Iniciativa de ley

1. Phishing

- Según la ley, ¿cómo se define y tipifica el phishing como delito cibernético?
- ¿Qué elementos deben estar presentes para que se considere que un ataque de phishing ha violado la ley de ciberseguridad?
- ¿Cuáles son las sanciones previstas en la ley para aquellos que cometan phishing, especialmente cuando se compromete información financiera o personal?
- ¿Cómo puede un abogado defender a una empresa afectada por phishing si esta evitó divulgar el ataque para proteger su imagen? ¿Qué obligaciones tiene la empresa bajo esta ley?
- En un caso de phishing que afecte a múltiples usuarios, ¿cómo puede la ley garantizar una reparación digna para las víctimas afectadas?

2. Ransomware

- ¿Cómo clasifica la ley los ataques de ransomware y qué sanciones impone a los perpetradores?
- ¿Qué procedimientos establece la ley para la recolección y preservación de pruebas en un caso de ransomware?
- ¿Cuáles son las responsabilidades de las entidades afectadas por ransomware en cuanto a notificar a las autoridades y proteger la integridad de los datos?
- ¿Qué mecanismos de recuperación establece la ley para ayudar a las organizaciones víctimas de ataques de ransomware a restaurar sus operaciones?
- ¿Cómo pueden las organizaciones afectadas justificar el pago de un rescate sin ser penalizadas bajo esta ley?

3. Ingeniería Social

- ¿De qué manera regula la ley los delitos cometidos a través de técnicas de ingeniería social?
- ¿Qué penas se imponen a quienes utilizan la ingeniería social para obtener acceso no autorizado a datos o sistemas informáticos?
- ¿Cómo pueden las empresas protegerse de ser víctimas de ingeniería social según los lineamientos de esta ley?
- ¿Qué medidas de detección y prevención de ingeniería social exige la ley a las entidades gestoras de infraestructuras críticas?

- ¿Cómo puede la ley apoyar a las víctimas de un ataque basado en ingeniería social, garantizando la recuperación de los datos afectados?

4. Responsabilidad de las Empresas

- ¿Cuáles son las responsabilidades y obligaciones de las empresas para evitar ser cómplices en casos de ciberdelitos como phishing y ransomware?
- ¿Qué tipo de colaboración se espera de las empresas con las autoridades en la preservación y presentación de datos ante un incidente de phishing o ransomware?
- En casos donde la vulnerabilidad proviene de un error humano (como en ingeniería social), ¿qué tipo de defensa puede plantearse para la empresa ante un posible incumplimiento de medidas de seguridad?

5. Medidas de Mitigación y Recuperación

- ¿Qué tipo de programas y políticas de ciberseguridad deben implementar las organizaciones para protegerse de ataques como phishing, ransomware e ingeniería social según la ley?
- ¿Qué mecanismos de recuperación ofrece la ley para las víctimas de ciberdelitos, y cómo pueden las empresas usarlos para minimizar los daños después de un ataque?
- ¿Cómo puede un abogado argumentar que una organización ha cumplido con los requisitos de la ley para mitigar los efectos de un ataque cibernético?

6. Cooperación Internacional

- ¿Qué mecanismos de cooperación internacional están previstos en la ley para investigar y procesar a los responsables de ataques de phishing y ransomware originados fuera de Guatemala?
- ¿Cómo puede la empresa colaboradora en la persecución de los ciberdelincuentes beneficiarse de los tratados internacionales previstos en la ley?

Norma ISO 27001

1. Cumplimiento de la Norma ISO 27001

- ¿La organización está certificada bajo la norma ISO 27001? ¿Qué partes de su sistema de gestión de seguridad de la información han sido auditadas y aprobadas?
- ¿Cómo puede demostrarse que la organización ha implementado los controles de seguridad requeridos por la norma ISO 27001?
- ¿Existen registros de auditorías internas y externas que prueben que el sistema de gestión de la seguridad de la información cumple con los requisitos de la norma?

2. Gestión de Riesgos

- ¿La organización ha realizado una evaluación formal de riesgos para identificar amenazas a la seguridad de la información, conforme a los requisitos de ISO 27001?
- ¿Se documentaron las acciones tomadas para mitigar los riesgos asociados con el incidente de ciberseguridad en cuestión?
- ¿Cómo puede la organización demostrar que implementó controles específicos para minimizar los riesgos identificados en su proceso de gestión de riesgos?

