The International Investment Funds Association
L'Association internationale des fonds d'investissement

FUNDAMENTOS BÁSICOS DE CIBERSEGURIDAD

Establecer un marco base: Un marco de ciberseguridad es similar a un conjunto de diversos programas (planes de acción). Ayuda a identificar el alcance de la información que se debe proteger y proporciona normas, lineamientos y mejores prácticas para gestionar el riesgo. Existen diversos esquemas reconocidos y efectivos que establecen un proceso para definir controles efectivos a través estándares rentables que promueven la protección y resiliencia de los sistemas. Sin embargo, esto no significa que una empresa necesite hacer referencia a un solo marco, ya que puede ser también efectivo tomar partes de diferentes marcos que sean más adecuados para su caso en particular.

Recursos y fuentes adicionales de información:

https://www.nist.gov/cyberframework https://www.iso.org/isoiec-27001-information-security.html

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

https://www.cisecurity.org/controls/

Capacitar al personal y crear conciencia en materia de seguridad: Los trabajadores interactúan con clientes, colegas, proveedores externos de servicios y otros actores, y son el "factor humano" que a menudo constituye el foco de los atacantes. Una defensa efectiva, es capacitarlos y crear conciencia acerca de la seguridad. Para que esta capacitación tenga el mayor impacto posible, debe ser continua, atractiva y probada en tiempo y forma aleatoria. Ayudar a entender cuáles son las áreas que podrían ser objetos de ataques, permitirá reducir el éxito de los mismos (tanto a nivel laboral como personal), por ejemplo a través del *spam*, el *phishing*, la ingeniería social, el *ransomware*, entre otros.

Recursos y fuentes adicionales de información:

https://resources.infosecinstitute.com/components-successful-security-awareness-program/#gref

https://www.sans.org/security-awareness-training

Definir un plan de respuesta ante incidentes: Un plan de respuesta a incidentes es un conjunto de instrucciones para ayudar al personal a detectar, responder y recuperarse ante un ataque. Este plan debe contener un curso de acción para todos los incidentes significativos (que deben ser definidos por cada administradora). Cuando ocurre una interrupción significativa, se requiere un plan de respuesta detallado y completo para ayudar al personal a detener, contener y controlar el incidente rápidamente. Una amenaza para una organización, ya sea virtual o física, puede ser paralizante, y un plan de respuesta a

incidentes puede ayudar a mitigar y prepararse para un sinnúmero de eventos. El plan de respuesta a incidentes debe someterse a prueba y actualizarse regularmente.

Recursos y fuentes adicionales de información:

https://www.ibm.com/downloads/cas/PY31LRX2

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Incident-Management-and-Response.aspx

Realizar ejercicios de simulación: Un plan de respuesta a incidentes bien pensado que se encuentra en un estante y no se pone en práctica o actualiza, no está cumpliendo con su propósito. Estos deben ser probados para identificar brechas, realizar cambios y mejorar las estrategias de mitigación. Asimismo, los integrantes del personal deben sentirse cómodos con sus roles y responsabilidades durante un incidente cibernético grave. Y como en muchas iniciativas, lo que se requiere es práctica.

Suponiendo que los participantes correctos ya han sido identificados, al realizar una simulación se debe establecer un objetivo claro con respecto al alcance del escenario que se supondrá –por ejemplo, un ataque distribuido de denegación de servicio (DDoS)– y detallar el grado de complejidad deseado para el ejercicio. También se deben establecer objetivos independientes de lo esperado: por ejemplo, identificar qué tan bien diseñadas están las políticas y procedimientos existentes para responder a una amenaza, y saber si la información de contacto está actualizada. Al ponerse en el escenario, el ejercicio permitirá validar estos y otros datos. Los hallazgos deben ser documentados, de modo que cualquier falencia en los procedimientos pueda abordarse según corresponda y de forma oportuna.

Recursos y fuentes adicionales de información:

https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/

https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

Definir y monitorear la actividad normal de la red: La actividad normal abarca tanto a los empleados como a las redes. Se recomienda definir estándares de referencia para la conducta de los trabajadores, así como del funcionamiento normal de la red. Es prudente procurar que los trabajadores únicamente tengan acceso a aquellas partes de la red que requieren para sus funciones; determinar qué direcciones de IP pueden comunicarse con su red (o usualmente), y conozca cómo se comporta el tráfico de su web. Comprender y monitorear la actividad normal de la red permite identificar anomalías que deben ser investigadas.

Recursos y fuentes adicionales de información:

https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps/monitoring

Intercambio de información confiable: La principal amenaza de ciberseguridad es la de "riesgo de vencindario". En otras palabras, todos estamos juntos en esto y por ende, somos más fuertes si actuamos en conjunto. Formar redes o comunidades es un buen punto de partida para que los responsables de la seguridad de los sistemas y redes de información, se conecten con quienes enfrentan los mismos riesgos. Compartir información sobre vulnerabilidades y amenazas (que no afecten la competencia) en estas redes informales o comunidades, es una buena manera para que diversos actores de la industria generen confianza. El intercambio de información funciona mejor cuando hay un componente de confianza entre los participantes.