# Gestión de riesgos en entidades del gobierno en Colombia

Wilmar Fabian Villamil Beltran
wfvillamil@gmail.com
*Especialización en Seguridad Informática*
*Universidad Piloto de Colombia – Bogotá, Colombia*

***Resumen*—El hacking ético es la manera de descubrir las debilidades y vulnerabilidades en el sistema o la red de computadoras. Esto basado en el hecho de que los ataques, han ocasionado en los gobiernos daño, robo o filtrado de información muy confidencial como a su vez daño en la infraestructura o violación de la seguridad para generar ataques al sistema. Por esta razón los hackers éticos están como una necesidad para probar y comprobar las vulnerabilidades y debilidades en el sistema actual. Sin embargo, existe otra cara de la moneda que dice que sin hackers las vulnerabilidades y agujeros de software permanecería sin descubrir [1]. El propósito de esta investigación es examinar un enfoque más proactivo para preparar adecuadamente la seguridad de la información futura en entornos gubernamentales. Los profesionales deben estar equipados con los conjuntos de habilidades necesarios para combatir una presencia cada vez mayor de actividad no deseada a través de Internet. Por lo tanto, se necesita tener habilidades y procedimientos en sistemas de gestión de seguridad de la información, para reconocer y defender adecuadamente las intrusiones no autorizadas. Esta investigación indaga en un énfasis en las preocupaciones éticas y legales asociadas con el hacking ético, las buenas prácticas en la red y los distintos niveles de gestión para mitigar, corregir y prevenir ataques.**

***Abstract*—The Ethical hacking is the way to discover weaknesses and vulnerabilities in the computer system or network. This is based on the fact that the attacks have caused data damage, theft or filtering of very confidential information such as once a damage to the infrastructure or the security of attacks on the system. For this reason, hackers are a necessity to test and verify vulnerabilities and weaknesses in the current system. However, there is one side of the coin that says that hackers vulnerabilities and software holes will remain undiscovered [1]. The purpose of this research is the focus of one more approach for the future. Professionals must be equipped with them. Therefore, it is necessary to have the skills and procedures in information security management systems, to recognize and defend unauthorized intrusions. This is an investigation into an emphasis on ethical tasks and relationships with ethical hacking, good practices in the network and different levels of management to mitigate, correct and prevent attacks**

## I. Introducción

El protagonismo de las tecnologías de la información y la creciente dependencia de las infraestructuras tecnológicas continúa filtrándose en toda la sociedad. Se puede argumentar que alguna preocupación se debe a la aparente falta de seguridad inherente a las tecnologías y sistemas de información.

El Hacking Ético, como su nombre sugiere, es una piratería, pero desde un enfoque ético, por lo que su actividad se centra en pruebas de penetración al sistema. Es la manera a través de la cual un hacker ético descubrirá alguna vulnerabilidad desde el punto de vista del hacker para que el sistema se pueda hacer más seguro y menos vulnerable.

El propósito de esta investigación es analizar el uso de metodologías como el Hacking ético, la gestión riesgos en la red, las buenas prácticas, la implementación de normas internacionales en términos de seguridad informática, entre otras prácticas para mejorar la instrucción de seguridad de la información.

En conjunto con el hacking ético se tiene lo que se llama un sistema de gestión de seguridad de la información (SGSI) es una necesidad para una nube de mediana a gran escala. Cada organización que construye una nube de este tamaño debe tener un conjunto completo de documentos de políticas y procedimientos. Una de las certificaciones de seguridad más comunes para una empresa es la ISO 27002, que identifica y detalla las mejores prácticas para las compañías que están implementando el SGSI. Basta con decir que el enfoque de este estándar es la seguridad continua de los sistemas y que la seguridad en las operaciones es un aspecto clave. La ISO 27002 exige que ciertas actividades se realicen antes de que un sistema esté en producción. Estas actividades incluyen lo siguiente: una evaluación de riesgos, una política de seguridad, estándares asociados, Gestión de activos, seguridad del personal, seguridad física y ambiental. Igualmente, importantes son las actividades que caen en la operación de una nube, como la gestión de comunicaciones y operaciones, el control de acceso, la gestión de incidentes y la gestión de la continuidad del negocio.

## II. Planteamiento del Problema

Existen empresas, entidades, organizaciones, comunidades entre otros que no se preocupan por implementar medidas de seguridad informática o si lo hacen, solo consideran externalidades y no tienen en cuenta los riesgos que se puedan presentar al interior de estas.

El modelo que se implementa establece que cuando la entidad es víctima de un ataque que se convierte en un incidente, esta aplica una contramedida para responder y solucionarlo, para lo cual debe hacer una inversión en recursos económicos y tecnológicos. Esta estrategia de solución no es óptima, ya que redunda en nuevas vulnerabilidades porque se está tomando medidas para solucionar los eventos a medida que surgen y no se hacen de una forma planificada ni con políticas de seguridad adecuadas. En este escenario, la situación de seguridad no mejora o lo hace muy poco y el costo de invertir en seguridad es muy elevado y se incrementa en términos inmediatos.

