Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

¿GOBIERNO DE LA CIBERSEGURIDAD?

Rosa Xóchitl Sarabia Bautista

ciberseguridad

numero-27

Hoy en día, las amenazas cibernéticas se introducen en las organizaciones de diversas formas, ya sea por medio de los empleados, aplicaciones o sistemas utilizados en las operaciones del negocio. Lo que se mantiene constante es que existen riesgos en todas partes. Hemos llegado a una nueva era del cibercrimen en la cual se realizan ataques dirigidos a las empresas con la intención de ocasionar daño.

La seguridad requiere la participación activa de los altos directivos de las empresas. El término que describe el compromiso de la alta dirección es el gobierno corporativo, que es el conjunto de responsabilidades y prácticas ejercidas por los responsables de una empresa (por ejemplo, el consejo y la alta dirección) con el objetivo de proporcionar dirección estratégica, asegurar que los objetivos sean alcanzados, garantizar que los riesgos sean gestionados adecuadamente, y verificar que los recursos de la empresa sean utilizados de manera responsable.

Por lo tanto, la ciberseguridad debe ser parte integral del gobierno corporativo para lograr sus objetivos, no sólo para cubrir las necesidades actuales sino también las futuras. En general el gobierno de la ciberseguridad se puede englobar en el de seguridad de la información, dado que este último puede manejar información fuera del ciberespacio.

El objetivo de la seguridad de la información es desarrollar, implementar y administrar un programa de seguridad que alcance los siguientes cinco resultados básicos de un gobierno eficaz de seguridad:

1. Alineación estratégica: Alinear la seguridad de la información con la estrategia de negocio.
2. Administrar los riesgos: Ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los activos de información.

3. Entrega de valor: Optimizar las inversiones en la seguridad.
4. Administración de recursos: Utilizar el conocimiento y la infraestructura de la seguridad de la información con eficiencia y eficacia.
5. Medición del desempeño: Monitorear y reportar métricas de seguridad de la información para garantizar que se alcancen los objetivos.

Para lograr un gobierno eficaz, la alta dirección debe establecer un marco que guíe el desarrollo y mantenimiento de un programa integral de seguridad como el que se muestra a continuación:

