización evoluciona, descubre las maneras de adaptarse al mercado, la competencia, las leyes y otros cambios en su entorno externo. También llega a comprender las formas de organizarse internamente –tanto formal (según el diagrama de la organización) como informal (la manera en que realmente se hace el trabajo). Estas maneras se convierten en la norma de la organización; se convierte en su cultura.

ISS Desafío Cultural

Varias realidades culturales afectan la capacidad de la organización para asegurar sus sistemas de información y la información sensible que contienen:

- **El ISS es un chico nuevo en el barrio**. En la mayoría de las organizaciones la función del ISS no existe desde hace tanto tiempo como otros departamentos. Este campo en sí sólo se remonta a 1970.[46]
- **El ISS dista mucho de ser lo principal de la organización.** Incluso cuando existen requerimientos legales para los controles de la seguridad de la información, estos son impulsados por la alta gerencia, sólo porque son exigidos legalmente. El apoyo de alto nivel para la ISS podría agotarse en un instante si el panorama legal y reglamentario cambiara.
- **Las preocupaciones del ISS parecen desconectadas de las de marketing, ventas, operaciones y financieras.** Como resultado, la subcultura del ISS se encuentra subordinada a las otras subculturas más dominantes.

- **“La seguridad de los sistemas de información” contiene la palabra “seguridad”.** La expectativa cultural es que el grupo ISS será, al igual que otras funciones de seguridad, se ocupa de sus propios asuntos sin la necesidad de que otros empleados se involucren.
- **La cultura de Seguridad del ISS toca el resto de la organización principalmente cuando alguien olvida su contraseña o cuando el sistema evita que alguien haga su trabajo.** Excepto por la educación anual de la conciencia, hay pocas oportunidades naturales para fusionar la cultura, llevando a que la subcultura del ISS evolucione en forma aislada de la cultura dominante.

Contra este telón de fondo es que la organización de seguridad de la información debe incrustar su cultura en la más amplia cultura organizacional. Esa es la única manera de transmitir a la organización más grande la forma correcta de percibir, pensar y sentir en relación a los desafíos del ISS. Shein (p.15) señala:

> La cultura y el liderazgo son dos lados de la misma moneda…Si la cultura se convierte en disfuncional, es la única función de liderazgo para percibir los elementos funcionales y disfuncionales de la cultura existente para manejar la evolución cultural y cambiar de tal manera que el grupo pueda sobrevivir en un entorno cambiante.
>
> El liderazgo…es la capacidad de salirse de la cultura…y empezar procesos de cambio evolutivos que son…adaptables. Esta capacidad para percibir las limitaciones de la propia cultura y para desarrollar la cultura adaptativa es la esencia y último desafío del liderazgo.

Este aspecto del liderazgo –para cambiar la cultura más grande en la dirección de la seguridad de la información- es una función crítica para los profesionales de la seguridad. Hasta que la manera de ver el mundo de la seguridad de la información se convierta en parte de la cultura de la organización, la organización es disfuncional. Toda vez que hay una brecha de seguridad cuya causa es humana, proporciona la evidencia de la disfunción.

El ISS ha llegado a entrelazarse para siempre con la práctica del profesional de la seguridad física. Los profesionales de la seguridad deben examinar la cultura de sus organizaciones desde fuera, moldeando y dando forma a su evolución, de modo que con el tiempo los empleados hagan lo correcto: sean cuidadosos, pongan atención, e incluso se capaciten entre sí – todo debido a que una mentalidad de seguridad de la información se ha incrustado en la cultura más grande.

ANEXO A

RECURSOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Organizaciones relacionadas con el ISS

ASIS International. ASIS proporciona numerosos recursos relacionados con el ISS, incluyendo una red de miembros; el Information Resources Center; la revista *Security Management*, junto con ediciones en línea diarias y semanales; y el Information Technology Security Council, http://www.asisonline.org.

Center for Internet Security (CIS). CIS es un líder en métricas de seguridad de la información y proporciona directrices de endurecimiento para garantizar que los sistemas están configurados adecuadamente. Ofrece servicios gratuitos y de pago, http://cisecurity.org.

Community Emergency Response Team (CERT). Este programa de la Carnegie Mellon University proporciona una amplia gama de recursos para abordar los problemas de seguridad de la información, http://www.cert.org.

Computer Security Institute (CSI). CSI es quizás más conocido por sus dos conferencias anuales y su encuesta anual de delitos informáticos y de seguridad, publicado en conjunto con el FBI, http://www.gocsi.com

Information Systems Audit and Control Association (ISAC). Esta organización, que se focaliza en auditorías y controles, tiene 86.000 miembros repartidos a través de 160 capítulos en todo el mundo, http://isaca.org.

Information Systems Security Association (ISSA). ISSA, la organización preeminente para profesionales de la seguridad de la información, es una organización internacional, sin fines de lucro que promueve la educación y defensa. ISSA tiene 142 capítulos y 10.000 miembros en 70 países en todo el mundo, https://www.issa.org.

InfraGard. Esta colaboración del sector privado del FBI proporciona numerosos recursos de seguridad de la información, http://www.infragard.net.

The National Institute of Standards and Technology (NIST). NIST es una agencia federal no reguladora del gobierno de Estados Unidos dentro del U.S. Department of Commerce. Su misión es promover la innovación estadounidense y la competitividad de la industria a través de los avances de la ciencia de las mediciones, los estándares y la tecnología. NIST ofrece mucha orientación en seguridad de la información, y su sitio Web lista muchas organizaciones profesionales de seguridad de la información, http://www.nist.gov.

Open Web Application Security Project (OWASP). Este es un recurso relacionado con temas de la seguridad de las aplicaciones Web, http://www.owasp.org.

Privacy Rights Clearinghouse (PRC). Esta, sin fines de lucro, proporciona información a los consumidores y defensa de los intereses del consumidor y es una fuente de datos de violación a la divulgación, http://www.privacyrights.org.

Secunia. Esta es una fuente muy útil para parches y vulnerabilidades, http://secunia.com.

System Administration, Networking, and Security Institute (SANS). Este es uno de los repositorios preeminentes de capacitación y conocimientos en la industria de la seguridad de la información. Ofrece programas de capacitación de muy buena reputación y también controla el Internet Storm Center (http://isc.scans.org), el cual es conocido por su actualización diaria mediante voluntarios administradores de incidentes, http://www.sans.org.

Certificaciones en Seguridad de la Información
Certified Information Security Manager (CISM) and Certified Information Security Auditor (CISA). Estas certificaciones provienen de ISACA, http://www.isaca.org.

Certified Information Systems Security Practitioner (CISSP). Esta certificación de la International Information System Security Certification Consortium es considerada el estándar de oro, https://www.isc2.org.

Global Information Assurance Certification (GIAC). Esta certificación está disponible en varias especialidades del ISS, http:///www.giac.org.

Una lista de certificaciones de ISS se puede encontrar en https://www.issa.org.

Recomendaciones de Seguridad de los Sistemas de Información y Blogs Técnicos
CERT Coordination Center/Carnegie Mellon University, http://www.cert.org/

Google Online Security Blog, http://googleonlinesecurity.blogspot.com/

Microsoft Malware Protection Center: Threat Research & Response Blog, http://blogs.technet.com/mmpc/default.aspx.

SANS Internet Storm Center, http://isc.sans.org

US CERT, http://www.uscert.gov

Blogs No Técnicos del ISS

CitadelOnSecurity. CitadelOnSecurity ofrece noticias y perspectiva sobre el mundo del cibercrimen. Las categorías incluyen empresas en riesgo, leyes y reglamentos, seguridad de los sistemas financieros, redes sociales, seguridad nacional, y gestión de vulnerabilidades, http://blog.citadel-information.com.

KrebsOnSecurity. Brian Krebs es un ex reportero del *Washington Post* cuya área incluía los delitos informáticos. El blog publica una serie de temas recurrentes, incluyendo las investigaciones del crimen

online, las últimas amenazas, actualizaciones de seguridad, violaciones de datos y, de vez en cuando, justicia cibernética, http://www.krebsonsecurity.com/

Schneier on Security. Bruce Schneier es un técnico en seguridad internacionalmente reconocido y autor, descrito por *The Economist* como un gurú de la seguridad, http://www.sheneier.com.

Nuevo Marco Jurídico

Leyes Federales y Reglamentos de Estados Unidos

Federal Trade Commission, Standards for Safeguarding Customer Information, 16 CFR 314

Health Insurance Portability and Accountability Act, 45 CFR 160 & 164

Privacy and Consumer Financial Information, 12 CFR 40 Sarbanes-Oxley Act of 2002, Public Law 107-204, Section 404

California Civil Code

Breach Disclosure Law, California Civil Code 1798.80-84

California Office of Privacy Protection. (2008). *California business privacy handbook*. http://www.privacy.ca.gov/ business/ca_business_privacy_hb.pdf

Otras Referencias Legales

Braun, R., & Stahl, S. (2005). Un estándar mínimo emergente del debido cuidado de la seguridad de la información. In H. Tipton and M. Krause (Eds.), *Information security management handbook* (6th ed.). Boca Raton, FL: Publicaciones Auerbach.

Braun, R., & Stahl, S. (2006, March). Un estándar mínimo emergente del debido cuidado de la seguridad de la información, *Privacy and Data Security Law Journal*.

Cook, W. (2004, June). Secretos (comerciales) abiertos: CSO Online. Disponible en: http://www.csoonline.com/article/219313/open-trade-secrets [2010, December 5].

Gestión de la Seguridad de la Información

Mesa Redonda. (2004) Asegurando el ciberespacio: Mesa redonda empresarial del marco para el futuro. Disponible en: http://citadel-information.com/library/2/securing-cyberspace-business-roundtables-framework-for-future-040520.pdf [2010, December 5].

ISACA. (2001). Gobernanza de la seguridad de la información: Guía para juntas de directores y gerencia ejecutiva, 2ª ed. Rolling Meadows, IL: ISACA, 2001.

National Cyber Security Summit Task Force. (2004) Informe de la Corporate Governance Task Force: Gobernanza de la seguridad de la información: Un llamado a la acción. National Cyber Security Partnership. Disponible en: http://citadel-information.com/library/2/infosec-governance-national-cybersecurity-partnership-040412.pdf [2010, December 5].

Directrices de Gestión, Estándares y Prácticas de ISS

Tecnología de la Información –técnicas de seguridad- código de prácticas para la gestión de la seguridad de la información, ISO 17799. (2000). Ginebra: International Organization for Standardization.

PCI Security Standards Council. (2010). *Payment Card Industry (PCI) data security standard*. Disponible en: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf [2010, December 5].
Publicaciones del National Institute of Standards & Technology:

Bowen, P., Hash, J. & Wilson, M. (2006). *Information security handbook: A guide for managers*. Special Publication 800-100. Gaithersburg, MD: NIST.

Grance, T., Hash, J., Peck, S., Smith, J., & Korow-Diks, K. (2002). *Security guide for interconnecting information technology systems*. Special Publication 800-47. Gaithersburg, MD: NIST.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response*. Special Publication 800-86. Gaithersburg, MD: NIST.

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management*. Special Publication 800-92. Gaithersburg, MD: NIST.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2008). *Security considerations in the information system development life cycle*. Special Publication 800-64. Gaithersburg, MD: NIST.

Kuhn, D., Walsh, T., & Fries, S. (2005). *Security considerations for voice over IP systems*. Special Publication 800-58. Gaithersburg, MD: NIST.

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling*. Special Publication 800-83. Gaithersburg, MD: NIST.

Scarfone, K., Grance, T., & Masone, K. (2008). *Computer security incident handling guide*, Special Publication 800-61. Gaithersburg, MD: NIST.

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention (IDP) systems*. Special Publication 800-94. Gaithersburg, MD: NIST.

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program.* Special Publication 800-50. Gaithersburg, MD: NIST.
Especificación para el sistema de gestión de seguridad de la información. En ISO 2700. (2005).

Requisitos de tecnología de la información –técnicas de seguridad - sistemas de gestión de la seguridad de la información. Ginebra: International Organization for Standardization.

