1. **Activos de Información**

- **Definición**: Cualquier forma de información, ya sea en formato digital, físico o hablado, que tiene valor para la organización y debe ser protegida. Esto incluye datos, sistemas informáticos, redes y otros recursos informáticos.
- **Importancia legal**: Identificar qué información es un activo valioso ayuda a protegerla y justificar las medidas de seguridad adoptadas por la organización.

**2. Sistema de Gestión de Seguridad de la Información (SGSI)**

- **Definición**: Un marco organizado de políticas, procesos, procedimientos y controles implementado para gestionar la seguridad de la información dentro de una organización.
- **Importancia legal**: Probar la existencia de un SGSI demuestra que la organización ha tomado medidas adecuadas para gestionar los riesgos de seguridad.

**3. Confidencialidad**

- **Definición**: Principio de asegurar que la información solo esté disponible para aquellas personas autorizadas para acceder a ella.
- **Importancia legal**: La violación de la confidencialidad puede llevar a consecuencias legales si se compromete información personal o confidencial, como en casos de ciberataques.

**4. Integridad**

- **Definición**: Principio que asegura que la información y sus métodos de procesamiento son precisos y completos, y no han sido alterados de manera no autorizada.
- **Importancia legal**: En casos de manipulación de datos, la falta de integridad puede ser un aspecto clave en la defensa.

**5. Disponibilidad**

- **Definición**: Asegurar que la información esté disponible para su acceso y uso por las personas autorizadas cuando se necesite.
- **Importancia legal**: La interrupción de la disponibilidad de sistemas puede generar responsabilidad legal si afecta la continuidad del negocio o servicios críticos.

**6. Gestión de Riesgos**

- **Definición**: El proceso de identificar, evaluar y mitigar los riesgos a la seguridad de la información. La ISO 27001 exige que se documente y evalúe periódicamente.
- **Importancia legal**: Demostrar que la organización ha gestionado adecuadamente los riesgos puede mitigar su responsabilidad en incidentes de ciberseguridad.

**7. Control de Seguridad de la Información**

- **Definición**: Medidas o mecanismos implementados para proteger la confidencialidad, integridad y disponibilidad de los activos de información. Los controles están listados en el **Anexo A** de la ISO 27001.
- **Importancia legal**: Los controles documentados ayudan a demostrar que la organización ha tomado medidas para prevenir y mitigar incidentes.

**8. Amenaza**

- **Definición**: Cualquier circunstancia o evento que pueda tener un impacto negativo en la seguridad de la información, como un ataque cibernético, desastres naturales o errores humanos.
- **Importancia legal**: Identificar y prevenir amenazas es esencial en la gestión de riesgos y puede ser utilizado como argumento en la defensa.

**9. Vulnerabilidad**

- **Definición**: Debilidad en un sistema de seguridad que puede ser explotada por una amenaza para obtener acceso no autorizado a datos o sistemas.
- **Importancia legal**: Las organizaciones deben demostrar que han abordado vulnerabilidades para reducir el riesgo de ciberataques.

**10. Auditoría Interna**

- **Definición**: Proceso de revisión regular realizado por la organización para verificar que su sistema de gestión de la seguridad de la información cumple con los requisitos de la norma y funciona de manera efectiva.
- **Importancia legal**: Las auditorías internas pueden ser usadas como evidencia de que la organización ha supervisado y mejorado sus controles de seguridad.

**11. Mejora Continua**

- **Definición**: Proceso de revisión constante para mejorar las políticas, procesos y controles de seguridad de la información de una organización.
- **Importancia legal**: Demostrar que la organización ha tomado medidas para mejorar su seguridad tras un incidente puede reducir su responsabilidad legal.

**12. Declaración de Aplicabilidad (SoA)**

- **Definición**: Un documento requerido por la ISO 27001 que especifica qué controles de seguridad han sido seleccionados para mitigar riesgos específicos, y justifica por qué se incluyen o excluyen ciertos controles.
- **Importancia legal**: La SoA puede ser una pieza crucial en la defensa, ya que muestra qué medidas de seguridad estaban en su lugar y por qué.

**13. Incidente de Seguridad de la Información**

- **Definición**: Un evento no deseado que compromete la confidencialidad, integridad o disponibilidad de la información.
- **Importancia legal**: La respuesta adecuada y documentada a un incidente de seguridad puede ser clave en la defensa contra acusaciones de negligencia.

**14. Plan de Respuesta a Incidentes**

- **Definición**: Un conjunto de procedimientos que una organización sigue para manejar y mitigar los efectos de un incidente de seguridad de la información.
- **Importancia legal**: Demostrar que la organización siguió su plan de respuesta a incidentes puede mitigar su responsabilidad y mostrar que actuó de manera diligente.

**15. Partes Interesadas**

- **Definición**: Cualquier persona u organización que pueda verse afectada por las decisiones o actividades relacionadas con la seguridad de la información, incluidos clientes, empleados, proveedores y reguladores.
- **Importancia legal**: La identificación y consideración de las expectativas de las partes interesadas es clave para demostrar cumplimiento con la norma.

**16. Evaluación de Riesgos**

- **Definición**: Proceso de analizar el impacto de las amenazas y vulnerabilidades sobre los activos de información de la organización, con el fin de priorizar los riesgos.
- **Importancia legal**: Mostrar que la organización realizó evaluaciones de riesgos antes del incidente ayuda a justificar que se tomaron medidas razonables.

**17. Controles Físicos**

- **Definición**: Medidas implementadas para proteger los activos de información de acceso no autorizado, daño físico o interferencia.
- **Importancia legal**: Los controles físicos, como cámaras de seguridad o acceso restringido, son parte de una defensa sólida en caso de incidentes que involucren intrusión física.

**18. Criptografía**

- **Definición**: El uso de técnicas de cifrado para proteger la información confidencial durante la transmisión o almacenamiento.
- **Importancia legal**: El uso de criptografía puede ser una defensa importante para demostrar que la organización protegió adecuadamente la información sensible.

**19. Monitoreo y Medición del Rendimiento**

- **Definición**: Proceso de supervisión continua de la efectividad de los controles de seguridad implementados.

- **Importancia legal**: Mostrar que la organización monitoreó y ajustó sus controles de seguridad puede ayudar a argumentar que se actuó diligentemente antes del incidente.

**20. Cumplimiento Legal**

- **Definición**: La obligación de cumplir con todas las leyes, regulaciones y normativas aplicables a la seguridad de la información.
- **Importancia legal**: Demostrar que la organización cumple con las leyes locales, como la **Iniciativa de Ley 6347** en Guatemala, refuerza su defensa en caso de litigio.