UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE DERECHO Y CRIMINOLOGÍA
LICENCIATURA EN CRIMINILOGIA
CIBERSEGURIDAD

GUÍA

1. **¿QUÉ ES UN RIESGO?**

Proximidad o contingencia de un posible daño. Es la probabilidad de que suceda un evento, impacto o consecuencia adverso. Probabilidad de que una amenaza se materialice utilizando una vulnerabilidad, generando un impacto con pérdidas o daños.

2. **¿QUE ES LA GESTIÓN DE RIESGOS? PREGUNTA ABIERTA**

La **Gestión de riesgos** es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.

3. **¿CUÁLES SON LAS ETAPAS DE LA GESTIÓN DE RIESGOS?**

La gestión de riesgos se puede dividir en **tres etapas** diferenciadas:

1. La identificación,
2. La evaluación y
3. El tratamiento de los riesgos.

4. **¿CÓMO PODEMOS PROTEGER EL SISTEMA INFORMÁTICO? PREGUNTA ABIERTA**

a) Primero hacer es un análisis de las posibles amenazas y vulnerabilidades para evaluar el riesgo.
b) A partir de ese análisis habrá que diseñar una política de seguridad para tratar el riesgo (evitar el riesgo, eliminar la fuente del riesgo, mitigar el riesgo, etc)
c) Implementar una Política de seguridad como un "documento sencillo que define las directrices organizativas en materia de seguridad".

5. **QUE ES UNA VULNERABILIDAD?**

Debilidad o falla presente en los sistemas informáticos

6. **¿QUE SON LAS AMENAZAS?**

Acciones dañinas. Acciones con consecuencias negativas a los sistemas informáticos

7. **COMO SE DEFINE LA PROBABILIDAD EN LA GESTIÓN DEL RIESGO**

Probabilidad: de ocurrencia de la amenaza, puede ser cualitativa o cuantitativa

8. **COMO SE DEFINE EL IMPACTO EN LA GESTIÓN DEL RIESGO**

Impacto: consecuencias de la ocurrencia de la amenaza, pueden ser Económicas, no Económicas

9. **QUE ES LA VALORACIÓN DEL RIESGO**

Proceso mediante el cual se establece la probabilidad de que ocurran daños o pérdidas materiales y la cuantificación de los mismos. La valoración del riesgo, es el producto de la Probabilidad de Amenaza por el impacto del daño, está agrupado en tres rangos.

- ❑ Bajo Riesgo = 1 – 6 (Verde)
- ❑ Medio Riesgo = 8 – 9 (amarillo)
- ❑ Alto Riesgo = 12 – 16 (rojo)

10. ELABORAR UNA MATRIZ DE RIESGOS EN TRES PASOS PREGUNTA ABIERTA

Paso 1:
Lógicamente el primer paso será identificar el máximo posible número de riesgos para nuestro proyecto. Para ello deberemos reunir la mayor información y analizar el posible origen de los riesgos.

Paso 2:
Después de la identificación de los riesgos, el siguiente paso sería hacer un análisis cualitativo y a ser posible también cuantitativo de los mismos para poder clasificarlos de mayor a menor importancia en nuestra Matriz de Riesgos.

Paso 3:
Una vez analizada la probabilidad y el impacto de los riesgos del proyecto, siguiendo los pasos 1 y 2, procederíamos a cumplimentar la Matriz de Riesgos En esta matriz indicaríamos por un lado el riesgo, y por otro su probabilidad e impacto, el resultado de multiplicar PxI (Probabilidad x Impacto) será la clasificación global del riesgo.

11. DEFINE HONEYPOT

Un honeypot, o sistema trampa o señuelo, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

12. ESCRIBE A QUE SE REFIERE LA DENEGACIÓN DE SERVICIO (DOS)

Un ataque DoS se produce cuando el cliente legítimo se le niega el acceso a los recursos de la red debido a la falta de disponibilidad de los servicios. Este tipo de ataque suele ser el trabajo de una colección de robots, o el número de usuarios múltiples veces usando programas sitio bombardeo.