Guías de Configuración de la Tecnología

Microsoft Corporation. (2009). *Windows Server 2003 security guide*. Disponible en: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8A2643C1-0685-4D89-B655-521EA6C7B4DB [2010, December 5]

National Security Agency. Múltiples guías disponibles en: http://www.nsa.gov.

Encuestas de Delitos en Sistemas Informáticos y de Seguridad

Annual CSI Computer Crime and Security Survey. http://gocsi.com

REFERENCIAS

Borodkin, M. (2001). Computer incident response team. SANS Institute. Available: http://www.sans.org/reading_room/whitepapers/incident/computer-incident-response-team_641 [2010, December 5].

CERT. (2006). Action list for developing a computer security incident response team (CSIRT). Available:http://www.cert.org/csirts/action_list.html [2010, December 5].

Citadel Information Group. (2009, September 23). Company sues bank after $588,000 stolen by cyberthieves. Citadel on Security. Available: http://citadelonsecurity.blogspot.com/2009/09/another-corporate-victim-of-cybertheft.html [2010, December 5].

Citadel Information Group. (2009, December 7). La. firm sues Capital One after losing thousands in online bank fraud. Citadel on Security. Available: http://citadelonsecurity.blogspot.com/2009/12/la-firm-sues-capital-one-after-losing.html [2010,December 5].

Cordeiro, B. (2010, January 8). UPDATE 2-Heartland in $60 mln settlement with Visa, shares rise. Reuters. http://www.reuters.com/article/idUSSGE6070I920100108.

Court to notify Countrywide customers about a class action settlement involving the theft of personal and financial data. (2010, April 12). PR Newswire. Available: http://www.prnewswire.com/news-releases/court-to-notify-countrywide-customers-about-a-class-action-settlement-involving-the-theft-of-personal-and-financial-data-90601539.html [2010, December 5].

Gilbert, F. (2008, February). Hot issues in cyberspace: Critical information privacy and security issues. *The Practical Lawyer*. Available: http://www.itlawgroup.com/resources/articles/139-marketing-and-sales.html [2010, December 5].

Gregg, M. (2009). *CISSP exam cram*. New York, NY: Pearson Publishing.

Heartland to pay up to $2.4 million to settle cardholder class action suit. (2009, December 21). DataBreaches.net. Available: http://www.databreaches.net/?p=8991 [2010, December 5].

ISACA. (2001). Information Security *Governance: Guidance for Boards of Directors and Executive Management,* 2nd ed. Rolling Meadows, IL: ISACA, 2001.

ISO 27001. (2005). Information technology—security techniques—information security management systems—requirements.

ISO 27002. (2005). Information technology—security techniques—code of practice for information security management.

Krebs, B. (2010). Cyber crooks leave traditional bank robbers in the dust. Krebs on Security. Available:

http://krebsonsecurity.com/2010/03/cyber-crooks-leave-bank-robbers-in-the-dust [2010, December 5].

Krebs, B. (2010). Texas bank sues customer hit by $800,000 cyber heist. Krebs on Security. Available: http://krebsonsecurity.com/2010/01/texas-bank-sues-customer-hit-by-800000-cyber-heist[2010, December 5].

Krebs, B. (2010). Victim asks Capital One, 'Who's in your wallet?' Krebs on Security. Available: http://krebsonsecurity.com/2010/03/another-la-e-banking-victim-suing-capital-one/#more-700 [2010, December 5].

Kurzweil, R., *The Age of Spiritual Machines*, Viking Penguin, 1999.

Lam, D., Pease, K., Stahl, S., & Takamine, K. (2007, July). Creating the information security village. *ISSA Journal*.

Mills, E. (2009, December 10). Heartland data breach lawsuit dismissed. CNET News. Available: http://news.cnet.com/8301-1009_3-10413194-83.html [2010, December 5].

O'Brien, K. (2009, December 28). Cellphone encryption code is divulged. *New York Times*.

Organisation for Economic Co-operation and Development. (2002). *OECD guidelines for the security of information systems and networks—Towards a culture of security*. Paris: OECD. Available: http://www.oecd.org/dataoecd/16/22/15582260.pdf [2010, December 5].

PCI Security Standards Council. (2010). *Payment card industry (PCI) data security standard.* Available: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf [2010, December 5].

Quigley, F., & Stahl, S. (1987). *Fundamental elements of information security.* TRW internal report.

Reed, D. (2003). Applying the OSI Seven Layer Network Model to information security. NIST. Available: http://www.isd.mel.nist.gov/projects/processcontrol/members/minutes/7-Sep-2004/OSI.pdf [2010, December 5].

SANS. (2006). Extranet policy. Available: http://www.sans.org/security-resources/policies/Extranet_Policy.doc [2010, December 5].

Scarfone, K., Grance, T., & Masone, K. (2008). *Computer security incident handling guide*. Gaithersburg, MD: National Institute of Standards and Technology.

Schein, E. (1992). *Organizational culture and leadership* (2nd ed.). San Francisco, CA: Jossey-Bass.

Stahl, S. (2006). Beyond information security awareness training: It's time to change the culture. In H. Tipton and M. Krause (Eds.), *Information Security Management Handbook* (3rd ed.). Boca Raton, FL: Auerbach Publications.

Turing, A. (1936-7). On computable numbers, with an application to the *Entscheidungsproblem*. *Proceedings of the London Mathematical Society*, Ser 2, vol. 42, pp. 230-265; corrections, ibid, vol 43, pp. 544-46.

U.S. Department of Commerce. (2000). Safe harbor privacy principals. Available: http://www.export.gov/safeharbor/eg_main _018247.asp [2010, December 6].

Wright, R. (2000). *Nonzero: the logic of human destiny.* New York, NY: Vintage.

Wu, S. (2010). Trends in state security and privacy laws and regulations. In *Privacy and Data Security Law Institute*. New York, NY: Practising Law Institute.

Zetter, K. (2009, September 4). Court Allows Woman to Sue Bank for Lax Security After $26,000 Stolen by Hacker. Wired (on-line). Available: http://www.wired.com/threatlevel/2009/09/citizens-financial-sued [2010, December 5].

CAPÍTULO 4
DESAFÍOS EN CONVERGENCIA DE LA SEGURIDAD

Según una definición, la convergencia es (Tyson, 2007, p.4)

> la integración, de manera formal, colaborativa y estratégica, de los recursos de seguridad acumulativos de la organización, con el fin de beneficiar a toda la empresa a través de la mitigación del riesgo, el aumento de la eficiencia y la efectividad operacional y del ahorro de costos.

La convergencia de la seguridad puede, efectivamente, incrementar la mitigación del riesgo, pero también puede aumentar el riesgo organizacional total. Esta sección examina los desafíos de la convergencia presentando en primer lugar dos ejemplos comunes (cámaras y sistema de control de acceso). Luego se describe cómo un sistema integral de gestión de la seguridad de la información (ISMS) puede ser el elemento "formal, colaborativo y estratégico" que se requiere para mitigar el riesgo.

4.1 RIESGO PARA LA RED

Cuando los profesionales de seguridad física ponen tecnología de seguridad física en la red, abren la puerta a importantes riesgos de seguridad basados en la red. Por ejemplo, todas las siguientes materias de interés para el profesional de seguridad de los sistemas de información (ISS) también pueden debilitar la seguridad física:

- **Denegación de servicios** (DOS por sus siglas en inglés): capacidad de un individuo malintencionado para detener el funcionamiento de un sistema informático
- **Inserción de datos inexactos:** agregar datos incorrectos en una base de datos o archivo
- **Robo de datos:** robar datos desde un sistema
- **Modificación de Datos:** cambiar datos o información en un sistema
- **Destrucción de Datos:** destruir datos en un sistemas

Los principios del ISS se centran en tres elementos básicos: confidencialidad, integridad y disponibilidad, también denominada tríada CIA. Estos principios aplican a los temas mencionados

anteriormente de la siguiente manera:

- **Denegación de servicios (DOS)**: disponibilidad
- **Inserción de datos inexactos:** integridad
- **Robo de datos:** confidencialidad
- **Modificación de Datos:** integridad
- **Destrucción de Datos:** disponibilidad

Para hacer frente a los riesgos de seguridad provocados por la convergencia, los profesionales de seguridad física deben ser capaces de clasificar el riesgo del ISS conforme a la tríada CIA. Este enfoque ayuda a evaluar rápidamente los tipos de riesgos que se enfrentan y luego aplicar las estrategias adecuadas para mitigar esos riesgos.

4.1.1 ESTUDIO DE CASO DE RED: SISTEMA DE CÁMARAS

Un sistema de video vigilancia moderno depende en gran medida de las redes, como se muestra en la Figura 4-1.

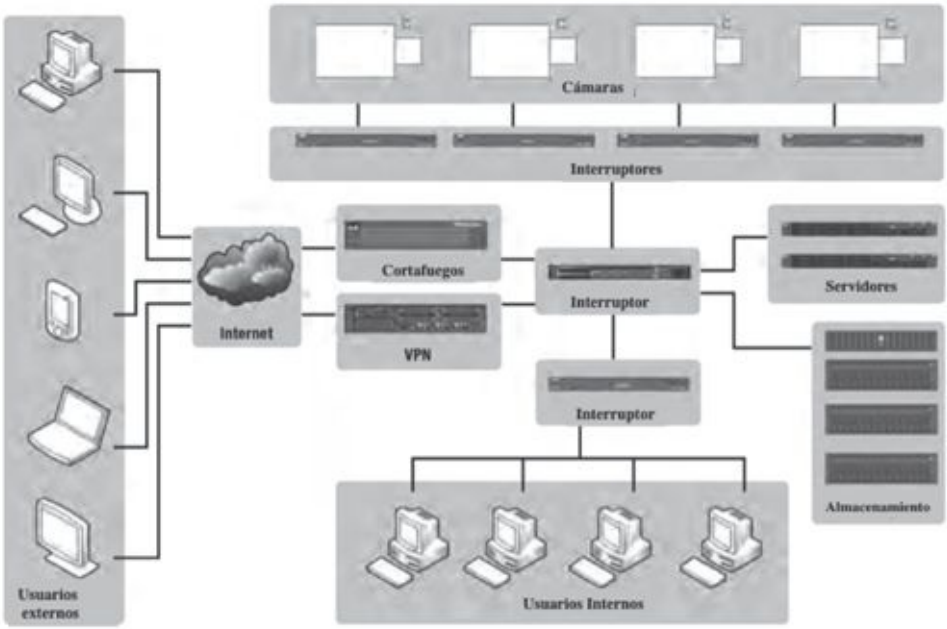


Figura 4-1
Sistema de Video Conectado a una Red

El lado izquierdo de la Figura 4-1 muestra a los usuarios externos en Internet que potencialmente podrían conectarse a los sistemas internos de una organización. Esos usuarios son segregados de la red interna mediante un firewall y un dispositivo de red virtual privada (VPN por sus siglas en inglés). En la parte inferior del diagrama están los usuarios internos, que normalmente tienen acceso a los activos de información a través de un switch (interruptor) de red, el dispositivo que une los activos de la red. En la parte superior del diagrama están las cámaras de video, las cuales generalmente están dispersas en toda

la empresa. Todas las cámaras conectan a un switch permitiendo que cada cámara converse con los otros dispositivos de la red. Algunos switches se conectan a otros switches por lo que todos los dispositivos pueden intercambiar información entre ellos.

En el lado derecho del diagrama se muestran los servidores que controlan las cámaras de video. Un servidor registra el video mientras otro proporciona comandos y control para todo el conjunto del sistema de seguridad física. Por debajo de estos dos servidores está el área de almacenamiento de la red, en la cual residen todos los datos.

