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

[32] N. del T: International Information Systems Security Certification Consortium, conocido como (ISC)[2]

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

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:

---

[43] 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".

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).

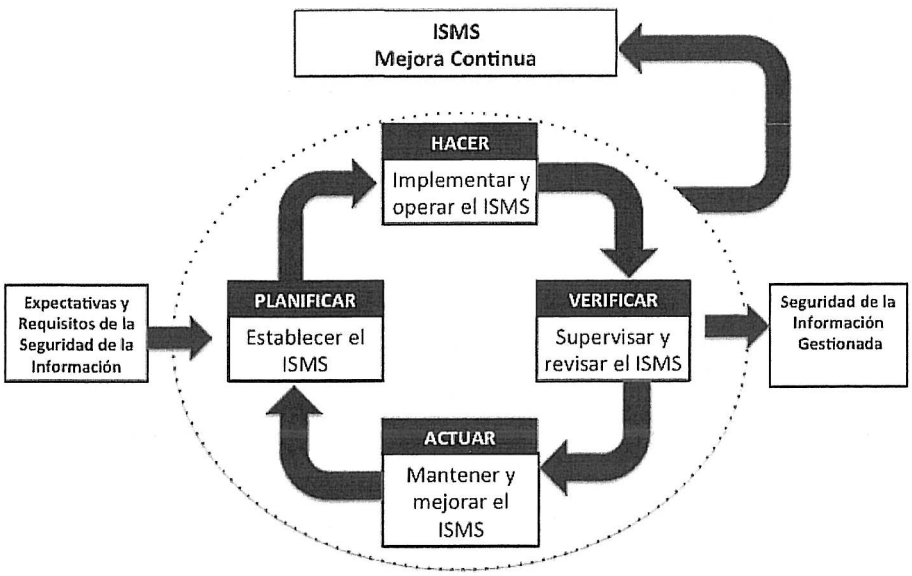

Figura 3-15
Modelo Planificar-Hacer-Verificar-Actuar
Aplicado a los Procesos ISMS

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

---

[44] 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).

[45] 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.

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,

[46] 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.

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.