13. CUALES ES EL OBJETIVO DE LAS POLITICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La información debe ser siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada. **El objetivo de la seguridad de la información es asegurar la continuidad del negocio en la organización y reducir al mínimo el riesgo de daño** mediante la prevención de incidentes de seguridad, así como reducir su impacto potencial cuando sea inevitable.

14. PARA CONFIGURAR SU POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ASEGURESE QUE: (PREGUNTA ABIERTA)

1. La **información** estará protegida contra cualquier acceso no autorizado.
2. No olvide tomar en cuenta la **confidencialidad** de la información.
3. La **integridad** de la información se mantendrá en relación a la clasificación de la información (especialmente la de “uso interno”).
4. La **disponibilidad** de la información cumple con los tiempos relevantes para el desarrollo de los procesos críticos de negocio.
5. **Se cumplen con los requisitos de las legislaciones** y reglamentaciones vigentes.
6. **Los planes de continuidad de negocio** serán mantenidos, probados y actualizados al menos con carácter anual.

7. La **capacitación** en materia de seguridad se cumple y se actualiza suficientemente para **todos los empleados.**
8. Todos los eventos que tengan relación con la **seguridad de la información** se comunicarán al responsable de seguridad **y serán investigados**.

15. LEGISLACIÓN EN CIBERSEGURIDAD

- Convenio de Budapest
- Constitución mexicana
- Ley de Telecomunicaciones y Radiodifusión (FTBL);
- Ley Federal de Protección de Datos Personales en poder de Particulares (Ley de Protección de Datos), sus reglamentos, recomendaciones, directrices y reglamentos similares sobre protección de datos;
- Norma Federal de Transparencia y Acceso a la Información Pública;
- Normas Generales como la Norma Oficial Mexicana con respecto a los requisitos que deben observarse al guardar mensajes de datos;
- Ley de la Policía Federal;
- Plan Nacional de Desarrollo 2013-2018;
- Estrategia Nacional de Ciberseguridad 2017;

16. CONVENIO DE BUDAPEST

Con el objetivo de establecer una política penal común y armonizar la cooperación internacionalsobre ciberdelincuencia, en 2001 el Comité de Ministros del Consejo de Europa sancionó el Convenio de Budapest. Al día de hoy se han adherido al convenio más de 56 países de todo el mundo

El convenio tiene cuatro capítulos, en los que además de definirse una serie de terminologías en común, se establecen tres ejes esenciales para hacer frente a los delitos informáticos:

En el primer eje se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática. Es decir, en este capítulo se definen los delitos y se los clasifica en 4 categorías:

- *Delitos que tienen a la tecnología como fin:* son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.

- *Delitos que tienen a la tecnología como medio:* se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.

- *Delitos relacionados con el contenido:* establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

- *Delitos relacionados con infracciones a la propiedad intelectual:* se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc.

En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato

electrónico. Entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

El último eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre **evidencia digital**, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición.

La **evidencia digital** es volátil e intangible, es decir, puede desaparecer o ser alterada muy rápido, por lo que las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas. Para esto, se requiere un proceso penal ágil y eficiente, con esfuerzo organizado por parte de los países. En este capítulo se establece la red 24×7, un punto de contacto que debe funcionar las 24 horas, los 7 días a la semana y asegurar una rápida asistencia entre las partes.

De esta manera, y según se define en el preámbulo del convenio, la armonización en ciberdelincuencia se logra tipificando conductas de delitos informáticos similares en todos los países, unificando normas procesales de cualquier delito que tengan evidencia digital y a través de una cooperación internacional, similar y armónica en todos los países.

17. **LEY FEDERAL DE SEGURIDAD PRIVADA**

Esta Ley define en el marco jurídico nacional que es la Seguridad de la Información. Artículos Relevantes:

Artículo 15.- Es competencia de la Secretaría, por conducto de la Dirección General, autorizar los servicios de Seguridad Privada, cuando estos se presten en dos o más entidades federativas y de acuerdo a las modalidades siguientes**: V. Seguridad de la información**. *Consiste en la preservación, integridad y disponibilidad de la información del prestatario, a través de sistemas de administración de seguridad, de bases de datos, redes locales, corporativas y globales, sistemas de cómputo, transacciones electrónicas, así como respaldo y recuperación de dicha información, sea ésta documental, electrónica o multimedia;"*

18. **ESTRATEGIA NACIONAL DE CIBERSEGURIDAD**

La estrategia nacional de seguridad cibernética de México se desarrolló en colaboración con el Comité Interamericano contra el Terrorismo. La estrategia subraya el compromiso de México con combatir el delito cibernético y reconoce la importancia de la información y la comunicación tecnologías en el desarrollo político, social y económico de México.