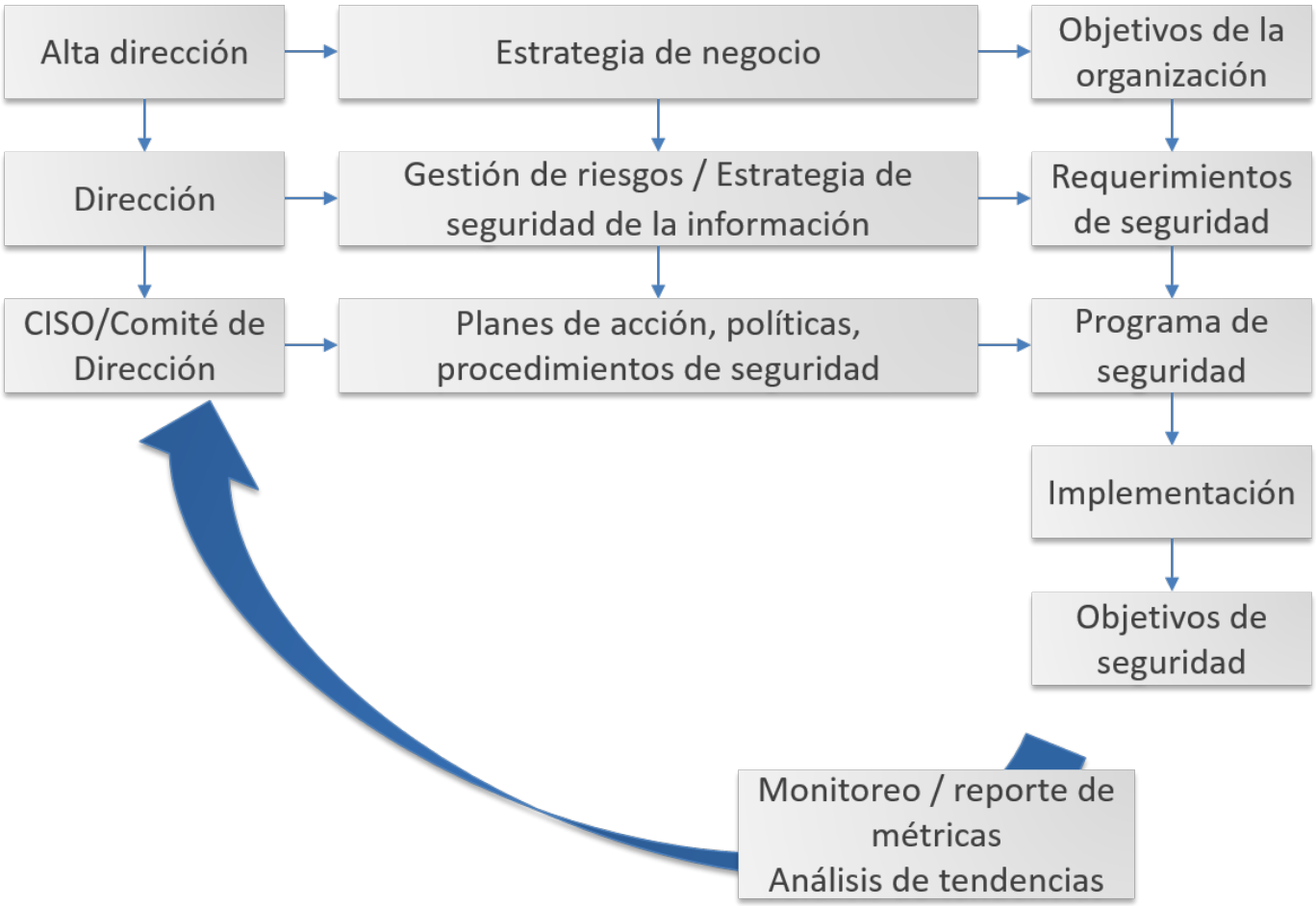


Figura 1 (IT Gobernance Institute, 2006)

La figura 1 muestra las relaciones y los participantes involucrados en el desarrollo de una estrategia de seguridad alineada a los objetivos de negocio. La estrategia tiene como entradas la estrategia de negocio, el estado actual y deseado de seguridad, los requerimientos del negocio y procesos, los resultados de la evaluación de riesgos y requisitos regulatorios. La estrategia proporciona la base para el desarrollo de los planes de acción (iniciativas de seguridad) en cumplimiento de los objetivos de seguridad.

Debido a que las organizaciones tienen diversas necesidades y sus enfoques de gobierno pueden variar, se ha identificado un conjunto básico de principios y buenas prácticas para ayudar a guiar estos esfuerzos.

Principios:

- El riesgo de seguridad de la información es más que un problema de TI: es un componente clave en la gestión de riesgos de la organización, lo que requiere la supervisión de la dirección.
- El riesgo tiene implicaciones legales que los directivos deben entender.
- El riesgo debe ser un tema de discusión en la junta de dirección de forma periódica.
- Los directores deben implementar un marco efectivo de gestión de riesgos en la organización.
- La alta dirección y el consejo deben evaluar el riesgo de seguridad de la información al igual que otros riesgos a nivel organización para asegurar que los riesgos se acepten, eviten, mitiguen o transfieran.

Buenas prácticas:

- Realizar una evaluación anual de la seguridad de la información a cargo de la alta dirección.
- Llevar a cabo evaluaciones de riesgos periódicos como parte de un programa global de gestión de riesgos.
- Implementar políticas y procedimientos basados en las evaluaciones de riesgos.
- Establecer una estructura de gestión de seguridad para asignar individualmente roles y responsabilidades.
- Desarrollar iniciativas para brindar seguridad de la información a redes, instalaciones, sistemas e información en general.
- Tratar la seguridad de la información como parte integral durante el ciclo de vida de los sistemas de información.
- Proporcionar concientización, capacitación y educación en seguridad de la información para todo el personal.
- Conducir pruebas y evaluaciones periódicas para medir la efectividad de las políticas y procedimientos de seguridad de la información.
- Crear y ejecutar planes de acción para manejar cualquier deficiencia de seguridad de la información.
- Desarrollar e implementar procedimientos de respuesta a incidentes.