Los cinco temas de riesgo nombrados anteriormente podrían aplicarse al sistema de video en red de la Figura 4-1 de la siguiente forma:

- **Denegación de servicios (DOS).** Las cámaras de video pueden tener un bloqueador de video para llegar a las estaciones de trabajo de clientes y dispositivos de grabación. Las personas empeñadas en tener acceso no autorizado a la instalación podrían apagar la capacidad de visualización del video.
- **Inserción de datos inexactos**. Se puede insertar datos inexactos en el video grabado, por ejemplo agregando un video inválido entre las secuencias de video válidas. Alguien que robó algo de la instalación podría insertar un video durante ese tiempo que mostrara que allí no había nadie.
- **Robo de datos.** Las secuencias de video podrían ser robadas y utilizadas con malas intenciones. Los ladrones de bancos, por ejemplo, podrían ser capaces de analizar las imágenes de las cámaras para ayudarlos a planificar el robo del banco.
- **Modificación de datos.** Los datos podrían ser modificados mientras el video estuviera en tránsito, interceptando el video correcto y mostrando un video grabado previamente al operador, por ejemplo mientras se comete el delito.
- **Destrucción de datos**. La evidencia de video grabada en un disco duro podría ser borrada, ocultando la evidencia de un robo.

Cada dispositivo en el diagrama se está comunicando en la red y es potencialmente capaz de comunicarse con todos los demás en la red. Los usuarios en la red interna son capaces de intercambiar información con los servidores y de intercambiar información con las cámaras de video. Alguien que pueda intercambiar información con un dispositivo disponible en la red puede tener la capacidad de controlar un elemento de seguridad física o elementos conectados a ella, posiblemente desde cualquier parte del mundo.

4.1.2 ESTUDIO DE CASO DE RED: CONTROL DE ACCESO

Un sistema de control de acceso electrónico plantea a los profesionales de seguridad física matices adicionales importantes. La Figura 4-2 representa una disposición del sistema.

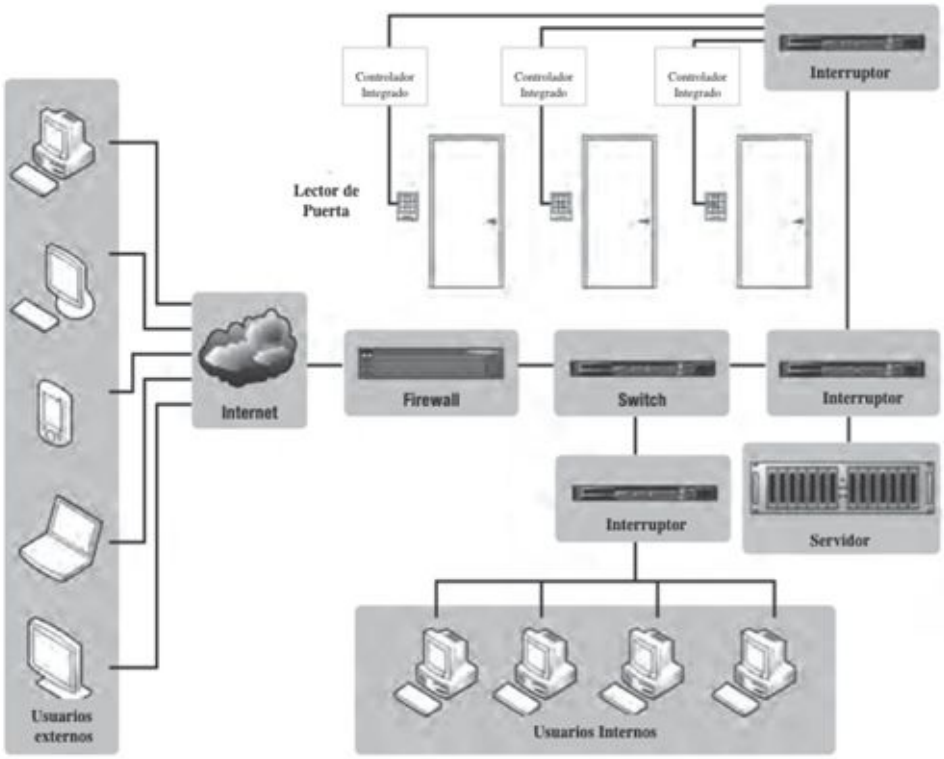


Figura 4-2
Sistema de Control de Acceso Conectado a una Red

La arquitectura de la red es similar a la del sistema de video (Figura 4-1). En la Figura 4-2, los usuarios internos se muestran en la parte inferior, mientras que los usuarios externos están en el lado izquierdo. Los usuarios externos son segregados de los usuarios internos por un dispositivos de seguridad, en este caso un firewall. Todos los elementos de la red están conectado mediante switches (interruptores), incluyendo el servidor de control de acceso, los usuarios y el controlador integrado. El lector de la puerta, también llamado lector de tarjetas, está conectado al controlador integrado, que está conectado a la red.

El lector de tarjetas de control de acceso intercambia infromación directamente con un dispositivo integrado que intercambia información con la red. El controlador integrado decide si alguien puede pasar por esa puerta.

El lector de tarjeta intercambia información con el controlador integrado, el cual intercambia información con la red

Figura 4-3
Comunicación del Sistema de Control de Acceso:
Lector al Controlador a la Red

Alternativamente, un servidor habla directamente a la red. No necesita un intermediario.

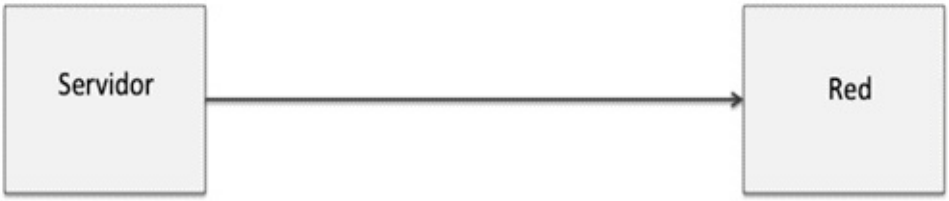


Figura 4-4
Comunicación del Sistema de Control de Acceso:
Servidor a la Red

Los dispositivos de control de acceso en la Figura 4-2 están conectados directamente a la red o conectados a un dispositivo que puede controlarlos, el cual está conectado a la red.

Las computadoras se comunican directamente e indirectamente. Las computadoras se comunican directamente (también llamadas capa 2) cuando pueden verse entre ellas e indirectamente (también llamadas capa 3) cuando necesitan un intermediario. La comunicación directa es como hablar con alguien más en una sala de reuniones. Si John quiere conversar con Mary en esa sala de reuniones, él dice, "¿Mary, puedo hablarte?" Cuando Mary reconoce a John, tienen una conversación. Si John necesitara conversar con alguien fuera de la sala de reuniones, él necesitaría un intermediario –un teléfono que sepa cómo marcar el teléfono de la otra persona y permitir la conversación.

La comunicación directa entre computadoras, que es la comunicación de la capa 2, ocurre de la misma manera. El puesto de trabajo que quiere conversar con el servidor de control de acceso dice, "¿el servidor de control de acceso está disponible para mí para hablar directamente?" En otras palabras, ¿la computadora está en la sala? Si es así, tienen la conversación.

La Figura 4-5 muestra el flujo lógico de comunicación que se lleva a cabo durante una conversación entre un puesto de trabajo y el servidor que maneja toda la información de control de acceso.

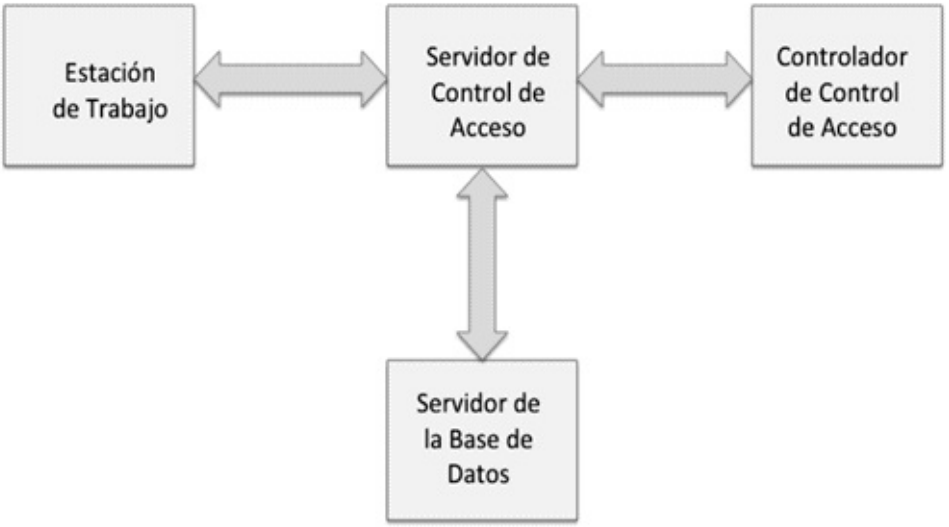


Figura 4-5
Flujo Lógico de Comunicación

El puesto de trabajo, a la izquierda, intercambia información con el servidor de control de acceso. El servidor de control de acceso toma cualquier solicitud que El puesto de trabajo le hace (activar una tarjeta), comunica la solicitud al servidor de la base de datos, y cuando el servidor de la base de datos responde, el servidor de control de acceso envía una comunicación de vuelta a El puesto de trabajo. Todo esto ocurre en conversaciones individuales entre dos computadoras, una después de la otra.

Para que esta conversación suceda directamente, todas las máquinas deben estar en el mismo switch y por lo tanto, capaces de verse unas a otras. La Figura 4-6 muestra los elementos del control de acceso conectados a un switch.

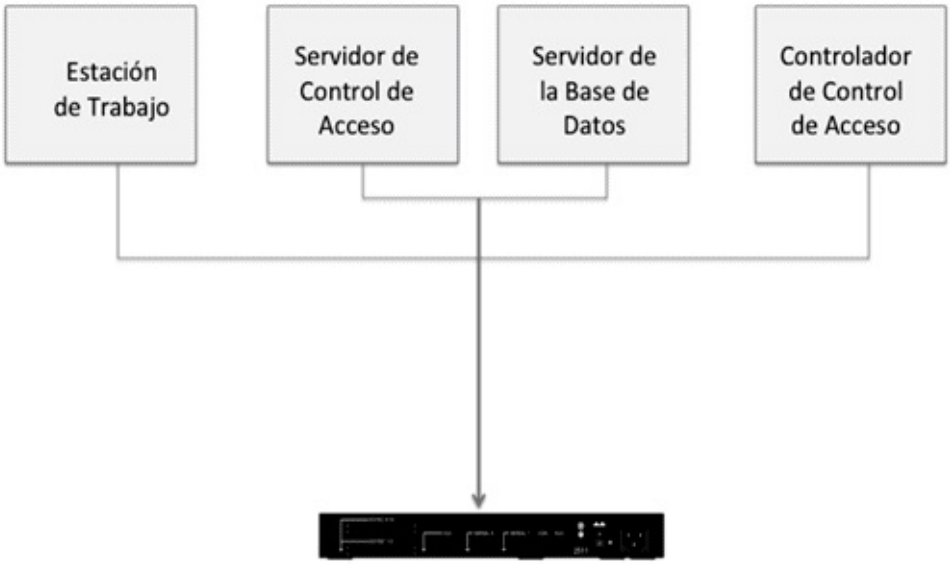


Figura 4-6
Elementos del Control de Acceso Conectados al Switch

En la Figura 4-6, para que El puesto de trabajo se comunique al servidor de control de acceso, necesita enviar una señal al switch, que entonces envía una copia de esa señal al servidor de control de acceso. Por lo general, el switch no enviaría la misma señal al servidor de base de datos, ya que no está destinada al servidor de la base de datos. La Figura 4-7 muestra como se produce dicha comunicación en la capa 2:

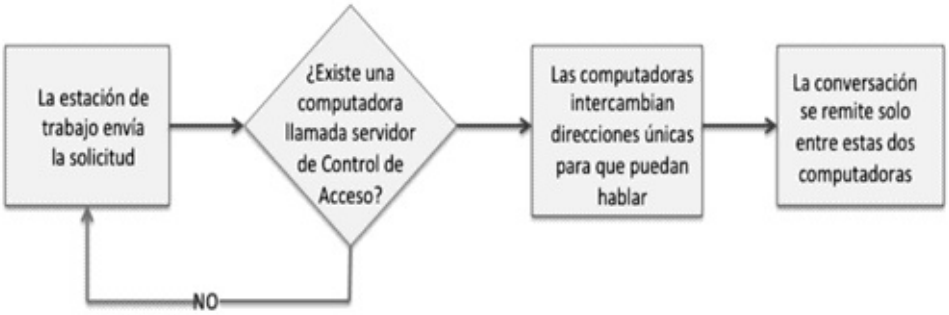


Figura 4-7
Comunicación de la Capa 2

Primero, El puesto de trabajo envía la solicitud para hablar al servidor de control de acceso. Si el servidor de control de acceso puede ser visto por El puesto de trabajo, envía de vuelta una dirección

única en la forma de un reconocimiento para que El puesto de trabajo pueda comunicarse con él.