Para los desarrolladores de software, la seguridad interfiere con las características del programa principal. Esto conlleva a

protocolos ampliamente utilizados para conexiones como TCP/IP las cuales son usadas para infiltrarse en la red y realizar conexiones a través de cuentas de dominio de los usuarios siempre y cuando usen la misma clave para cada aplicación

[2], o una secuencia interminable de errores de desbordamiento de búfer en programas que normalmente se ejecutan con privilegios, cada uno haciendo posible que un atacante tome el control del sistema.

Para los usuarios y administradores, la seguridad interfiere con la realización del trabajo de manera inconveniente. Esto es muy importante, ya que hay más usuarios que desarrolladores. Además, si la configuración es demasiado permisiva nadie se dará cuenta de la falta de seguridad a menos que haya una auditoría o un ataque. Esto conduce a cosas como que los usuarios cuya contraseña es su nombre de pila, o una empresa grande en la que más de la mitad de los servidores de base de datos instalados tienen una contraseña de administrador en blanco [3], o acceso público a bases de datos de números de tarjetas de crédito [4,5] o clientes de correo electrónico que ejecutan datos adjuntos que contienen código arbitrario con los privilegios del usuario [6].

También se tiene, el término seguridad cibernética se usa a menudo indistintamente con el término seguridad de la información. Aunque hay una superposición sustancial entre la seguridad cibernética y la seguridad de la información, estos dos conceptos no son totalmente análogos. En la seguridad cibernética, este factor tiene una dimensión adicional, tener presente la condición de los humanos como posibles objetivos de ataques cibernéticos o incluso sin saberlo, participar en un ataque cibernético.

Por lo tanto, surge la iniciativa de redes inteligentes, una red que depende cada vez más de su infraestructura cibernética para soportar las numerosas aplicaciones de energía necesarias para proporcionar capacidades mejoradas de monitoreo y control de redes. Sin embargo, los hallazgos recientes documentados en informes del gobierno y en otras publicaciones, indican la creciente amenaza de ataques cibernéticos en número y sofisticación dirigida a la red eléctrica de la nación y otras infraestructuras críticas.

## III. Definiciones

Étical Hacking:

Se llamará a una persona como hacker ético cuando no destruya la seguridad del sistema, tampoco cometa actos vandálicos así tenga la capacidad de hacerlo y realice prácticas dentro de un entorno dónde sus servicios sean conocidos y con consentimiento, de manera que se ocupará de la seguridad del sistema desde el punto de vista del pirata informático.

Así que el Hacking ético puede ser definido como la metodología adaptado por Hackers para descubrir las vulnerabilidades existentes en los entornos operativos de los sistemas de información.

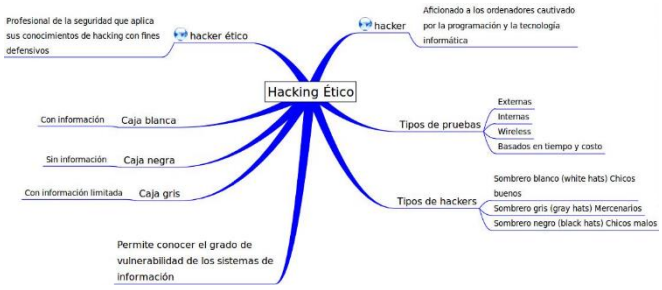

Fig. 1. Definición del hacking ético.

Por su parte el Hacking se define como el conjunto de técnicas y procedimientos utilizados por una persona con gran cantidad de conocimiento en el ámbito de la informática.

Sistema de Gestión de Seguridad de la Información:

La norma internacional para Sistemas de Gestión de Seguridad de la Información es la norma ISO de los documentos de la serie ISO 27000. Dentro de los 2 documentos iniciales, ISO 27001 e ISO 27002, se definen 14 clases de control de seguridad. La clase de control 12.7 en la norma ISO 27001/27002 proporciona la guía básica para la auditoría y revisión de las clases de control ISO. Tiene derecho a 12.7 Consideraciones de auditoría de sistemas de información y establece que las auditorías de TI deben planificarse y controlarse para minimizar los efectos adversos en los sistemas de producción o el acceso inadecuado a los datos. Se enlaza con los documentos ISO posteriores en las series 27000 ISO 27007 y 27008.