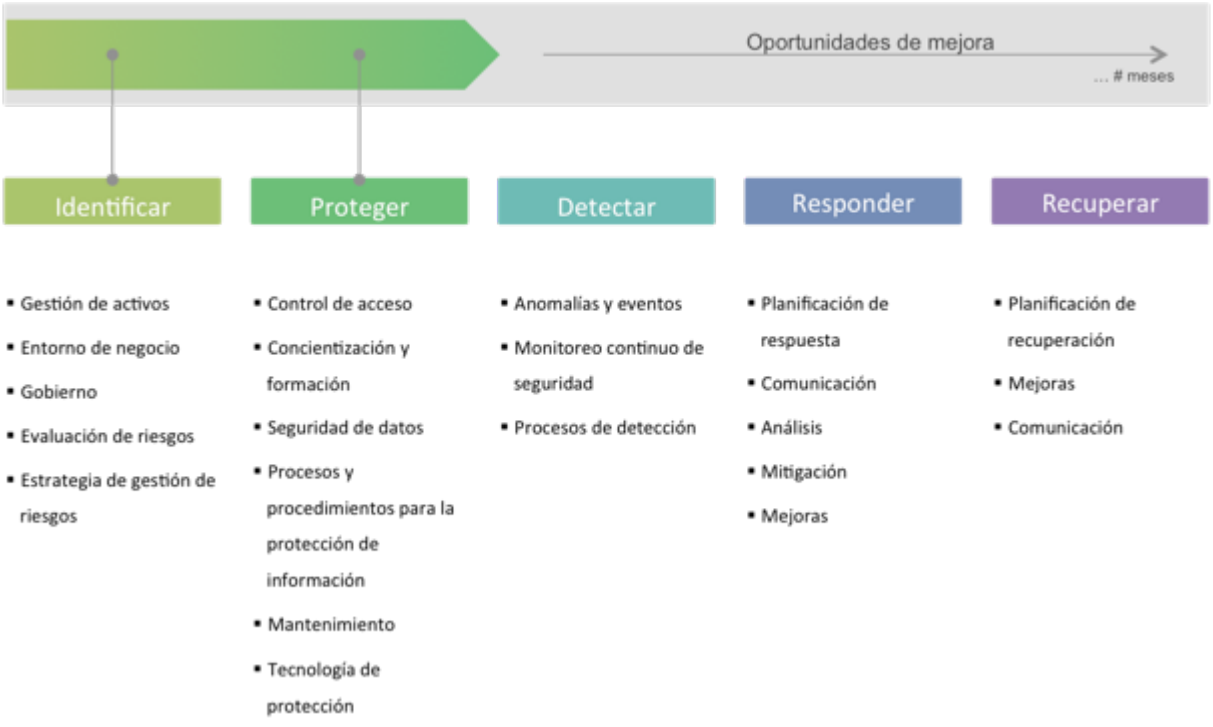
- Establecer planes, procedimientos y pruebas para proporcionar continuidad de las operaciones.
- Utilizar las mejores prácticas como ISO 27001, NIST SP 800, CoBIT, entre otros.

MARCO DE CIBERSEGURIDAD DEL NIST

Recientemente, el Instituto Nacional de Estándares y Tecnología (NIST) publicó un marco de ciberseguridad que permite a las organizaciones, independientemente de su tamaño, grado de riesgo o sofisticación de sus medidas de protección, aplicar las mejores prácticas para la gestión de riesgos que permita mejorar la seguridad y resiliencia de sus infraestructuras.

Son cinco las funciones básicas del marco que se definen a continuación:

1. Identificar: Desarrollar el conocimiento de la organización para gestionar riesgos de seguridad en sistemas, activos, datos y capacidades.
2. Proteger: Desarrollar e implementar las salvaguardas adecuadas para garantizar la prestación de servicios.
3. Detectar: Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de seguridad.
4. Responder: Desarrollar e implementar las actividades apropiadas para actuar ante un evento de seguridad detectado.
5. Recuperar: Desarrollar e implementar las actividades apropiadas para mantener planes de resiliencia y restaurar las capacidades o servicios que fueron perjudicados debido a un evento de seguridad.



CONCLUSIONES

Para la mayoría de las organizaciones, el establecimiento de un gobierno de seguridad de la información eficaz es una tarea primordial para integrar los esfuerzos aislados de seguridad que puedan existir y lograr resultados significativos en la reducción de pérdidas.

La tendencia hoy en día es que conforme las organizaciones crecen, éstas se vuelven más dependientes de sus activos de información y al mismo tiempo están expuestas a amenazas cada vez más sofisticadas, por ejemplo, *ransomware*, ataques de denegación de servicio distribuido (DDoS), las amenazas persistentes avanzadas (APT), entre otras.

Es por ello que se requiere el apoyo de la alta dirección y la asignación de los recursos adecuados, así como la definición de una estrategia que guíe las iniciativas de seguridad.

REFERENCIAS

- Binwal, P. (2015, 29 de junio). Creating a Cybersecurity Governance Framework: The Necessity of Time. *Security Intelligence.* Recuperado de https://securityintelligence.com/creating-a-cybersecurity-governance-framework-the-necessity-of-time/
- Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010, September). Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology. *The MITRE Corporation*. Recuperado de: https://www.mitre.org/sites/default/files/pdf/10_3710.pdf

- IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd edition). IL, Estados Unidos: IT Governance Institute.
- National Institute of Standards and Technology. (2014, February 12). *Framework for Improving Critical Infrastructure Cybersecurity*. Recuperado de http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
- R. Westby, J. (2015, October 2). *Governance of Cybersecurity: 2015 Report*. Washington, Estados Unidos: Georgia Tech Information Security Center. Recuperado de https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf
- The Corporate Governance Task Force. (2004, April). Information Security Governance: A Call to Action. *National Cyber Security Summit Task Force.*
- Threat Brief. (s.f.). Cyber Security and Corporate Governance: The five principles every corporate director should embody. *Threat Brief.* Recuperado de http://threatbrief.com/cyber-security-corporate-governance-five-principles-every-corporate-director-embody/

SI QUIERES SABER MÁS CONSULTA:

- Normatividad en las organizaciones: Políticas de seguridad de la información - Parte I
- Riesgo tecnológico y su impacto para las organizaciones parte I
- Buenas prácticas, estándares y normas

Source URL: http://revista.seguridad.unam.mx/numero27/%C2%BFgobierno-de-la-ciberseguridad