Volver al ejemplo de la sala de reuniones puede ayudar a explicar el siguiente nivel de la comunicación informática. Si John no puede ver a Mary, él sabe que Mary no está en la sala. Por lo tanto, el levanta el teléfono y la llama. El teléfono es un intermediario que facilita la comunicación. John y Mary están en diferentes habitaciones, diferentes ciudades o diferentes países. En el ejemplo de la computadora, si dos computadoras no pueden verse entre ellas directamente, están en redes separadas y debe usar un router (enrutador) como un intermediario para comunicarse entre ellas.

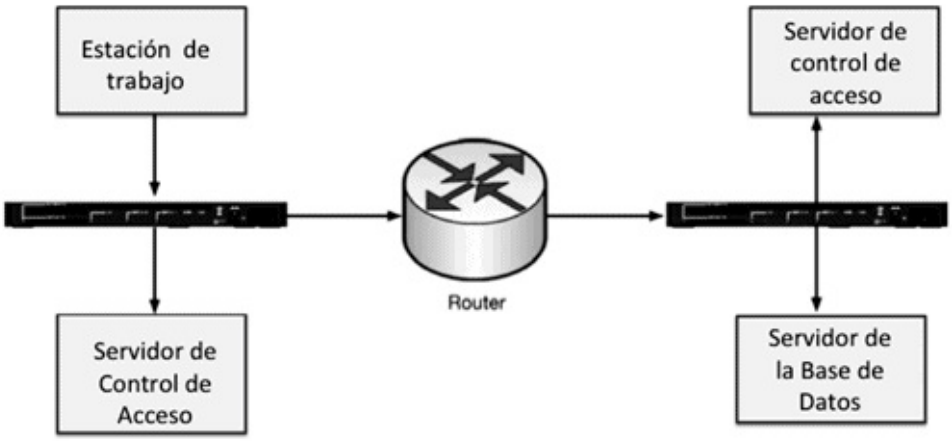


Figura 4-8
Comunicación de Control de Acceso mediante Router

Tal como muestra la Figura 4-8, si El puesto de trabajo quiere intercambiar información con el controlador del control de acceso, puede hacerlo sólo porque El puesto de trabajo puede ver al controlador del control de acceso. Está en el mismo switch (análogo a esta en la misma sala de reuniones). Para comunicarse con el servidor de control de acceso, no obstante, El puesto de trabajo primero comienza por ver si el servidor de control de acceso está en la misma red. Si no, le pregunta al router si puede llegar hasta el servidor de control de acceso. Si el router puede redirigirlo, lo hace.

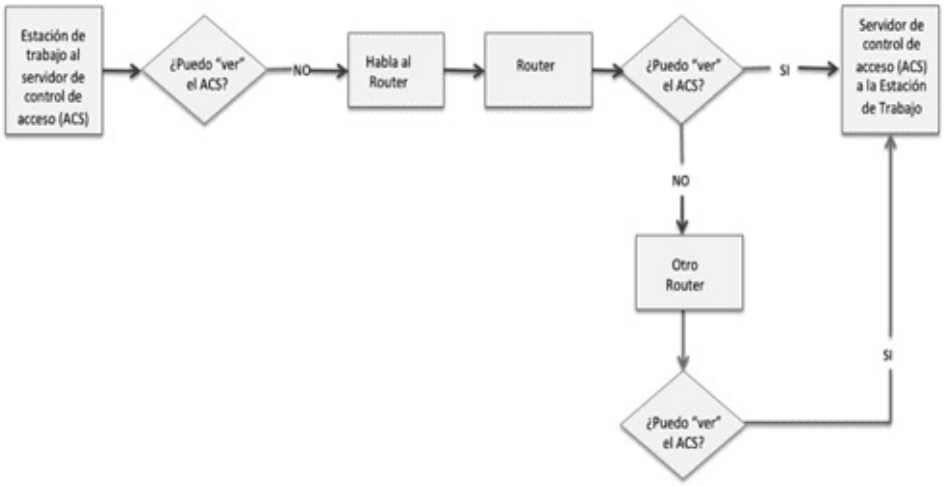


Figura 4-9
Flujo de Datos del El puesto de trabajo al Servidor de Control de Acceso

La comunicación de la capa 3 es el mecanismo que permite a las computadoras interactuar a través de

Internet en todo el mundo. Hay poca diferencia entre el diagrama de la Figura 4-9 y lo que sucede cada día en Internet. En un paradigma convergente, las computadoras y los activos físicos de seguridad son potencialmente accesibles desde todo el mundo –y por lo tanto- vulnerables.

Estas reglas de las comunicaciones aplican a todos los elementos que operan en la red. Todo dispositivo conectado a la red es accesible para cualquier otro conectado a la red.

Los cinco temas de riesgo mencionados anteriormente podrían aplicarse al sistema de control de acceso en red de la Figura 4-2 de la siguiente manera:

- **Denegación de servicio (DOS).** Un ataque de DOS podría impedir a una organización la actualización de su servidor de control de acceso.
- **Inserción de datos inexactos.** La inserción de un registro inexacto podría dar acceso a una persona no autorizada a la instalación física. Un grupo terrorista podría entrar en una computadora disponible de la red, y luego otorgar acceso a una tarjeta no autorizada de modo que su grupo podría ingresar al centro de envío de la instalación.
- **Robo de datos.** Alguien podría robar los registros de una compañía y averiguar con quién, con ingeniería social, obtener una credencial. Por ejemplo, alguien podría averiguar el nombre de un empleado con el acceso apropiado al edificio, encontrarse con el empleado en un bar, y subrepticiamente copiar la credencial del empleado.
- **Modificación de datos.** Alguien podría modificar un registro y otorgarse acceso dónde no lo tiene. Una vulnerabilidad del sistema podría hacer que el sistema de acceso esté disponible en la red. Por ejemplo, un empleado podría obtener acceso a una zona inapropiada de un banco aprovechando la vulnerabilidad del sistema y modificando sus registros para obtener un permiso de acceso adicional sin autorización.
- **Destrucción de datos**. Alguien podría destruir el rastro de su acceso a un área en particular de la compañía. Por ejemplo, después de acceder a un área sensible donde se almacenan los valores de comprobación, un empleado interno podría destruir el rastro de auditoría que mostraba que estuvo allí.

Los dos ejemplo –un sistema de video y un sistema de control de acceso- ilustran que cuando los dispositivos de seguridad física se colocan en la red corporativa, el profesional de seguridad debe manejar el aumento de un conjunto de riesgos. La siguiente sección analiza la variedad de tipos de ataques contra los sistemas de seguridad de la red.

4.2 ATAQUES DE COMUNICACIÓN

Una vez que los sistemas de seguridad se comunican sobre la red, son susceptibles al ataque. Estos ataques pueden provenir de múltiples vectores. Aquí se presentan algunas de las posibilidades:

Ingeniería social:	Alguien convence a un usuario que comparta sus credenciales para entrar en la red.
Hacking directo:	Alguien sigue un sistema, accediendo directamente en él a través de canales normales o explotando una vulnerabilidad.
Malware:	Alguien ataca un sistema instalando un software en él, ya sea con el conocimiento del usuario (generalmente oculto en otro software o e-mail) o automáticamente, sin conocimiento del usuario.
Ataque a la Web:	Alguna parte de la interfaz Web con el usuario (como buscando en una página Web) permite el acceso al sistema.

4.2.1 INGENIERÍA SOCIAL

La ingeniería social es la manipulación de las personas para conseguir que hagan algo que debilite la seguridad de la red. Una de las formas en que los criminales usan la ingeniería social es convencer a las personas que les den su identificación de usuario y contraseñas.

En el caso de un sistema de grabación de video, algunos usuarios son capaces de acceder al sistema. Generalmente, necesita entrar un nombre de usuario y contraseña (en muchos casos, el mismo que utilizan para acceder a la red). Muchas empresas también hacen que el software esté disponible desde ubicaciones remotas, en Internet. Ciertamente, es conveniente para un número de personas tener la posibilidad de acceder al video en cualquier momento, sin importar su ubicación.

Sin embargo, sin controles adecuados, el software de grabación de video podría verse comprometido. En un ataque común de ingeniería social, el hacker llama, simula ser del departamento de TI, y le dice al usuario que le diga su contraseña para poder arreglar el sistema. Si el usuario no está educado en forma apropiada (o es una persona amable por naturaleza) dará su nombre de usuario y contraseña. El intruso ahora puede acceder fácilmente al sistema de grabación.

Un sistema de control de acceso podría ejecutarse en un servidor Web en Internet (“cloud computing”), o en su lugar podría ejecutar en un servidor interno. De cualquier modo, un hacker podría obtener acceso al servidor de control de acceso utilizando las credenciales de ingeniería social. Una vez dentro, el podría crear su propia credencial o quizás incluso abrir una puerta.

4.2.2 HACKING DIRECTO

En un ataque de piratería informática (hacking) directo, un hacker trabaja con herramientas bajo su control para obtener el acceso a la red. La analogía con la seguridad física para esto es el ladrón de bancos que hace túneles en una bóveda para robar el dinero. Él está directamente involucrado en el crimen. Del mismo modo, el hacker necesita identificar qué defensas existen y luego derrotarlas.

Mientras menos defensas existan, más fácilmente puede el hacker comprometer el sistema.

Con respecto al software de grabación de video, los hackers suelen empezar comprobando un sitio Web fácilmente accesible. Si pueden robar la contraseña mediante la ingeniería social, lo harán.

Si no, podrían utilizar un crackeador (adivinador) de contraseñas de fuerza bruta que les permita intentar muchas contraseñas muy rápidamente. Sin embargo, muchos sistemas ahora tienen herramientas para bloquear los hackers después de intentar demasiadas contraseñas.

A continuación, los hackers buscan las vulnerabilidades (fallas del programa que permiten a las personas hacer cosas que no debieran). Por lo general, usan herramientas gratis automatizadas para aprovechar esas vulnerabilidades. En el caso de un servidor que ejecuta un sistema de grabación de video, un hacker podría aprovechar un error desconocido o no reparado en el sistema para obtener el acceso a la máquina y crearse una cuenta o cambiar una contraseña.

En algunos casos, un sistema actualizado, incluso uno totalmente “patched” (parchado), puede llegar a ser vulnerable. Un ingeniero podría configurar el sistema de forma incorrecta o cometer un error de arquitectura, como enchufar un servidor interno en un switch que es accesible a través de Internet.

Las consecuencias son idénticas a las de la ingeniería social. Con acceso total a un sistema, un hacker puede hacer cualquier cosa que un administrador del sistema pueda hacer, es decir, todo.

4.2.3 MALWARE

Uno de los más insidiosos mecanismos que los hackers utilizan hoy en día para atacar sistemas es el malware (programa maligno). El malware –virus, worm (gusano), spyware (programa espía), rootkit[47], troyano, etc.- está diseñado para dar al cibercriminal o hacker el control de la computadora en la cual está instalado. El malware a menudo elude las medidas preventivas. Entre las razones se encuentran:

- El software antivirus no se mantiene actualizado
- Usuarios inexpertos abren correos y archivos caza bobos (booby-trapped) o visitan sitios caza bobos en Internet
- Los administradores del sistema permiten a los usuarios instalar software en el escritorio

El malware puede instalarse, ya sea como parte de otro software, automáticamente cuando se abre un correo electrónico y mediante varios otros métodos. Es particularmente insidioso, porque sus diseñadores lo programan para ser principalmente silencioso. En los primeros días de la piratería, los hackers querían hacer una declaración –querían que las personas supieran que se habían apoderado de la máquina. Ahora, muchos hackers están interesados solamente en ganar dinero. Mientras más tiempo pueden permanecer sigilosos, apropiándose de los sistemas de una organización y robando su información, más pueden obtener.