Las entidades gubernamentales que alinean sus prácticas de seguridad de la información con un estándar de la serie ISO 27000 pueden:

- Asegurar sus activos críticos.
- Administrar los riesgos de forma mucho más efectiva.
- Mejorar y mantener la confianza del cliente.
- Demostrar conformidad con las mejores prácticas internacionales.
- Evitar daños de marca, pérdida de ganancias o posibles multas regulatorias.
- Desarrollar su postura de seguridad de la información junto con los desarrollos tecnológicos.

Ciclo PHVA

El ciclo PHVA, también conocido como ciclo Deming, propone procesos que deben ser analizados y medidos para identificar fuentes de variaciones que causan los productos que se desvían de los requerimientos del cliente. Es la metodología más utilizada para implementar un sistema de mejora continua en una empresa u organización.

El nombre de PDCA proviene del acrónimo "Planificar, Hacer, Verificar, Actuar" (PHVA en español), y también se lo

conoce como el ciclo de mejora continua o Ciclo de Deming (por el nombre de su autor, Edwards Deming). Esta metodología describe los cuatro pasos esenciales que deben llevarse a cabo de manera sistemática para lograr una mejora continua, definida como una forma continua de mejorar la calidad de nuestros productos y procesos (reducir fallas, aumentar la eficacia y la eficiencia, resolver problemas, evitar riesgos potenciales ...).

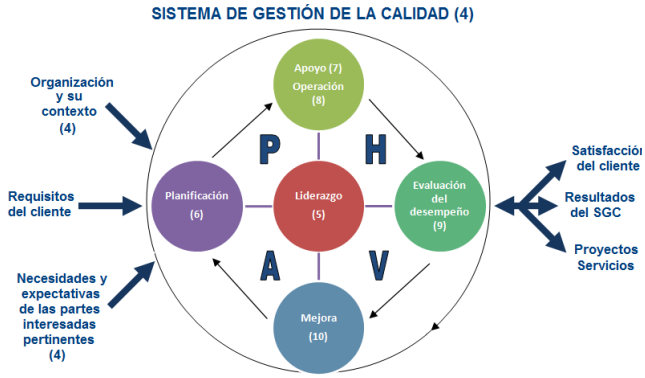


Fig. 2. Sistema de Gestión de la Calidad.

## IV. Principios de la Seguridad Informática

La seguridad de la información (infosec) se refiere a los procesos y herramientas diseñados e implementados para proteger la información de modificaciones, interrupciones, destrucción e inspección.

Por lo tanto, la seguridad de la información abarca muchas áreas de investigación como la criptografía, la computación móvil, la cibernética, las redes sociales y muchas otras áreas más que amenacen con la seguridad de la informática:

- Los programas dedicados a los sistemas de seguridad de la información se basan en 3 objetivos, comúnmente conocidos como: confidencialidad, integridad, disponibilidad.
- Confidencialidad: la información no se divulga a personas, entidades y procesos no autorizados.
- Integridad: es mantener la exactitud y la integridad de los datos. Esto significa que los datos no se pueden editar de forma no autorizada.
- Disponibilidad: significa que la información debe estar disponible cuando sea necesario.

En el núcleo de la Seguridad de la información (infosec) se encuentra el aseguramiento de la información, que significa el acto de mantener la información, asegurando que la información no se vea comprometida de ninguna manera cuando surjan problemas críticos.

Por lo tanto, la seguridad de la información es un conjunto de estrategias para administrar los procesos, herramientas y políticas necesarias para prevenir, detectar, documentar y contrarrestar las amenazas a la información digital y no digital.

### *A. Conceptos relacionados*

*1. La seguridad de la información describe las actividades que se relacionan con la protección de la información y los activos de la infraestructura de la información contra los riesgos de pérdida, mal uso, divulgación o daño.*

*2. Administrador de seguridad de la información certificado: la capacitación CISM es una credencial de TI única para los profesionales de TI que diseñan, construyen y administran la seguridad de la gestión de la información empresarial.*

*3. La gestión de la seguridad de la información (ISM) describe los controles que una organización necesita implementar para garantizar que administra con sensatez estos riesgos.*

*4. Sistema de gestión de la seguridad de la información (SGSI): un conjunto de políticas relacionadas con la gestión de la seguridad de la información o los riesgos relacionados con la TI.*

### *B. Principios de un sistema de gestión de seguridad de la información*

Si bien la implementación de un SGSI variará de una organización a otra, hay principios subyacentes que todos los SGSI deben cumplir para ser eficaces en la protección de los activos de información de una organización. Estos principios, algunos de los cuales se mencionan a continuación, lo guiarán en la certificación ISO / IEC 27001.

El primer paso para implementar con éxito un SGSI es hacer que las partes interesadas clave estén al tanto de la necesidad de seguridad de la información. Sin la participación de las personas que implementarán, supervisarán o mantendrán un SGSI, será difícil lograr y mantener el nivel de diligencia necesario para crear y mantener un SGSI certificado.

