Fundamentos de Seguridad de la Información
Unidad 2
Glosario

A

Autoridad de control: Organismo encargado de supervisar y hacer cumplir las leyes de protección de datos en un país o región.

C

Capacitación en ciberseguridad: Programas educativos y de entrenamiento diseñados para mejorar la conciencia y las habilidades en materia de seguridad cibernética.

Ciberdelincuencia: Actividades delictivas llevadas a cabo en el ciberespacio, como el hacking, el phishing y el fraude en línea.

Ciberseguridad: Conjunto de medidas y prácticas diseñadas para proteger sistemas, redes y datos contra ataques cibernéticos.

Ciberataques: Ataques maliciosos llevados a cabo por hackers o actores cibernéticos con el objetivo de dañar sistemas informáticos o robar información.

Confidencialidad: Principio de protección de la información que garantiza que los datos personales solo sean accesibles por personas autorizadas.

Consentimiento: Permiso explícito dado por un individuo para el procesamiento de sus datos personales con un propósito específico.

Consentimiento informado: Permiso explícito dado por un individuo después de comprender completamente los términos y condiciones del procesamiento de sus datos personales.

Cooperación internacional: Colaboración entre países para abordar problemas comunes, como la ciberdelincuencia, de manera coordinada y efectiva.

Cooperación policial: Colaboración entre agencias policiales nacionales e internacionales para investigar y combatir la ciberdelincuencia.

Coordinación interinstitucional: Colaboración entre diferentes agencias gubernamentales y sectores para garantizar una respuesta coordinada a amenazas cibernéticas.

Cumplimiento: Adherencia a las disposiciones y regulaciones establecidas por las normativas de protección de datos.

D

Delegado de protección de datos: Persona designada para supervisar y garantizar el cumplimiento de la normativa de protección de datos dentro de una organización.

Delitos informáticos: Crímenes que involucran el uso de computadoras y redes, como el robo de datos, la intrusión en sistemas y el malware.

Derechos de los titulares: Derechos otorgados a las personas sobre sus datos personales, como el acceso, rectificación y eliminación.

E

Estrategia nacional: Plan integral diseñado por un país para abordar los desafíos de la ciberseguridad y proteger sus intereses nacionales.

Evaluación de impacto en la privacidad: Análisis sistemático de los posibles efectos de un proyecto o actividad en la privacidad de los individuos.

Extradición: Proceso legal mediante el cual una persona acusada de un delito en un país puede ser entregada a otro país para ser enjuiciada.

F

Fichero: Conjunto organizado de datos personales, ya sea electrónico o en papel.

G

Gestión de riesgos: Proceso de identificación, evaluación y mitigación de riesgos relacionados con la seguridad cibernética.

I

Infraestructura crítica: Activos físicos, tecnológicos y humanos esenciales para el funcionamiento de una sociedad, como energía, agua y telecomunicaciones.

Intercambio de información: Compartir datos y conocimientos entre países y organizaciones para mejorar la detección y prevención de amenazas cibernéticas.

Investigación digital: Recopilación, análisis y presentación de pruebas digitales en casos de delitos informáticos y ciberdelincuencia.

J

Jurisdicción: Autoridad legal de un país para enjuiciar y hacer cumplir la ley dentro de su territorio, incluso en casos de delitos cibernéticos transfronterizos.

M

Monitoreo y alerta temprana: Vigilancia continua de redes y sistemas para detectar y responder rápidamente a posibles ciberataques.

N

Notificación de violaciones de datos: Obligación de informar a las autoridades y a los individuos afectados sobre cualquier violación de seguridad que afecte a sus datos personales.

P

Privacidad: Derecho fundamental que protege la autonomía y la intimidad de las personas al controlar el acceso a su información personal.

Protección de datos: Conjunto de medidas y regulaciones destinadas a garantizar el manejo adecuado y seguro de la información personal.

Protección de datos personales: Salvaguardar la privacidad y seguridad de la información personal de los individuos en línea, incluidos nombres, direcciones y números de identificación.

Protección de la soberanía digital: Preservación de la independencia y la autonomía de un país en el ciberespacio, incluida la protección de infraestructuras críticas y datos sensibles.

R

Resiliencia cibernética: Capacidad de resistir, adaptarse y recuperarse de ciberataques y otras amenazas cibernéticas.

Responsabilidad: Obligación de las organizaciones de implementar medidas.

Responsable del tratamiento: Persona u organización que determina los propósitos y medios del tratamiento de datos personales.

Resiliencia cibernética: Capacidad de resistir, adaptarse y recuperarse de ciberataques y otras amenazas cibernéticas.

S

Sanciones: Penas o multas impuestas a personas u organizaciones por violar las disposiciones de la ley de protección de datos.

Seguridad de la información: Prácticas y controles diseñados para proteger la confidencialidad, integridad y disponibilidad de la información.

Seguridad de la información de salud: Prácticas y controles diseñados específicamente para proteger la confidencialidad, integridad y disponibilidad de la información médica.

Sanciones: Penas o multas impuestas a personas u organizaciones por violar las disposiciones de la ley de protección de datos.

T

Transferencia internacional de datos: Movimiento de datos personales fuera del territorio nacional a otro país u organización.

Transparencia: Obligación de informar a los individuos sobre cómo se recopilan, utilizan y comparten sus datos personales.

Tratamiento de datos: Cualquier operación realizada con datos personales, como la recopilación, almacenamiento, uso y divulgación.