La primera cosa que un hacker necesita es acceso al sistema. Normalmente hay dos tipos de mecanismos para obtener acceso con un malware. Un ataque general se centra en obtener acceso a cualquier sistema que podría dar al hacker acceso a un sistema; un ataque focalizado se dirige a una persona específica y toma medidas como pasar información a un intruso o permitiendo el control remoto del sistema.

Las estaciones de trabajo dentro de la red generalmente están protegidas por un firewall y VPN, de modo que no parezcan ser inmediatamente accesibles. Sin embargo, los usuarios pueden recibir malware en una serie de formas: desde un e-mail, descargando una parte del software, o a través de un ataque basado en la Web. Una vez que el malware ha sido descargado en una computadora, puede conceder el control remoto a un hacker o realizar cualquier cosa que esté programado para hacer.

Una vez que un criminal ha tomado control de El puesto de trabajo de un usuario, especialmente si captura las contraseñas de usuario, puede hacer todo lo que el usuario puede hacer, incluyendo tomar el control del sistema de seguridad física.

4.2.4 ATAQUES A LA WEB

Los ataques a la Web pueden centrarse en los clientes (estaciones de trabajo de los usuarios, por ejemplo) o en los servidores (obtienen acceso directo no autorizado a los recursos e información del sistema). Un ataque a la Web es particularmente peligroso, debido a que puede derrotar casi todos los controles.

Con respecto a los ataques a los clientes, cuando los usuarios están accediendo a la Web, pueden tomar el malware simplemente yendo a un sitio Web comprometido. Una serie de sitios, algunos de ellos de grandes marcas, han sido comprometidos con malware en el pasado. Por ejemplo, en el 2010, un código maligno fue añadido a los sitios alojados por Network Solutions (Krebs, 2010).

Una vez que un usuario va a un sitio Web en el que se ha insertado un malware, el malware podría ser descargado en la computadora del usuario incluso si el usuario no hace click en ninguna parte (porque un navegador Web ejecuta el código en la página Web automáticamente).

Los hackers también atacan los sitios Web para obtener información de las personas que visitan esos sitios. El Proyecto de Seguridad de Aplicaciones Web Abiertas (Web Application Security Project) (http://www.owasp.org) publica periódicamente una lista de los 10 ataques top a la Web. Los siguientes son los tipos de defectos encontrados comúnmente en los sitios Web, permitiendo a los hackers el acceso o control no autorizado:

Injection (Inyección)
Las fallas de inyección, particularmente inyección de Lenguaje de Consulta Estructurado (SQL por sus siglas en inglés), son comunes en las aplicaciones Web. La inyección permite a un atacante ejecutar un comando directamente en una base de datos contrario a los derechos de acceso permitido. Los usuarios generalmente sólo pueden ingresar datos, no comandos. Un ataque de inyección SQL ocurre cuando un

hacker es capaz de enviar la entrada a un servidor a través de un campo de formulario o URL que le da al servidor una instrucción para devolver información que no debiera devolver.

Cross-site scripting (XSS) (Secuencia de Comandos entre sitios)
Un error de secuencia de comandos entre sitios Web permite a un atacante ejecutar un código maligno desde un segundo sitio Web (controlado por el cibercriminal) en el navegador de la persona que está viendo el primer sitio Web. Este código malicioso puede hacer cualquier cosa para la cual el cibercriminal lo haya programado, incluyendo la instalación de un troyano en la computadora del usuario.

Broken authentication and sesión management (Autenticación interrumpida y gestión de sesión)
Esta clase de vulnerabilidades permite a los cibercriminales comprometer las contraseñas, claves, o dispositivos de autenticación (token) para asumir la identidad de un usuario legítimo.

Insecure direct object references (Referencias a objetos inseguros directos)
El no prohibir el acceso directo a "objetos" internos –archivos, directorios, programas, etc.- en un servidor Web puede llevar a uso ilegítimo del servidor.

Cross-site request forgery (CSFR) (Falsificación de solicitud entre sitios)
La falsificación de solicitud entre sitios es un ataque en el cual el navegador de la víctima es engañado para emitir un comando a una aplicación Web vulnerable. A diferencia del cross-site scripting (XSS), el cual aprovecha la confianza que un usuario tiene por un sitio en particular, la CSFR aprovecha la confianza que el sitio tiene en el navegador de un usuario.

Security misconfiguration (Mala configuración de seguridad) Cuando un servidor Web o aplicación no está configurado de acuerdo a requerimientos de seguridad apropiados, entonces es sujeto de ataques y peligros que afectan la confidencialidad, integridad y disponibilidad.

Insecure cryptographic storage (Almacenamiento criptográfico inseguro)
Las claves criptográficas y otros elementos de criptografía deben ser almacenados en forma segura de modo que no puedan ser comprometidos. (Fue un almacenamiento criptográfico inseguro la vulnerabilidad que llevó a TJ MAXX a la pérdida de 34 millones de tarjetas de crédito).

Failure to restrict URL Access (No restringir el acceso al URL)
Si bien los sitios Web a menudo tienen subpáginas que no se muestran a los usuarios sin derechos de acceso (páginas de administrador, por ejemplo), si no se restringe el acceso al URL, un cibercriminal puede escribir la URL sospechosa directamente en la barra del navegador URL, obteniendo por lo tanto, un acceso ilegítimo a las páginas.

Insufficient transport layer Protection (Insuficiente protección de la capa de transporte)
Los sitios Web que no protegen los datos en tránsito con Secure Sockets Layer (SSL) o con Transport Layer Security (TLS) son vulnerables a la interceptación y modificación del tráfico.

Unvalidated redirects and forwards (redirecciones y reenvíos inválidos)

Las aplicaciones Web a menudo redirigen y reenvían a los usuarios a otros sitios y páginas. Un redireccionamiento y reenvío debe ser validado por el servidor antes de ser ejecutado. Si el redireccionamiento y reenvío no es validado por el servidor, entonces un cibercriminal puede comprometer la redirección o reenvío previsto hacia sitios de phishing o malware o usando reenvíos para acceder a páginas no autorizadas.

Muchas organizaciones utilizan plataformas de aplicaciones Web, usando una interfaz de servidor Web que ejecuta el software al que se accede a través de un navegador Web. En la interfaz de la Web, después que los usuarios inician sesión, pueden interactuar con la aplicación. Por ejemplo, un usuario podría acceder a un registro de acceso para hacer modificaciones. En un código mal escrito, esa consulta podría ser una parte del URL- por ejemplo, http://www.yourcompany.com/query.asp?employeeid=5551111.

Si el software no está escrito en forma segura, poniendo datos incorrectos en la consulta (por ejemplo, http://www.yourcomany.com/query.asp?employeeid=999999'99) podría divulgar si es posible obtener más información. Si el servidor y la aplicación son configurados en forma inadecuada, pueden devolver un conjunto de mensajes de error. Examinando los mensajes de error, un hacker podría crear comandos apropiados para la siguiente consulta, la cual podría verse así:

> www.yourcompany.com/query.asp?employeeid=99999999'%20or%201=1--

Dependiendo de la base de datos y de la aplicación, esta consulta podría decirle a la base de datos que devuelva los registros incorrectos del empleado o más registros a los cuales el hacker no debería tener acceso. Un comando enviado a la base de datos podría divulgar los contenidos de la base de datos, destruyéndolos, o tomar el control del servidor.

Los profesionales de la seguridad deben examinar si sus sistemas son susceptibles de tales ataques, averiguar cómo arreglar el código (en forma interna o con un proveedor), y si se pueden poner controles de mitigación en el medio.

4.3 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los profesionales de la seguridad física mitigan los riesgos a través de las políticas, referencias y marcos. Los profesionales de ISS mitigan los riesgos a través de los sistemas de gestión de la seguridad de la información (ISMS), como el que describe la norma IDO 27001 y 27002).

Como señalan los autores que escriben en *ISSA Journal* (Lam, Pease, Stahl & Takamine, 2007):

> En el mundo actual, todo el mundo está en riesgo de un delito informático. Y, nos llevará a todos reducir el riesgo a niveles aceptables. La seguridad de los sistemas de información ya no involucra simplemente a aquellos que trabajan en el campo como profesionales.

Los profesionales de la seguridad pueden contribuir a la gestión del riesgo y a las perspectivas de seguridad para los esfuerzos de protección.

Según la ISO 27001, los siguientes son elementos esenciales de un ISMS:

- la existencia de un sistema de gestión de la seguridad de la información (ISMS)
- la adecuación de cualquier sistema en el lugar para la organización
- permanente identificación y gestión del riesgo
- incorporación de los controles adecuados en el ISMS
- apropiada supervisión, revisión, mantención y mejora del ISMS
- adecuada responsabilidad de gestión
- auditoría interna o revisión
- revisión de la gestión del ISMS

El primer trabajo de la persona encargada del ISS de la organización es crear un ISMS adecuado al tamaño de la organización. Si la ISO ISMS no se adapta bien, uno puede encontrar buenos modelos de ISS online para empresas pequeñas.

La evaluación de riesgos continua, hace posible identificar cualquier riesgo nuevo y planificar los controles o contramedidas. Este es un proceso común en seguridad física; en ISS es un proceso más fluido, ya que los riesgos cambian significativamente y continuamente. Los controles apropiados deben existir desde el inicio y luego actualizados constantemente para enfrentar el cambiante panorama. Por ejemplo, un firewall podría haber sido suficiente control hace 20 años, pero ya no es así.

Debe existir una responsabilidad de gestión adecuada para el ISMS en cada organización. Esto generalmente significa asignar el rol de oficial jefe de seguridad de la información (CISO por sus siglas en inglés) a una persona, de preferencia a tiempo completo. Para fortalecer la cultura de ISS de la organización, la alta gerencia debe apoyar el proceso. En realidad, la gerencia debiera esta preocupada por el ISS. Por ejemplo, al CEO se le podría entregar un informe trimestral del ISS. Además, la alta gerencia debe asignar funciones de auditoría interna para asegurarse que el ISMS está haciendo lo que necesita hacer. El CISO podría informar directamente al comité de auditoría.

Es fundamental para el profesional de seguridad física colaborar con el departamento de ISS para garantizar que la seguridad física es un buen socio del ISS y cumple con las políticas y procedimientos.

La norma ISO 27002 (p.4) enumera los siguientes elementos como fundamentales para el éxito de un ISMS:

- política de seguridad
- organización del ISS
- gestión de activos
- seguridad de recursos humanos
- seguridad física y ambiental
- gestión de las comunicaciones y operaciones

- control de acceso
- adquisición, desarrollo y mantención de los sistemas de información
- gestión de incidentes de seguridad de la información
- gestión de continuidad del negocio
- cumplimiento

4.3.1 POLÍTICA DE SEGURIDAD

Sin una política, es difícil decirle a la gente lo que deben hacer para estar seguros. La creación de una política de seguridad es, por lo general, una función multidisciplinaria y multidepartamental. La participación de seguridad física es fundamental por dos razones. Primero, la política de ISS afecta las operaciones de seguridad física cotidiana (la interacción del personal con las computadoras y las conexiones de los dispositivos de seguridad a la red y la interacción con la red). Segundo, la política de ISS define qué tipo de dispositivos están permitidos en la red. Algunos dispositivos de seguridad física no son maduros desde una perspectiva de ISS; la participación en la creación y actualización de la política de ISS puede ayudar a garantizar que se han abordado las preocupaciones de la seguridad física y se han seleccionado los elementos de seguridad física adecuados.

4.3.2 ORGANIZACIÓN DEL ISS

Algunos elementos de la organización del ISS son familiares a los profesionales de la seguridad física, tales como contactos con las fuerzas del orden y los grupos con intereses particulares. Algunos problemas específicos del ISS incluyen el acceso al sistema y la revisión por terceros.