Para que el SGSI de una organización sea efectivo, debe analizar las necesidades de seguridad de cada activo de información y aplicar los controles adecuados para mantenerlos seguros. No todos los activos de información necesitan los mismos controles, y no hay una solución mágica para la seguridad de la información. La información viene en todas las formas y tamaños, al igual que los controles que mantendrán su información segura.

Para mantener a una organización a salvo de las amenazas de la información, un SGSI debe crecer y evolucionar continuamente para satisfacer el panorama técnico que cambia rápidamente. Por lo tanto, la reevaluación continua de un Sistema de Gestión de Seguridad de la Información es una necesidad. Al probar y evaluar con frecuencia un SGSI, una organización sabrá si su información aún está protegida o si es necesario realizar modificaciones.

### *C. La seguridad de la información es una función de gestión*

Si bien hay muchos aspectos técnicos para crear un Sistema de Gestión de Seguridad de la Información, una gran parte de

un SGSI se encuentra en el ámbito de la administración.

Uno de los eslabones más débiles en el cambio de seguridad de la información es un empleado: la persona que accede o controla la información crítica todos los días. Un SGSI debe incluir políticas y procesos que protejan a una organización del mal uso de los datos por parte de los empleados. Estas políticas deben contar con el respaldo y la supervisión de la administración para que sean efectivas.

Además de los cambios de políticas y procesos formales, la administración también debe cambiar la cultura de una organización para reflejar el valor que otorga a la seguridad de la información. Esta no es una tarea fácil, pero es fundamental para la implementación efectiva de un SGSI.

*D. La gestión de la seguridad de la información es un proceso.*

Al igual que las organizaciones se adaptan a los entornos empresariales cambiantes, los sistemas de gestión de seguridad de la información deben adaptarse a los avances tecnológicos cambiantes y la nueva información organizativa. Para adaptarse a estas condiciones cambiantes, ISO / IEC 27001 adopta un enfoque basado en procesos para un SGSI utilizando la metodología Planificar-Hacer-Verificar-Actuar.

*E. Modelos de seguridad organizacional.*

Algunas de las mejores prácticas que facilitan la implementación de los controles de seguridad incluyen los Objetivos de control para información y tecnología relacionada (COBIT), ISO / IEC 17799 / BS 7799, Biblioteca de infraestructura de tecnología de la información (ITIL) y Evaluación de amenazas operacionales, amenazas y vulnerabilidad ( OCTAVA).

1. *COSO: El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), es una iniciativa del sector privado de los Estados Unidos, creada en 1985. Su principal objetivo es identificar los factores que causan informes financieros fraudulentos y hacer recomendaciones para reducir su incidencia. COSO ha establecido una definición común de controles internos, estándares y criterios con los cuales las empresas y organizaciones pueden evaluar sus sistemas de control.*

2. *ITIL: La Biblioteca de Infraestructura de Tecnología de la Información (ITIL) es un conjunto de conceptos y técnicas para administrar la infraestructura, el desarrollo y las operaciones de la tecnología de la información (TI). ITIL se publica en una serie de libros, cada uno de los cuales cubre un tema de administración de TI.*

3. *COBIT 4.X: Los Objetivos de control para la información y la tecnología relacionada (COBIT 4.X) son un conjunto de mejores prácticas (marco) para la gestión de la tecnología de la información (TI) creado por la Asociación de control y auditoría de sistemas de información (ISACA) y el Instituto de gobierno de TI (ITGI). ) en 1992. COBIT proporciona a los gerentes, auditores y usuarios de TI un conjunto de medidas, indicadores, procesos y mejores prácticas generalmente aceptados para ayudarlos a maximizar los beneficios derivados del uso de la tecnología de la información y desarrollar un gobierno y control de TI adecuados en una empresa.*

4. *Serie ISO 27000: La serie ISO / IEC 27000 (también conocida como 'Familia de Normas ISMS' o 'ISO27' para abreviar) comprende normas de seguridad de la información publicadas conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie proporciona recomendaciones de mejores prácticas sobre la gestión de la seguridad de la información, los riesgos y los controles en el contexto de un Sistema de gestión de la seguridad de la información (SGSI) general, similar en diseño a los sistemas de gestión para el control de calidad (la serie ISO 9000) y la protección del medio ambiente (la ISO 14000). serie). La serie tiene un alcance deliberadamente amplio, que abarca más que la privacidad, la confidencialidad y los problemas de seguridad técnica o de TI. Es aplicable a organizaciones de todas las formas y tamaños. Se recomienda a todas las organizaciones que evalúen sus riesgos de seguridad de la información y luego implementen los controles de seguridad de la información adecuados de acuerdo con sus necesidades, utilizando la orientación y las sugerencias cuando sea pertinente. Dada la naturaleza dinámica de la seguridad de la información, el concepto de SGSI incorpora una retroalimentación continua y actividades de mejora, resumidas por el enfoque de "planificar-hacer-verificar-actuar" de Deming, que busca abordar los cambios en las amenazas, vulnerabilidades o impactos de los incidentes de seguridad de la información.*

## V. Gestión de riesgos

La gestión del riesgo de la información (IRM) es el proceso de identificar y evaluar el riesgo, darse cuenta de las limitaciones para reducirlo a un nivel aceptable e implementar los mecanismos adecuados para mantener ese nivel.