3. Controles de Seguridad

- ¿Qué controles de seguridad específicos (del Anexo A de la ISO 27001) estaban implementados en la organización al momento del incidente?
- ¿Cómo puede la organización demostrar que los controles relacionados con **phishing**, **ransomware**, o **ingeniería social** estaban operando correctamente?
- ¿Se siguió un procedimiento documentado para la implementación, monitoreo y mejora de los controles de seguridad de la información?

4. Respuesta a Incidentes

- ¿Qué medidas de **respuesta a incidentes** fueron tomadas por la organización, y están alineadas con los procedimientos establecidos en la ISO 27001?
- ¿La organización tiene un plan documentado de **gestión de incidentes** de seguridad de la información? ¿Este plan fue ejecutado correctamente en el incidente de ciberseguridad?
- ¿Se notificó a las autoridades y a las partes interesadas de acuerdo con los requisitos de la norma y la legislación vigente?

5. Capacitación del Personal

- ¿Cómo puede demostrar la organización que el personal ha sido **capacitado** regularmente en las políticas de seguridad de la información, incluyendo la identificación de amenazas como el phishing o la ingeniería social?
- ¿Qué registros de capacitación tiene la organización que evidencien que los empleados estaban preparados para manejar incidentes de ciberseguridad?
- ¿El personal relevante estaba consciente de los riesgos y las políticas de seguridad de la información, de acuerdo con las disposiciones de la norma ISO 27001?

6. Auditoría y Mejora Continua

- ¿La organización ha llevado a cabo **auditorías internas y externas** sobre su sistema de gestión de seguridad de la información, según lo exigido por la ISO 27001?
- ¿Cómo puede la organización demostrar que ha implementado **mejoras continuas** en sus políticas y controles de seguridad?

- ¿Existen informes de auditoría que muestren que se han abordado las no conformidades encontradas durante las auditorías, y cómo?

7. Cumplimiento Legal

- ¿La organización ha identificado y cumplido con todos los **requisitos legales** aplicables relacionados con la seguridad de la información, de acuerdo con la norma?
- ¿Cómo puede la organización demostrar que tomó las medidas necesarias para cumplir con la **Iniciativa de Ley 6347** de Guatemala u otras normativas aplicables al incidente de ciberseguridad?

8. Registro y Documentación de Incidentes

- ¿Qué **evidencias documentales** tiene la organización para probar la existencia de un **sistema de gestión de incidentes** eficaz que cumpla con ISO 27001?
- ¿Se registraron y documentaron adecuadamente los eventos previos, durante y después del incidente?
- ¿Existen registros que muestren cómo se gestionó el incidente, incluyendo la recolección de pruebas y la preservación de los datos?

9. Protección de Datos y Confidencialidad

- ¿Cómo puede la organización demostrar que ha protegido la **confidencialidad** de los datos personales o sensibles, conforme a los principios de la ISO 27001?
- ¿Qué medidas estaban implementadas para asegurar que no se violara la integridad o disponibilidad de la información durante el ataque?
- ¿La organización ha seguido los procedimientos para notificar y remediar violaciones de datos, tal como lo exige la norma?

10. Gestión de Proveedores y Terceros

- ¿La organización tenía políticas de **seguridad en la cadena de suministro** o en la relación con proveedores, según lo estipulado por la ISO 27001?
- ¿Cómo puede la organización demostrar que los servicios de terceros utilizados (por ejemplo, proveedores de servicios en la nube) cumplían con los requisitos de seguridad de la información?
- ¿Qué controles se implementaron para gestionar los riesgos de seguridad de la información provenientes de **terceros**?

11. Controles Preventivos y Correctivos

- ¿Qué **controles preventivos** estaban en su lugar antes del incidente de ciberseguridad y cómo puede demostrarse su eficacia?

- Después del incidente, ¿qué **acciones correctivas** se tomaron para evitar futuros eventos similares, y cómo estas se alinean con las recomendaciones de mejora continua de la ISO 27001?

12. Uso de la Criptografía y Control de Acceso

- ¿Cómo puede la organización demostrar el uso adecuado de la **criptografía** para proteger la información sensible, conforme a los lineamientos de la ISO 27001?
- ¿Qué **controles de acceso** estaban implementados para garantizar que solo el personal autorizado tenía acceso a la información crítica?