Respecto a la video vigilancia, un profesional de la seguridad podría querer un proveedor para configurar las cámaras. Para intercambiar información con esas cámaras, el proveedor puede necesitar acceso a la red de la organización. Para lograr ese acceso, el proveedor probablemente necesita autenticación, lo que significa que el proveedor necesita credenciales. La autenticación también puede ser necesaria para el hardware de seguridad física real. Si la organización terceriza la gestión del sistema de video, las políticas del ISMS aplican también al proveedor.

Asimismo, en la medida en que la nube informática se convierte en prevalente (permitiendo a terceros acceder a la información o sistemas de una organización), los proveedores de la nube deben adherir a las políticas de la organización, y los profesionales de la seguridad física deben asegurarse que esos proveedores cumplen. En la mayoría de los casos, antes que un tercero pueda tener acceso a los datos de una organización, debe pasar por un proceso de investigación. Ese proceso debe garantizar que su ISMS es adecuado para la información que está siendo compartida y que el cliente será capaz de auditar al proveedor en el futuro.

4.3.3 GESTIÓN DE ACTIVOS

Esto se refiere a los requerimientos especiales para la información que es transmitida en la red y almacenada en dispositivos que residen en la red. Alguna información relacionada con seguridad física puede requerir un manejo especial. Un video podría contener contenido altamente sensible que necesite ser especialmente protegido. Un sistema de control de acceso contiene las claves para las puertas de una organización y deben existir controles especiales para garantizar que no se vea comprometida.

4.3.4 GESTIÓN DE RECURSOS HUMANOS

Las necesarias verificaciones de antecedentes, las condiciones de la selección para el empleo, la conciencia y educación en materia de seguridad, procesos disciplinarios y prácticas de terminación en el contexto de ISMS son similares a los que los profesionales de seguridad física ya conocen. Debido a que los profesionales de seguridad física tienen una comprensión madura de la gestión de recursos humanos, pueden contribuir mucho en este ámbito.

4.3.5 SEGURIDAD FÍSICA Y AMBIENTAL

En esta materia, claramente, el profesional de seguridad física puede y debe ofrecer su experiencia para ayudar al profesional de ISS. La capacidad para asegurar las áreas en las cuales residen los activos de ISS es fundamental para la protección de esos activos. Asimismo, dañaría la organización si un servidor de control de acceso o de grabación de video fuera robado. A medida que se incrementa la colaboración entre la seguridad física y lógica, se producirán mejores soluciones para todos los involucrados.

4.3.6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

La gestión de las comunicaciones y operaciones se ocupa de muchos asuntos que deben ser abordados desde una perspectiva de seguridad (ISO 27002, pp.37-59):

- encendido del sistema computarizado
- apagado del sistema computarizado
- procedimientos de apagado de emergencia
- gestión del cambio
- segregación de funciones
- prestación de servicios de terceros
- gestión de la capacidad
- gestión del sistema
- aceptación del sistema

- protección de códigos maliciosos
- sistema de respaldo
- controles de seguridad de red
- manejo de medios de comunicación
- seguridad de la documentación del sistema
- intercambio de información
- transacciones en línea
- supervisión
- sincronización del reloj

Encendido, Apagado y Procedimiento de Apagado de Emergencia del Sistema Informático

Los sistemas computarizados pueden tomar un tiempo inesperadamente largo para encender y apagar. En los antiguos sistemas de video vigilancia, después de que un apagón fuera restaurado, las cámaras de video se encenderían rápidamente y se conectarían a través de un cable coaxial al grabador. En el caso de una falla de un sistema moderno, un determinado número de sistemas pueden necesitar encender en un cierto orden, incluyendo los servidores, las áreas de almacenamiento de redes y las conexiones a Internet. Esos sistemas pueden necesitar esperar por energía una determinada cantidad de tiempo (para que un generador cargue las baterías en un sistema de alimentación ininterrumpido) o puede enfrentar ciertas fallas que no estaban consideradas previamente. Los profesionales de seguridad física se benefician al comprender estas limitaciones y planificarlas.

Del mismo modo, los sistemas computarizados pueden tomar mucho más tiempo en apagarse. La repetición (reinicio) de un sistema en caso de un problema podría representar importantes problemas, tales como dejar abajo el sistema de video de una organización durante el reinicio.

Otras emergencias pueden forzar el apagado de un sistema. Una fuga de agua, por ejemplo, puede requerir que toda una sala de equipos computacionales se cierre. Aunque en un entorno análogo uno podría haber sido capaz simplemente de mover el grabador de video digital (DVR por sus siglas en inglés) a otra ubicación, no es posible llevar fuera una sala completa de servidores, especialmente si hay varios sistemas involucrados en la operación del sistema de video. Una solución es tener otra sala de servidores disponible en una ubicación diferente para hacerse cargo de las operaciones de grabación de esas cámaras.

Gestión del Cambio

La gestión del cambio es fundamental para TI, y puede afectar seriamente las operaciones de seguridad física. Por ejemplo, las unidades de seguridad física no pueden simplemente actualizar sus sistemas de control de acceso sin tener un intercambio de información con TI. Un cambio puede afectar toda la red. La actualización de una cámara de video, por ejemplo, podría causar un tormenta de difusión en la red

debido a una falla en la cámara, provocando no sólo que esa cámara de video, sino que también otros sistemas dejen de funcionar.

Por el contrario, los departamentos de TI deben trabajar con los profesionales de seguridad física para asegurarse que los cambios hechos en la red no perjudiquen los activos de seguridad física. Por ejemplo, una actualización a un sistema operativo del servidor puede impedir que el software del servidor de control de acceso funcione correctamente.

Segregación de Funciones

La segregación de funciones también es familiar para muchos profesionales de seguridad física. En el contexto de TI, es importante entender que algunos de los sistemas al cual los profesionales de seguridad física tienen acceso son altamente sensibles. En un sistema de control de acceso, los usuarios pueden crear sus propias credenciales para acceder prácticamente a cualquier área de la compañía. Sin una separación de funciones, la misma persona que tiene acceso a crear las tarjetas de control de acceso podría ser la misma persona que está patrullando un edificio y no debe ingresar con acceso no autorizado.

Prestación de Servicios de Terceros

Desde una perspectiva operacional, debido a que terceras partes pueden ahora prestar servicios, todos los acuerdos de nivel de servicio existentes para los proveedores internos también deben ser para las terceras partes. Los sistemas críticos son críticos independiente de quién los provea. Por ejemplo, a un proveedor externo de video se le debe exigir tener suficiente ancho de banda para mostrar los videos de una organización 24 horas al día. Los profesionales de ISS pueden ayudar a garantizar que la organización está protegida con los acuerdos de nivel del servicio.

Gestión de la Capacidad

En un ambiente moderno de video, un video normal puede fluir a una soEl puesto de trabajo. En una emergencia, un importante número de personas pueden necesitar ver el video, incluyendo a través de Internet. Si estas preocupaciones operacionales no se expresan con antelación, la amplitud de banda necesaria no existirá. Desde una perspectiva de seguridad, la A^{48} en CIA sería violada, en la medida que el sistema no estaría disponible haciéndola inútil en ese momento.

Gestión de Sistemas

Los sistemas que se ejecutan en las computadoras tienen necesidades específicas que no eran necesariamente críticas cuando eran sistemas integrados. Por ejemplo, los sistemas ahora necesitan ser parchados para solucionar problemas con el software. Esto puede significar que un sistema en particular puede quedar temporalmente fuera de servicio. El profesional de la seguridad física debe considerar si a un activo (como una cámara fundamental) se le puede permitir que quede fuera de funcionamiento. Si no, debería haber una forma de mantener esa cámara en funcionamiento, o podría ser posible instalar un reemplazo temporal. En algunos casos, puede ser conveniente tener muchas cámaras enfocadas en un solo lugar para garantizar que el nuevo paradigma no se interpone en los elementos operacionales críticos del

sistema.

Aceptación del Sistema

La aceptación del sistema es el proceso de asegurarse de que los sistemas estén acorde a las especificaciones. Es un proceso útil para los usuarios finales (la gente que realmente usa el producto), pero también es una exigencia para el personal del ISS garantizar que los sistemas que se ejecutan en la red no van a poner en peligro la red u otros dispositivos conectados a ella. Los profesionales de la seguridad física deben estar preparados para pasar el proceso de aceptación para asegurarse que están obteniendo lo que ellos quieren y que el sistema es seguro para la red.

Protección de Código Malicioso

Los virus, troyanos y otros códigos maliciosos, pueden dejar inoperables los sistemas y toda una red. En el caso de control de acceso, no colocar un antivirus u otro software de protección del host en la máquina que ejecuta el sistema podría dejarlo susceptible a ser comprometido o de fallar. Peor aún, esa máquina podría echar abajo toda la red. Los sistemas de seguridad física necesitan tener protección para esos ataques, y esas protecciones requieren ser actualizadas.

Respaldo del Sistema

Las computadoras son máquinas con partes en movimiento y en ocasiones pueden fallar. Si no se ha hecho copia de seguridad de los datos, se pueden perder. Una organización podría tener un requisito de cumplimiento para conservar un video por un cierto período de tiempo, por lo que necesita respaldar esa información en caso de falla del hardware o del sistema. Respecto al software de control de acceso, si la información no es respaldada y se pierde, es posible que sea reconfigurada a mano, volviendo inoperativo el sistema por un periodo, provocando una denegación de servicio y probablemente los costos de reparación de un consultor.

Controles de Seguridad de la Red

Los sistemas de seguridad necesitan cumplir con determinados tipos de tecnologías y controles. Por ejemplo, un DVR que no está diseñado correctamente podría no tener la seguridad adecuada para estar en la red. Además, si las cámaras no son ".1x compatible", es posible que no se puedan conectar a la red en forma segura.

Manejo de los Medios de Comunicación

La información puede existir en diversos medios, tales como los discos duros, memorias USB o cintas de respaldo. Los profesionales de la seguridad deben considerar la importancia de la información y lo que pueden hacer para protegerla, tanto de ser perdida como de verse comprometida. Por ejemplo, sería desastroso si alguien robara una unidad USB que contiene un importante video para una investigación en desarrollo.

Seguridad de la Documentación del Sistema

Una necesidad fundamental es la importancia de proteger la documentación del sistema. Si los hackers obtienen la documentación de un software de control de acceso de la organización, pueden ser capaces de descubrir cómo crear y agregar tarjetas de proximidad no autorizadas. Si saben cómo opera el sistema de cámaras de video de una organización, pueden ser capaces de ver tanto los videos grabados como en vivo para averiguar la manera de comprometer la instalación.

Intercambio de Información

A menudo es útil intercambiar información con las fuerzas de respuestas primaria. Sin embargo, pueden no estar totalmente conscientes de las implicaciones de acceder a los datos de una organización en Internet. Una empresa podría querer que la policía local tenga acceso a sus videos en el caso de un ataque terrorista, pero no querría compartir con ellos inapropiadamente las credenciales de inicio de sesión. Las personas que tienen acceso a los sistemas de una organización deben ser capacitadas en las políticas de seguridad para que no pongan en peligro el sistema.

Transacciones En Línea

Si una compañía proporciona servicios en línea o transacciones comerciales electrónicas, debe aplicar los correspondientes estándares, políticas y procedimientos de la industria, así como el cumplimiento de todas las leyes y reglamentos pertinentes. Muchas compañías han sido sancionadas por no tener adecuados sistemas de gestión del ISS o políticas durante la realización de comercio electrónico.

Supervisión

Así como los profesionales de seguridad física supervisan los perímetros de los edificios, los profesionales de ISS supervisan diversos aspectos de la red y sus sistemas, revisando los registros (asegurándose que los cortafuegos no estén siendo atacados) y revisando las máquinas (asegurándose que no estén en peligro).