Categorías de Riesgos

- Daños físicos: incendio, agua, vandalismo, pérdida de energía y desastres naturales
- Interacción humana: acción accidental o

intencional o inacción que puede interrumpir la productividad

- Mal funcionamiento del equipo - Fallo de sistemas y dispositivos periféricos.
- Ataques internos y externos: piratería, grietas y ataques.
- Uso indebido de datos: compartir secretos comerciales, fraude, espionaje y robo
- Pérdida de datos: pérdida intencional o no intencional de información a través de medios destructivos
- Error de aplicación: errores de cálculo, errores de entrada y desbordamientos de búfer
- Estado social - Pérdida de la base de clientes y reputación.

Las estrategias de manejo de riesgos

Como es imposible tener un sistema o un entorno que sea 100% seguro, debería existir un nivel de riesgo aceptable.

Riesgo Residual vs. Riesgo Total

- Riesgo residual: donde siempre hay algo de riesgo por resolver.
- Riesgo total: donde no existen medidas de riesgo y el riesgo es del 100%. Este tipo de riesgo es aceptable cuando los resultados del análisis costo / beneficio indican que este es el mejor curso de acción.
- La relación:
    - Amenazas * Vulnerabilidad * Valor del activo = Riesgo total
    - Amenazas * Vulnerabilidad * Valor del activo * Brecha de control = Riesgo residual

Maneras de lidiar con el riesgo

Hay cuatro formas básicas de lidiar con los riesgos:

- Transfiérelo: Si el riesgo total o residual de una compañía es demasiado alto y compra un seguro, entonces es una transferencia de riesgo a la compañía de seguros
- Rechazar: si una empresa niega su riesgo o lo ignora, lo rechaza.
- Reducirlo: si una empresa implementa contramedidas, está reduciendo el riesgo
- Aceptarlo: si una empresa entiende el riesgo y decide no implementar ningún tipo de contramedidas, está aceptando el riesgo. Y esto es realmente a lo que se reducen todos los sistemas informáticos. No hay manera de mitigar el riesgo si el sistema se va a conectar a Internet. Tener un solo usuario sin ningún tipo de conexión en red con otros sistemas informáticos es el armario que puede tener para no tener ningún riesgo.

**Evaluación / Análisis de Riesgos**

El análisis de riesgos es un método para identificar vulnerabilidades y amenazas y evaluar los posibles daños para determinar dónde implementar las salvaguardas de seguridad.

**Identificar las Vulnerabilidades y Amenazas**

Hay muchos tipos de agentes de amenazas que pueden aprovechar varios tipos de vulnerabilidades, lo que resulta en una variedad de amenazas específicas.

Tabla1.
Vulnerabilidades y Amenazas.

| Agente de amenazas | Puede explotar esta vulnerabilidad | Resultando en esta amenaza |
|---|---|---|
| Virus | Falta de software antivirus | Infección vírica |
| Hacker | Potentes servicios que se ejecutan en un servidor. | Acceso no autorizado a información confidencial. |
| Usuarios | Parámetro mal configurado en el sistema operativo | Error del sistema |
| Fuego | Falta de extintores | Daño a la instalación y la computadora, y posiblemente pérdida de vidas. |
| Empleado | Falta de capacitación o cumplimiento de normas<br>Falta de auditoría | Compartir información de misión crítica.<br>Modificar las entradas y salidas de datos de las aplicaciones de procesamiento de datos |
| Contratista | Falta de mecanismos de control de acceso. | Robando información confidencial |
| Agresor | Aplicación mal escrita.<br>Falta de configuraciones estrictas de firewall | Realización de un desbordamiento de búfer<br>Realización de un ataque de denegación de servicio |
| Intruso | Falta de guardia de seguridad | Rompiendo ventanas y robando computadoras y dispositivos. |

## VI. Implementar el Sistema de Gestión de Seguridad de la Información

Las organizaciones pueden beneficiarse significativamente de la implementación de un SGSI, lograr el cumplimiento de la norma ISO 27001 y garantizar la seguridad de sus activos informativos, pero se requiere un proceso completo de implementación y capacitación para obtener los beneficios completos del SGSI. Aquí le mostramos cómo comenzar a implementar el SGSI en su organización:

Pasó uno: Identificación y valoración de activos

El primer paso para implementar un SGSI es identificar los

activos que deben protegerse y determinar su valor relativo para la organización. Recuerde, un SGSI basado en el riesgo tiene en cuenta la importancia relativa de los diferentes tipos de datos y dispositivos y los protege en consecuencia. En este paso, las organizaciones recopilan datos de la documentación para identificar los activos de TI críticos para el negocio y su importancia relativa para la organización.