19. **PRINCIPIOS RECTORES DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD**

La estrategia se basa en tres principios rectores:

a. derechos humanos,
b. gestión de riesgos y
c. cooperación multidisciplinaria.

20. **OBJETIVOS ESTRATEGICOS DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD**

El documento se apoya en cinco objetivos estratégicos:

1. Sociedad y derechos;
2. Economía e innovación;
3. Instituciones públicas;
4. Seguridad Pública; y
5. Seguridad nacional

- **ESTÁNDARES EN CIBERSEGURIDAD**

Los estándares de Ciberseguridad son técnicas generalmente establecidas en materiales publicados que intentan proteger el entorno cibernético de un usuario u organización. [2] Este entorno incluye a los propios usuarios, redes, dispositivos, todo el software, procesos, información en almacenamiento o tránsito, aplicaciones, servicios y sistemas que pueden conectarse directa o indirectamente a las redes.

- **ISO/IEC**

Que publicada en octubre de 2013 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).Su nombre completo es ISO / IEC 27001: 2013 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información

ISO / IEC 27001 especifica formalmente un sistema de gestión destinado a brindar seguridad de la información bajo control explícito de gestión.

ISO/IEC 27002 incorpora principalmente parte 1 del estándar de buenas prácticas de gestión de seguridad BS 7799 . proporciona un esquema o guía de buenas prácticas para la gestión de la seguridad cibernética

- **NERC**

Un intento inicial para crear para crear estándares de seguridad de la información para la industria de la energía eléctrica fue creado por NERC en 2003 y fue conocido como NERC CSS (Cyber Security Standards) Después de las pautas de CSS, NERC evolucionó y mejoró esos requisitos. El estándar de seguridad NERC moderno más ampliamente reconocido es NERC 1300, que es una modificación / actualización de NERC 1200. La versión más nueva de NERC 1300 se llama CIP-002-3 a CIP-009-3 (CIP = Protección de infraestructura crítica). Estas normas se utilizan para asegurar sistemas eléctricos a granel, aunque NERC ha creado normas dentro de otras áreas. Los estándares del sistema eléctrico a granel también brindan administración de seguridad de la red y al mismo tiempo respaldan los procesos industriales de mejores prácticas.

- **NIST**

El Marco de Seguridad Cibernética del NIST (NIST CSF) "proporciona una taxonomía de alto nivel de resultados de seguridad cibernética y una metodología para evaluar y gestionar esos resultados". Su objetivo es ayudar a las organizaciones del sector privado que proporcionan infraestructura crítica con orientación sobre cómo protegerla, junto con protecciones relevantes para la privacidad y las libertades civiles.

21. **COBIT**

COBIT (Objetivos de control para la información y las tecnologías relacionadas) es un marco creado por ISACA para la gestión de la tecnología de la información y el gobierno de TI.
El marco define un conjunto de procesos genéricos para la gestión de TI, con cada proceso definido junto con entradas y salidas del proceso, actividades clave del proceso, objetivos del proceso, medidas de rendimiento y un modelo de madurez elemental.

22. **ISACA**

Es el acrónimo de ***Information Systems Audit and Control Association*** (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

ISACA lanzó COBIT por primera vez en 1996, originalmente como un conjunto de objetivos de control [se necesita aclaración] para ayudar a la comunidad de auditoría financiera a maniobrar mejor en entornos

relacionados con TI. [COBIT 5, lanzado en 2012, se basa en los marcos COBIT 4.1, Val IT 2.0 y Risk IT y se basa en el Marco de Aseguramiento de TI (ITAF) de ISACA y el Modelo de Negocio para la Seguridad de la Información

23. GOBIERNO TIC

Gobierno de TI es el alineamiento de las Tecnologías de la información y la comunicación (TI) con la estrategia del negocio. Hereda las metas y la estrategia a todos los departamentos de la empresa, y proporciona el mejor uso de la tecnología y de sus estructuras organizativas para alcanzarlas.