Sincronización del Reloj

Una práctica notable del ISS es la sincronización del reloj. Esto por lo general se hace con un protocolo llamado Network Time Protocol (NTP) y permite que todos los sistemas en la red tengan la misma hora. Cuando se correlacionan eventos en la red, ya sea una intrusión de seguridad física, un ataque a la red o incluso ajustar la hora en el sistema de video vigilancia, con el objetivo de dejar evidencias, es importante que todos los elementos registren la misma hora.

4.3.7 CONTROL DE ACCESO

Los sistemas de seguridad que residen en una red, como los sistemas de control de video vigilancia y de acceso físico, requieren un control de acceso lógico de algún tipo. Un mecanismo de nombre de usuario/contraseña puede no ser suficiente dado la sensibilidad y criticidad de la información almacenada en el sistema. Los profesionales de seguridad física deben analizar este tema con los especialistas de ISS de modo que los datos de seguridad sean tratados como fundamentales.

El control de acceso también es un concepto familiar para el profesional de la seguridad física. La idea es dejar entrar sólo a aquellas personas que están autorizadas, después de una adecuada identificación. En seguridad física, esto es hecho normalmente con un oficial de seguridad, una clave o una tarjeta de acceso.

Debido a que en la actualidad alguien puede acceder a los sistemas de la empresa desde cualquier parte del mundo, la verificación de la identidad es vital. Por ejemplo, un proveedor de seguridad física puede querer que el video esté disponible en Internet. Sin embargo, las políticas de ISS corporativas prohíben el acceso a la información confidencial sin la utilización del segundo factor de autenticación. El segundo factor de autenticación utiliza algo como una contraseña única o un escáner de huella dactilar para que sea mucho más difícil que alguien ingrese al sistema.

Esta situación hace más compleja la selección de un proveedor, debido a que el proveedor de servicios preferido puede no ofrecer un segundo factor de autenticación. El proveedor puede ser bueno desde una perspectiva de seguridad física y malo desde una perspectiva del ISS. El profesional de la seguridad física debe trabajar con los expertos de ISS para tomar una decisión apropiada.

Otro tema es que el servidor de control de acceso que desea el departamento de seguridad para instalar en la red puede ejecutar un sistema operativo que no adhiere a la política corporativa de seguridad. Puede ser incapaz de autenticar debidamente a los usuarios, dejando el sistema susceptible a ataques, o puede ser un sistema operativo antiguo, no actualizado, con vulnerabilidades sin parches.

4.3.8 ADQUISICIÓN, DESARROLLO Y MANTENCIÓN DE LOS SISTEMAS DE INFORMACIÓN

Cuando una operación de seguridad adquiere nuevos sistemas, desarrolla nuevos software o actualiza los sistemas existentes, debe asegurarse que ninguna de esas acciones expongan a la organización a riesgos indebidos o creen un problema en alguna parte de la tríada CIA: confidencialidad, integridad o disponibilidad.

Respecto a las cámaras de video, por ejemplo, el profesional de la seguridad debe asegurarse que la grabación de video muestra lo que realmente está sucediendo y las vistas de las cámaras estén todo el tiempo disponibles. Más aun, es importante encriptar la transmisión de video y garantizar que cada vez que las credenciales pasen entre un puesto de trabajo y el dispositivo, no puedan ser fácilmente robadas de la red. De lo contrario, la organización puede enfrentar uno de esos problemas familiares: denegación de servicios, inserción de datos inexactos, robo, modificación y destrucción de información.

4.3.9 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

En cuanto a la gestión de incidentes de seguridad de la información, los profesionales de seguridad física pueden ser de ayuda, ya que tienen una práctica a gran escala en el manejo de incidentes. Los examinadores forenses, que a menudo son fundamentales para el proceso de respuesta a incidentes, a

menudo también provienen del ámbito de la seguridad física.

Los profesionales de seguridad física pueden estar especialmente interesados en los aspectos legales de la gestión de incidentes de seguridad de la información, específicamente respecto a las evidencias de una computadora, servidor o pista de red incautado.

4.3.10 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

En la medida que la continuidad del negocio está planificada, existen numerosas áreas de participación para el profesional de la seguridad física.

Primero, los activos de tecnología de seguridad física requeridos para la operación tienen que ser capaces de continuar funcionando en el evento de un incidente inesperado. Por ejemplo, TI debe seguir proporcionando servicios de video vigilancia a los departamentos de seguridad física, de modo que ellos puedan mantener la seguridad. Si la información (imágenes, videos de datos de control de acceso) no están disponibles porque no fueron planificados adecuadamente para un estado de emergencia, entonces la empresa puede verse comprometida cuando más se necesiten estas herramientas. En el caso de que no haya energía, es importante que los sistemas basados en la red, tales como el control de acceso, mantengan la funcionalidad.

Segundo, el personal aún tiene que estar disponible en caso de una emergencia. El personal de seguridad física generalmente es muy versado en el cuidado de estos tipos de necesidades logísticas, tales como la forma de albergar una gran cantidad de personas por un largo período. De este modo, la activa participación del profesional de seguridad física puede ser una ayuda fundamental para los profesionales de ISS.

Tercero, puede ser necesario un lugar fuera de la instalación como parte del plan de continuidad del negocio. Si es así, el personal de seguridad física puede trabajar con el personas de ISS y el personal de TI puede estar tranquilo de que el lugar es seguro, está disponible y es capaz de albergar al personal.

4.3.11 CUMPLIMIENTO

Algunos problemas de cumplimiento afectan directamente a la seguridad física y al ISS. En primer lugar, algunas decisiones de seguridad pueden no ser negociables desde una perspectiva legal. Por ejemplo, ciertas organizaciones gubernamentales deben tener un nivel de control de acceso específico en el lugar. Las organizaciones bajo la jurisdicción de la ley Sarbanes-Oxley (SOX) deben cumplir otros requerimientos para estar en conformidad.

Es fundamental para el profesional de seguridad física entender muy bien este aspecto de la política de seguridad, para que no ponga otros sistemas en riesgo o tenga la posibilidad de que sus propios sistemas fallen de manera que provoquen que la empresa quede fuera de cumplimiento.

4.3.12 RESUMEN DEL ISMS

Esta revisión de los elementos de un ISMS analizó numerosas intersecciones donde el profesional de la seguridad física y el profesional de ISS pueden beneficiarse trabajando juntos. Muchos ejemplos se han proporcionado para mostrar la forma en que ISS es fundamental para asegurar los activos de seguridad física en un entorno convergente. Al mismo tiempo, los elementos vulnerables de la seguridad física pueden debilitar el ISS. Comprendiendo el ISMS y trabajando dentro de su marco junto al ISS, los profesionales de la seguridad física pueden los obtener beneficios de la convergencia en tanto que reduce los riesgos.

4.4 CONCLUSIÓN

En la medida que las organizaciones siguen el proceso de convergencia con el fin de aprovechar los beneficios de incorporar los sistemas de seguridad en la infraestructura de la red, la seguridad de los activos físicos se entrelaza con la seguridad de los sistemas de información. Las inseguridades en la convergencia de los sistemas físicos e informáticos amplían el portafolio de riesgos contra los cuales el profesional de la seguridad física debe responder. Ellos necesitan un flujo de datos protegidos, ya sea que el flujo sea un cable de punto a punto o vaya a través de la red.

La convergencia en seguridad destaca la importancia de unir el paradigma de la seguridad física, el punto de vista del profesional de la seguridad física, al de la contraparte de los profesionales de la seguridad de los sistemas de información, el paradigma de la seguridad lógica. Para hacer frente al nuevo desafío, los profesionales de seguridad física deben (Lam & Stahl, 2010)

> aumentar su Paradigma de Seguridad Física con un nuevo Paradigma de Seguridad Lógica adecuado para enfrentar los únicos, nunca antes vistos, desafíos de la seguridad de los sistemas de información.

Los profesionales de la seguridad física deben intercambiar información con sus colegas de ISS, comprender los problemas del ISS y el paradigma de la seguridad lógica que impregna ese trabajo y compartir el paradigma de la seguridad física con el personal de ISS. La alta gerencia, también, puede jugar un rol en la integración de los paradigmas de seguridad física y lógica en una organización.

REFERENCIAS

ISO 27001. (2005). *Information technology—security techniques— information security management systems—requirements*. Geneva, Switzerland: International Organisation for Standardization.

ISO 27002. (2005). *Information technology—security techniques— code of practice for information security management*. Geneva, Switzerland: International Organisation for Standardization.

Krebs, B. (2010). Network Solutions again under siege. Krebs on Security. Available: http://krebsonsecurity.com/2010/04/network-solutions-again-under-siege [2010, December 5].

Lam, D., Pease, K., Stahl, S., & Takamine, K. (2007, July). Creating the information security village. *ISSA Journal*.

Lam, D., & Stahl, S. (2010, January). Convergence, paradigm shifts and reaching the village. *ISSA Journal*.

Tyson, D. (2007). *Security convergence: Managing enterprise security risk*. Burlington, MA: Butterworth-Heinemann.

[1] Nota del Traductor: el término en general se utiliza para referirse a la investigación de empresas o personas. No existe una traducción oficial, las más comunes son “debida diligencia”, “auditoría”, o se mantiene el uso del término en inglés, el cual se utilizará en este trabajo de traducción.

[2] Para más información sobre las regulaciones de la información automatizada, ver la *Regulatory Compliance Planning Guide* en http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/defaul mfr=true.

[3] Nota del Traductor: en la ley de patentes de U.S.A., reducción a la práctica (reduction to practice) es un concepto que significa la realización y prueba del invento.

[4] Nota del Traductor: conocida también en Latinoamérica como “La Gran Estafa”.

[5] N. del T.: a pesar de no estar reconocido por el Diccionario de la lengua española (RAE), en este trabajo de traducción se utilizará el término por ser de uso masivo.

[6] Este segundo ejemplo es un código limpio utilizado en una prueba de penetración para obtener números de seguro social y otra información confidencial de una supuesta base de datos segura.

[7] Los cross-site scripting realizados en los sitios Web representaron más del 80% de las vulnerabilidades de seguridad documentadas en la segunda mitad del 2007

[8] Malcolm Gladwell data el inicio de la revolución de la microcomputadora en enero de 1975, cuando “la revista *Popular Electronics* lanzó un reportaje sobre una máquina extraordinaria llamada Altair 8800” Gladwell, 2008, p.63)

[9] Códigos Civiles de California 1798.29, 1798.82, y 1798.84.

[0] N del T: estafas por suplantación de identidad

[1] N del T: aféresis de robot, programa informático que imita el comportamiento humano.

[2] N. del T: anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez.

[3] N. del T: tipo de malware que ayuda a encontrar datos personales examinando la memoria RAM.

[4] N. del T: ocultar la propia identidad o falsificar la de otro usuario

[5] N. del T: varias computadoras infectadas con software malicioso

[6] N. del T: CIA corresponde al acrónimo confidentiality, integrity and availability.

[7] Esta definición combina las definiciones del Committee on National Security Systems Instruction (CNSSI) 4009, el SANS Institute (SysAdmin, Audit, Network, Security) y RFC2828 (Glosario de Seguridad de Internet). La CNSSI 4009 define “amenaza” como “cualquier circunstancia o acontecimiento con el potencial para afectar adversamente un sistema de información mediante el acceso no autorizado, destrucción, divulgación, modificación de datos y/o denegación del servicio”. SANS y RFC2828 define “amenaza” en forma más o menos análoga como “potencial de violación de

la seguridad, la cual existe cuando hay una circunstancia, capacidad, acción o evento que podría violar la seguridad y causar daño". La diferencia principal es que CNSSI 4009 es más explícita respecto al significado de "violación de la seguridad" y "causar daño".

[8] Esta definición de vulnerabilidad es una amalgama de la CNSSI4009 y la RFC2828. La CNSSI4009 define "vulnerabilidad" como cualquier "debilidad en el IS, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados". La RFC2828 define "vulnerabilidad" como un "defecto o debilidad en el diseño, implementación u operación y gestión que podría ser explotada para violar la política de seguridad del sistema".