Las organizaciones deben crear una Declaración de Sensibilidad (SoS) que asigne una calificación a cada uno de sus activos de TI en tres dimensiones distintas: confidencialidad, integridad y disponibilidad:

- Confidencialidad: garantizar que la información sea accesible exclusivamente para personas autorizadas.
- Integridad: garantizar que la información a proteger sea precisa y completa, y que la información y los métodos de procesamiento estén protegidos.
- Disponibilidad: garantizar que las personas autorizadas tengan acceso a la información y los activos protegidos cuando sea necesario.

Paso dos: realizar una evaluación de riesgos detallada

Una vez que se ha completado la identificación y valoración de los activos y la organización ha formulado un SoS, es hora de realizar una evaluación de riesgos detallada que informará la producción del SGSI. Un análisis de evaluación de riesgos incluye cuatro pasos importantes para determinar cómo se debe proteger el activo de TI:

1. Amenazas: la organización debe analizar las amenazas al activo al documentar cualquier evento no deseado que pueda resultar en un mal uso, pérdida o daño deliberado o accidental de los activos.
2. Vulnerabilidades: las amenazas son una descripción concreta de lo que podría suceder, y las vulnerabilidades son una medida de cuán susceptible podría ser el activo de TI a las amenazas identificadas en la primera parte del análisis. Aquí es donde comienza a diferenciar los diferentes tipos de activos: mientras que un ataque de software malintencionado es una amenaza para servidores, computadoras portátiles y teléfonos, aquí podemos indicar que los teléfonos son más vulnerables a la amenaza porque se usarán de forma remota y podrían serlo. conectado a varias redes externas, mientras que los servidores estarán monitoreados durante todo el día a través de herramientas de monitoreo.
3. Impacto y probabilidad: la organización ahora puede evaluar la probabilidad de que ocurran ciertos tipos de violaciones junto con la magnitud del daño potencial que resultaría de cada tipo de violación de datos. Las organizaciones pueden usar un análisis de costo-beneficio para ayudarlos a identificar las infracciones más potencialmente dañinas con las medidas de seguridad más agresivas.
4. Las organizaciones deben lograr un equilibrio entre asegurar los activos y hacerlos accesibles a las personas autorizadas que pueden necesitar los datos para realizar su trabajo.
5. Mitigación: finalmente, la organización propone métodos para minimizar las amenazas, vulnerabilidades e impactos reconocidos a través de políticas y procedimientos en el SGSI.

Paso Tres: Establecer el SGSI

Ahora que la organización ha identificado los activos que deben protegerse y ha realizado una evaluación completa de riesgos, puede proceder a documentar las políticas y procedimientos reales que conforman el SGSI. Las organizaciones deben establecer el SGSI de conformidad con la norma ISO 27001 si desean obtener una certificación de las mejores prácticas en la gestión de la seguridad de la información.

Retomando el ejemplo tomado del paso dos sobre las vulnerabilidades del teléfono móvil sin garantía, ¿qué pasos podría tomar la organización para garantizar que la información en el teléfono esté protegida adecuadamente en caso de pérdida o robo del teléfono? Aquí hay algunos ejemplos de políticas que podrían implementarse para ayudar a mitigar el riesgo:

- Los teléfonos perdidos o robados deben informarse al departamento de TI dentro de las ocho horas. Si no sabe dónde está su teléfono, comuníquese con IT inmediatamente.
- TI debe tener la capacidad de rastrear y borrar de forma remota cualquier teléfono de propiedad de la empresa.
- Los teléfonos de la compañía deben estar protegidos por una contraseña biológica que corresponda al cesionario: se debe usar una tecnología de huellas dactilares, escaneo de retina o reconocimiento facial para desbloquear el teléfono.
- Los teléfonos de la compañía se emiten con una funda de cintura segura, lo que alienta a los empleados a evitar perder el activo asegurándolo a su persona cuando no está en uso.

Este conjunto de políticas y procedimientos minimizaría la posibilidad de que se produzca una violación de datos debido a la pérdida de un teléfono. El requisito de una contraseña biológica aumenta significativamente el nivel de sofisticación requerido para obtener acceso no autorizado al teléfono, los requisitos de informe introducen una responsabilidad adicional para el usuario del teléfono y TI puede eliminar datos confidenciales de cualquier teléfono que se informa que falta.