24. INGENIERÍA INVERSA

La ingeniería inversa o retroingeniería es el proceso llevado a cabo con el objetivo de obtener información o un diseño a partir de un producto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí y cuál fue el proceso de fabricación

TÉCNICAS DE ANONIMATO

25. Uso de Proxys

El **uso** de un **proxy** hace que todas las solicitudes sean hechas por el servidor **proxy**, no por tu enlace de Internet, eso hace que el proveedor de tu servicio a Internet (ISP) no sepa a qué destinos de Internet te estás dirigiendo.

26. Virtual Private Networks (VPN)

Una **red privada virtual** (**RPV**) (en inglés, ***Virtual Private Network***, **VPN**) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.

27. The Onion Router Browser (TOR)

TOR - El Onion Router Tor Browser es el navegador web más utilizado para navegar por los sitios web de Onion, cuyo nombre es sinónimo de Deep Web. Este navegador es uno de los navegadores web más potentes que te ayudan a proteger tu anonimato en esta parte de la web.

28. METASPLOIT FRAMEWORK

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "**Pentesting**" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

29. KALI LINUX

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.
Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

30. ¿QUÉ ES EL *RANSOMWARE*?

El ransomware es un tipo de *malware*, **cuyo objetivo es conseguir el control del equipo** para cifrar el acceso al mismo y/o sus archivos o discos duros **a cambio de una condición que suele el pago de un rescate** por parte del propietario. Según ***Business Insider***, el Ransomware genera más de 2**5 millones de dólares** cada año a los cibercriminales.

31. SEGURIDAD EN LAS CADENAS DE SUMINISTROS

Cada vez es más habitual ver en la misma frase los conceptos 'cadena de suministro' y 'servicios **TIC**' y es que, desde la expansión de la computación en la nube (del inglés cloud computing), conocida también como servicios en la nube, informática en la nube, nube de cómputo (la informática en la nube es el suministro de servicios informáticos, incluidos servidores, almacenamiento, bases de datos, redes, software, análisis e inteligencia, a través de Internet "la nube"), los servicios TIC cada vez son más asimilables a un suministro más de la propuesta de valor de cualquier cadena de producción que podamos pensar. El Cloud Coputing (Servicios en la nube) proporciona un entorno seguro y sencillo de utilizar, en el cual tanto desarrolladores como usuarios pueden encontrar una gran selección de recursos que facilitan en gran medida la gestión de las aplicaciones. Podemos diferenciar entre tres grandes grupos:

- **Infraestructura (IaaS)**
- **Plataforma (PaaS)**
- **Software (SaaS)**

32. CIBERRESILIENCIA

La ciberresiliencia o resiliencia cibernética surge de la aptitud y suficiencia de las empresas de proteger sus sistemas informáticos ante un ataque cibernético. Es así, como las organizaciones a lo largo de los años han ido adquiriendo diversas estructuras tecnológicas que favorecen los procesos y agilizan la producción de sus empleados. Las empresas deberán hacer **uso de diversos programas y herramientas con plataformas orientadas a eliminar los riesgos informáticos en los que se puede estar vulnerable**. Y esto se ha convertido casi en una tendencia que invita a la ***ciberresiliencia*** en las compañías para que reconsideren sus prácticas en Ciberseguirad

33. CENTRO NACIONAL DE RESPUESTA A INCIDENTES CIBERNÉTICOS DE LA POLICÍA FEDERAL

La Policía Federal alberga al **Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT- MX), instancia encargada de vigilar la integridad de la infraestructura tecnológica estratégica del país.** El CERT-MX opera áreas especializadas en temas de prevención e investigación de este tipo de ilícitos y **es la única autoridad acreditada a nivel federal para realizar intercambio de información con policías cibernéticas nacionales y organismos policiales internacionales, En materia de prevención, se intercambia información con agencias internacionales sobre nuevas amenazas cibernéticas descubiertas en servicios, protocolos y fabricantes tanto de software como de hardware**; ello contribuye a brindar una mejor atención y orientación a la ciudadanía.