[9] Esta definición es del SANS Institute, muy conocido en la comunidad de la seguridad de los sistemas de información por el manejo del Internet Storm Center y por la calidad de sus programas de capacitación. La CNSII4009 define "riesgo de la seguridad de los sistemas de información" como la "posibilidad de que una amenaza en particular impacte adversamente un IS mediante la explotación de una vulnerabilidad en particular". Una variación común es incluir la cantidad de pérdida en la definición de riesgo. Por ejemplo, la RFC2828 define "riesgo de la seguridad de los sistemas de información" como la "expectativa de pérdida expresada como la posibilidad de que una amenaza en particular explote una vulnerabilidad en particular con un resultado de daño en particular".

[0] La CNSSI4009 define una "contramedida" como una "acción, dispositivo, procedimiento, técnica u otra medida que reduce la vulnerabilidad de un sistema de información". La RFC2828 la define como "una acción, dispositivo, procedimiento o técnica que reduce una amenaza, vulnerabilidad o ataque eliminándolo o evitándolo, minimizando el daño que puede causar o descubriéndolo o informándolo de modo que se pueda tomar una acción correctiva.

[1] Esto simplemente es llamado riesgo residual en el National Institute of Standards and Technology's Glossary of Key Information Security Terms, (NISTIR 7298, 2006)

[2] Esta definición integra la definición de riesgo residual del NIST con la definición de la ISO27001:2005 de riesgo residual ("riesgo que queda después que se ha tratado el riesgo") y la de RFC2828 "el riesgo que queda después que las contramedidas han sido aplicadas".

[3] N. del T: "Teletranspórtame Scotty" (frase utilizada por los personajes de la serie de televisión de ciencia ficción Star Trek antes de ser teletransportados).

[4] N. del T: acto de manipular usuarios para conseguir información confidencial

[5] Ver, por ejemplo, Kurzweil (1999) y Wright (2000).

[6] N. del T: back-end es la parte de la aplicación que el usuario no ve. Front-end es la parte de la aplicación orientada al usuario-cliente.

[7] Por ejemplo, una instrucción simple puede decir, "Sume el número N1 en la ubicación de almacenamiento S1 y el número N2 en la ubicación de almacenamiento S2 y ponga la suma en la ubicación de almacenamiento S3". Otra instrucción simple puede decir, "Lea el número N1 en S1 y ejecute la instrucción N1". El programa obtendrá diferentes resultados dependiendo de que el número N1 pase a ser almacenado en S1 en el momento en que se ejecuta la instrucción. Si bien las

instrucciones como esta son muy comunes en los programas –y proporcionan al programador una gran capacidad- ellas también son una fuente de complejidad que se encuentra en el corazón del desafío de seguridad de los sistemas de información.

[8] Más información sobre la tríada en http:///datatracker.ietf.org/wg/aaa (Internet Engineering Task Force).

[9] Un corolario simple del principal resultado del documento de Turing de 1936, es que no hay ningún algoritmo para distinguir entre programa y datos

[0] N. del T: Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago.

[1] N. del T: Se conservarán los nombres en inglés porque corresponde a la denominación de uso masivo de las distintas tecnologías.

[2] N. del T: International Information Systems Security Certification Consortium, conocido como (ISC)[2]

[3] N. del T: Ley de Modernización de Servicios Financieros, más conocida como Ley Gramm-Leach-Bliley (GLBA)

[4] Por ejemplo, la 12 CFR 30 (Office of Comptroller of the Currency); 12 CFR 208, 211, 225, 263 (Board of Governors of the Federal Reserve System); 12 CFR 308, 364 (Federal Deposit Insurance Corporation); 12 CFR 568, 570 (Office of Thrift Supervision); 16 CFR 314 (Federal Trade Commission); y 17 CFR 248 (Securities and Exchange Commission).

[5] Los detalles de cada multa están disponibles en http://www.ftc.gov/opa

[6] Por ejemplo: 12 CFR 41 (Comptroller of the Currency); 12 CFR 222 (Federal Reserve Board); 12 CFR 334 y 364 (Federal Deposit Insurance Corporation); 12 CFR 571 (Office of Thrift Supervision); 12 CFR 717 (National Credit Union Association); y 16 CFR 681 (Federal Trade Commission).

[7] http://www.ftc.gov/privacy/privacyinitiatives/promises.html.

[8] Detalles de todos estos casos están disponibles en http://www.ftc.gov/opa. TJX, así como la información persona de aproximadamente 455.000 consumidores que devolvieron las mercancías a las tiendas. Los bancos han afirmado que decenas de millones de dólares en cargos fraudulentos se han hecho en las tarjetas y millones de tarjetas han sido canceladas y vueltas a emitir.

[9] Los detalles están disponibles en http://www.ftc.gov/opa

[0] Los detalles están disponibles en http://ftc.gov/opa

[1] La National Conference of State Legislatures mantiene una lista de las notificaciones de violaciones a la seguridad estatal, incluyendo vínculos a las leyes estatales, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotific

[2] N. del T: una transferencia ACH (Automatic Clearing House) es una transferencia electrónica de fondos entre bancos y cooperativas de crédito.

[3] La frase proviene de la novela de Lewis Carroll *Through the Looking Glass*, en la cual la Reina Roja le dice a Alicia, “Ahora, aquí, usted ve, es preciso correr mucho, para permanecer en el mismo lugar”.

[4] Véase, por ejemplo, lo siguiente: W.E. Deming en la mejora continua (*The New Economics*, 1994); Igualmente el transcendental libro de Peter Senge en el aprendizaje de organizaciones, *(The Fifth Discipline*, 1990); La explicación de Stan Stahl de la teoría W de Barry Boehm, ("User Involvement in Project Success" en *Information Security Management Handbook* de H. Tipton & M. Krause, 1997); y en las agudas historias de lo que realmente funciona en la línea del frente de Tom Petzinger, (*The New Pioneers*, 1999).

[5] Esta sección se basa en S.Stahl, "Beyond Information Security Awareness Training. It's Time to Change the Culture", en H. Tipton y M. Krause (Eds.), *Information Security Management Handbook* (3ª ed.), Boca Raton, Fl.; Publicaciones Auerbach, 2006.

[6] El origen del campo se puede fijar en la fecha de publicación de *Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security*, editado por W.Ware. Una versión clasificada se publicó en 1970 por la Office of the Secretary of Defense. La Rand Corporation publicó una versión no clasificada en 1979.

[7] N. del T: Herramienta que se oculta a sí misma, u otros programas o procesos, permitiendo un acceso de privilegio continuo no autorizado para obtener información sensible o comandar remotamente una computadora.

[8] N. del T: corresponde a la disponibilidad (availability) de la tríada

ÍNDICE

A

acuerdo de no divulgación, 34, 44, 64, 73
Almacenamiento criptográfico inseguro, 242
almacenamiento de información, 155
amenazas de los sistemas de información, 106
Amenazas Naturales, 24
amenazas virtuales, 134
ANSIR, 20
anti-forense, 109
antivirus, 55, 107, 108, 111, 136, 137, 169, 180, 191, 239, 251
Aplicabilidad, 63
aplicaciones Web, 160, 214, 241, 242, 243
archivos electrónicos, 43
armas nucleares, 20
arquitectura de seguridad, 175
ataque de DOS. *Véase* Denegación de servicios
auditorías, 66, 209, 213

B

barreras, 38
Blogs, 215

C

capacitación, 7, 32, 33, 40, 66, 131, 135, 138, 214
China, 18, 48
cibernética, 107, 109, 122, 123, 124, 133, 216
ciberterrorismo, 133
Clasificación e intercambio de información, 63
computabilidad, 140
comunicaciones informáticas, 144
contraespionaje, 22
Contramedidas de los Sistemas de Información, 131
Contramedidas de Vigilancia Técnica, 54
contraseñas, 55, 57, 58, 104, 136, 137, 154, 155, 160, 179, 191, 237, 238, 240, 241
controlador integrado, 229, 230
controles administrativos, 136, 181, 202
controles físicos, 136
controles técnicos, 136

Convergencia de la Seguridad, 225
cortafuegos, 55, 108, 111, 136, 137, 179, 191, 253
Criptografía, 174
Cuentas Cubiertas, 188

D

Defensa en Profundidad, 34
Demandas Colectivas, 199
Denegación de servicios, 226, 228
desastres naturales, 24, 132
Directiva de Protección de Datos, 179, 195
Due Diligence, 29

E

espías, 18, 20, 133
espionaje industrial, 19, 123

F

Falsificación de solicitud entre sitios, 241
Firma digital, 56
firmware, 70, 143

G

gestión de activos, 110, 173, 245
gestión de incidentes, 65, 173, 245, 255
gestión de la capacidad, 248
gestión de las comunicaciones, 245, 248
Gestión de Vulnerabilidades, 180
gestión del sistema, 246, 248
Gobernanza de la seguridad de la información, 217
gusanos, 18, 115, 169

H

hackers, 25, 127, 143, 147, 198, 238, 239, 240, 252
hardware, 70, 143, 162, 175, 246, 251

I

incidentes de seguridad, 110, 204, 205, 206
información altamente restringida, 70 información periférica, 41

Informes Técnicos, 87
infraestructura de los sistemas de información, 135, 137, 138
Infraestructura de Video, 116
ingeniería reversa, 37
ingeniería social, 134, 135, 197, 236, 237, 238, 239
Inserción de datos inexactos, 226, 228, 235
integridad de la información, 191
intercambio de información, 22, 46, 68, 73, 84, 203, 248, 249

K

Keyloggers, 134
Koobface, 134

L

lector de tarjeta, 117, 118, 230
Ley de Privacidad, 47

M

malware, 104, 107, 108, 109, 110, 123, 125, 134, 170, 204, 218, 239, 240, 242
manejo de medios de comunicación, 248
Máquina de Turing, 140
Modificación de Datos, 226

N

nombre de usuario, 142, 149, 152, 154, 160, 198, 237, 253
nube informática, 159, 246

O

OPSEC, 41

P

PBX, 161, 162, 163, 165
pérdida de información, 30, 59, 60, 87, 89
phishing, 106, 115, 123, 126, 134, 42
PIN, 109
piratería, 22, 28, 29, 106, 143, 238, 239
plan de continuidad del negocio, 40, 174, 256
planificar-hacer-verificar-actuar, 208, 209
Política de protección de activos de información, 62

políticas de seguridad de la información, 113, 203, 210
POTS, 163
privacidad de los empleados, 64
Procedimiento de Apagado de Emergencia, 248
proceso de autorización, 42
Protección de Código Malicioso, 251
protocolo de Internet, 117
Puntos de Entrada Lógica, 149

R

Recursos de TI, 69
red social, 106, 185
Regla de las Banderas Rojas, 178, 187
reputación, 17, 30, 58, 75, 106, 188, 214
requerimientos de seguridad, 29, 208, 242
respaldo, 24, 44, 56, 156, 165, 205, 248, 252
respuesta a incidentes, 204, 205, 206, 255
robo de datos, 104
rootkit, 239
router, 133, 147, 233, 234

S

SANS, 130, 131, 168, 205, 214, 215, 220, 222
Sarbanes-Oxley, 178, 186, 216, 256
sección 404, 186
secreto comercial, 50, 51, 71, 75, 87, 89, 111
segregación de funciones, 248, 250
Seguridad de Aplicaciones, 241
Seguridad de las operaciones. *Véase* OPSEC
seguridad del personal, 38, 202
seguridad nacional, 26, 110, 124, 215
Seisint, 190, 191
sistema operativo, 117, 143, 151, 152, 249, 254
sistemas informáticos, 113, 132, 134, 139, 140, 184, 197
sistemas integrados, 117, 121, 166, 251
spyware, 115, 123, 134, 239

T

TCP/IP, 117, 121, 122, 144
tecnología de la información, 62, 104, 204, 218

Tecnologías de seguridad de la información, 169
tríada AAA, 153, 174
tríada CIA, 153, 226, 254
troyano, 134, 239, 241
TSCM, 54

U

URL, 104, 241, 242, 243

V

VOIP, 163, 164, 165, 166
VPN, 158, 227, 240

W

WAF, 170
WLAN, 56

X

XSS, 241, 242

Z

Zeus, 104, 134

1625 Prince Street
Alexandria, VA 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org