## VII. Mejores prácticas de seguridad

La industria de la tecnología de la información (TI) es un buen modelo para la protección de la ciberseguridad basada en su experiencia, exposición y direccionamiento de los problemas. La industria de las telecomunicaciones ayudó a acelerar el avance de las actividades de piratería y exponer los sistemas clave (hardware y software) mediante el avance de las redes y la habilitación del desarrollo de Internet.

La industria de seguridad de TI, desarrolló las mejores prácticas a lo largo de los años que incluyen el principio básico de que la seguridad de la información es un proceso de ciclo de vida.

Mientras que todos los elementos de un programa de gestión de riesgo de ciclo de vida son importantes, tal vez el elemento más vital de cualquier programa de ciberseguridad es realizar evaluaciones de riesgo en todos los sistemas, subsistemas, y dispositivos para determinar qué vulnerabilidades están presentes.

Es importante que los análisis de riesgo identifican y cuantifican las consecuencias de los riesgos. Una metodología muy eficaz para la evaluación de riesgos es el desarrollo de escenarios de casos de uso. El modelado adecuado de amenazas de ciberseguridad puede ayudar a crear un plan de mitigación de riesgos mejor y más eficaz a través de:

- Énfasis en la gestión de activos y reducción de riesgos antes de la adquisición de tecnologías de información y seguridad.
- Selección de contramedidas correctas
- Justificación de inversiones en seguridad, cumplimiento y gestión de riesgos.

Las industrias individuales examinan las mejores prácticas de este enfoque de ciclo de vida y crean pautas de seguridad específicas de la industria que abordan la necesidad de una sólida gestión de riesgos que incluya la evaluación, el diseño, la implementación y las fases de operación de sistemas éticos.

La investigación de las diversas industrias estudiadas ha dado algunos ejemplos de buenas prácticas, que se muestran en la siguiente tabla.

TABLA 2
Investigación sobre ciberseguridad.

| ***Observación clave*** |
|---|
| La ciberseguridad es un proceso de ciclo de vida que incluye elementos de evaluación, diseño, implementación y operaciones, así como un programa de pruebas y certificación eficaz |
| La industria de la aviación tiene muchos paralelismos con la industria automotriz en el área de ciberseguridad |
| El aprendizaje compartido continuo con otras agencias del gobierno federal es beneficioso |
| El uso de los estándares de ciberseguridad NIST como línea de base es una manera de acelerar el desarrollo de Directrices de ciberseguridad específicas de la industria |
| Los esfuerzos internacionales de ciberseguridad son una fuente clave de información |
| Los estándares de ciberseguridad para toda la cadena de suministro son importantes |
| Grupos de ciberseguridad para el intercambio de información de ciberseguridad |
| Utilice la creación de capacidad profesional para abordar el desarrollo de habilidades de ciberseguridad diseñadores e ingenieros del sistema |
| La seguridad del vehículo conectado debe ser de extremo a extremo; vehículos, infraestructura yV2Xcomunicacióndeberíatodosersegura. |
| Un fuerte liderazgo del gobierno federal podría ayudar al desarrollo de estándares de ciberseguridad específicos de la industria, directrices y mejores prácticas. |

El mapeo de estas observaciones clave al proceso de un programa de seguridad de la información del ciclo de vida produce las etapas en cada una de las fallas. Esto se muestra en la figura de abajo.

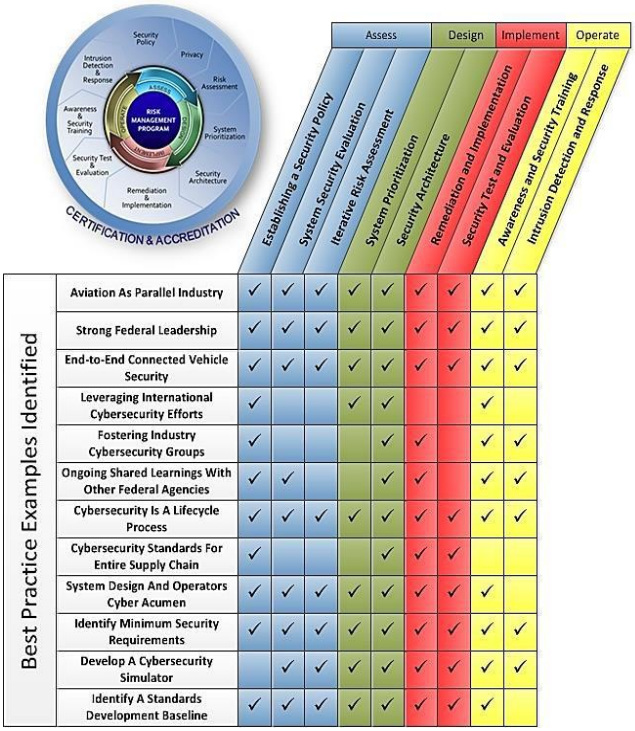


Fig 3. Ciclo de vida de la ciberseguridad. [16]

Si bien todos los elementos son importantes, tal vez el elemento más vital de cualquier programa de ciberseguridad es realizar evaluaciones de riesgos en todos los sistemas, subsistemas y dispositivos para determinar qué vulnerabilidades están presentes. Este proceso es importante para las organizaciones, ya que se utiliza para descubrir y categorizar los problemas de seguridad en sus sistemas. También es importante que los análisis de riesgos identifiquen y cuantifiquen las consecuencias de los factores de riesgo en escenarios de casos de uso aplicables. La evaluación de riesgos ayuda a crear un plan de mitigación de riesgos:

- Enfatiza el enfoque en la gestión de activos y reducción de riesgos antes de la adquisición de tecnologías de información y seguridad.
- Es necesarios la selección de las contramedidas correctas a menudo priorizando el monitoreo antes de la prevención de pérdida de datos (como ejemplo)
- Justifica inversiones en seguridad, cumplimiento y gestión de riesgos

Los desgloses detallados de los elementos del ciclo de vida de la información se muestran en la tabla 3.

TABLA 3
Fase de Evaluación y Fase de Diseño.

| | |
|---|---|
| **Fase de evaluación** | |
| **Establecer una política de seguridad** | Una política de seguridad incluye los requisitos y procedimientos administrativos en todas las áreas. Desempeñar un papel activo en el desarrollo de una política de seguridad robusta. |
| **Evaluación de seguridad del sistema** | Los sistemas deben examinarse y evaluarse para sus necesidades de seguridad utilizando normas y mejores prácticas establecidas a lo largo de su ciclo de vida para descubrir vulnerabilidades potenciales. |
| **Evaluación de riesgos iterativa** | Los riesgos se miden a través de la evaluación de la probabilidad de explotar la vulnerabilidad, así como la severidad para el sistema, organización, público, etc. |
| **Fase de diseño** | |
| **Priorización del sistema** | Una vez identificados y clasificados los riesgos, deben ser priorizados basado en la capacidad de la organización para aplicar los recursos apropiados (financiación, conjuntos de habilidades técnicas, etc.) |
| **Arquitectura de seguridad** | El examen de la arquitectura de seguridad de un sistema es la pieza final del plan de ciberseguridad. Evaluación de la seguridad del sistema y el comienzo de abordar las vulnerabilidades identificadas en la evaluación fase. |

## REFERENCIAS


[1] Jon Erickson, 2008, "Hacking : The Art of Exploitation", 2nd Edition, No Starch Press Inc., ISBN-13: 978-1-59327-144-2, ISBN-10: 1-59327-144-1

[2] Schneier and Mudge, Cryptanalysis of Microsoft's point-topoint tunneling protocol. 5th ACM Conf. Computer and Communications Security, San Francisco, 1998, 132-141, www.acm.org/pubs/citations/proceedings/commsec/288090/p132-schneier.

[3] Gray, J., personal communication.

[4] ZDNet, Stealing credit cards from babies. ZDNet News, 12 Jan.2000, www.zdnet.com/zdnn/stories/news/0,4586, 2421377,00.html.

[5] ZDNet, Major online credit card theft exposed. ZDNet News, 17 Mar. 2000, www.zdnet.com/zdnn/stories/news/0, 4586,2469820,00.html.

[6] CERT Coordination Center, CERT advisory CA-2000-04 Love Letter Worm, www.cert.org/advisories/CA-2000-04.html

[7] *A Wallis(2018, June 2018). What is Information Security? Why it's Important, Job Outlook and More [Online]*. Avilable: https://www.snhu.edu/about-us/newsroom/2018/06/what-is-information-security.

[8] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[9] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[10] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[11] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.

[12] ITU-T, European Network and Information Security Agency (ENISA), Network and Information Security Steering Group (NISSG) (2007). ICT Security Standards Roadmap, version 2.2, September 2007. http://www.itu.int/ITUT/studygroups/com17/ict/index.html.

[13] ISO/IEC JTC1/SC27 (2008). Standing Document 6 (SD6): Glossary of IT Security Terminology, 2008-03-19. http://www.jtc1sc27.din.de/sce/SD6.

[14] . Internet Engineering Task Force (2007). Internet Security Glossary, August 2007. http://www.ietf.org/rfc/rfc4949.txt.

[15] ITU Telecommunication Standardization Sector (2008). Security Compendium, Part 2—Approved ITU-T Security Definitions, http://www.itu.int/dmspub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc.

[16] NHTSA (2014). A Summary of Cybersecurity Best Practices. https://www.hsdl.org/?view&did=806518.