CAPITULO 1
Nociones de Seguridad de la Información
Aspectos Legales, Regulatorios y Contractuales de la Seguridad

Jenny Torres, PhD.

Aspectos Legales

- El cumplimiento de requisitos legales es un dominio de control importante dentro de ISO 27001. Veamos cuales son las particularidades que una empresa que esté buscando la certificación debería tener en cuenta en los temas relacionados el **cumplimiento legal**.

Convenio de Budapest

Historia

- El Convenio sobre ciberdelincuencia, Convenio de Budapest sobre ciberdelincuencia o Convenio de Budapest es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes.

- Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón y China como estados observadores.

- El convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001.

Convenio de Budapest

Historia

- A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la convención, mientras que otros 16 estados firmaron la convención, pero no la ratificaron.
- El 1 de marzo de 2006 entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético.
- Los estados que lo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobas e insultos.
- Su principal objetivo es "*aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional*"

Convenio de Budapest

Objetivos

- El Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que trata en particular de:
  - infracciones de derechos de autor
  - fraude informático
  - pornografía infantil
  - delitos de odio
  - violaciones de la seguridad en redes.

Reglamento General de Protección de Datos

GDPR

Reglamento General de Protección de Datos

GDPR

- **Derecho a estar informado:** también conocido como derecho a la transparencia de la información e indica que antes de que se recolecten sus datos un sujeto de datos tiene el derecho de saber cómo serán recolectados, procesados, almacenados y con qué propósitos.

- **Derecho al acceso:** luego de que sus datos hayan sido recolectados un sujeto de datos tiene el derecho de saber como se han recolectado los datos existentes como han sido procesados, almacenados y con qué propósitos.

- **Derecho a la corrección** ("Rectificación"): un sujeto de datos tiene el derecho de poder corregir los datos que se encuentren incorrectos o incompletos.

- **Derecho a la eliminación (Derecho a ser olvidado):** un sujeto de datos tiene el derecho de eliminar todos sus datos de manera permanente.

Reglamento General de Protección de Datos

GDPR

- **Derecho a restringir el procesamiento:** un sujeto de datos tiene el derecho de bloquear o eliminar sus datos personales en el momento en el que están siendo procesados o en uso.

- **Derecho a la portabilidad de datos:** un sujeto de datos tiene derecho a mover, copiar, transferir sus datos personales de un controlador a otro en forma segura, en un formato legible y comúnmente usado

- **Derecho a objetar el procesamiento:** Un sujeto de datos tiene derecho a objetar que autoridades o empresas procesen sus datos sin consentimiento explícito y también tiene derecho a detener la inclusión de sus datos en bases de datos de marketing directo

- **Derecho a no ser sujeto de toma de decisiones automatizadas:** Un sujeto de datos tiene el derecho de pedir la intervención humana en lugar de ser objeto de toma de decisiones de solo algoritmos.

Código Orgánico Integral Penal

Ecuador

- Entre otros aspectos delictivos sobre las telecomunicaciones y TICs se incluyen tipificaciones sobre:
  - explotación sexual infantil y adolescente por medios electrónicos e informáticos
  - violación a la intimidad
  - aprovechamiento ilícito de servicios públicos
  - apropiación fraudulenta por medios electrónicos
  - alteración de datos
  - reemplazo o alteración de identificación

Código Orgánico Integral Penal

Ecuador

- comercialización ilícita de equipos terminales móviles
- alteración y suplantación de identidad
- revelación integral de datos
- apropiación lícita de activos patrimoniales
- ataque a la integridad de sistemas informáticos
- delitos contra la información pública
- acceso no consentido a un sistema telemático y de telecomunicaciones
- interceptación de comunicaciones o datos informático.

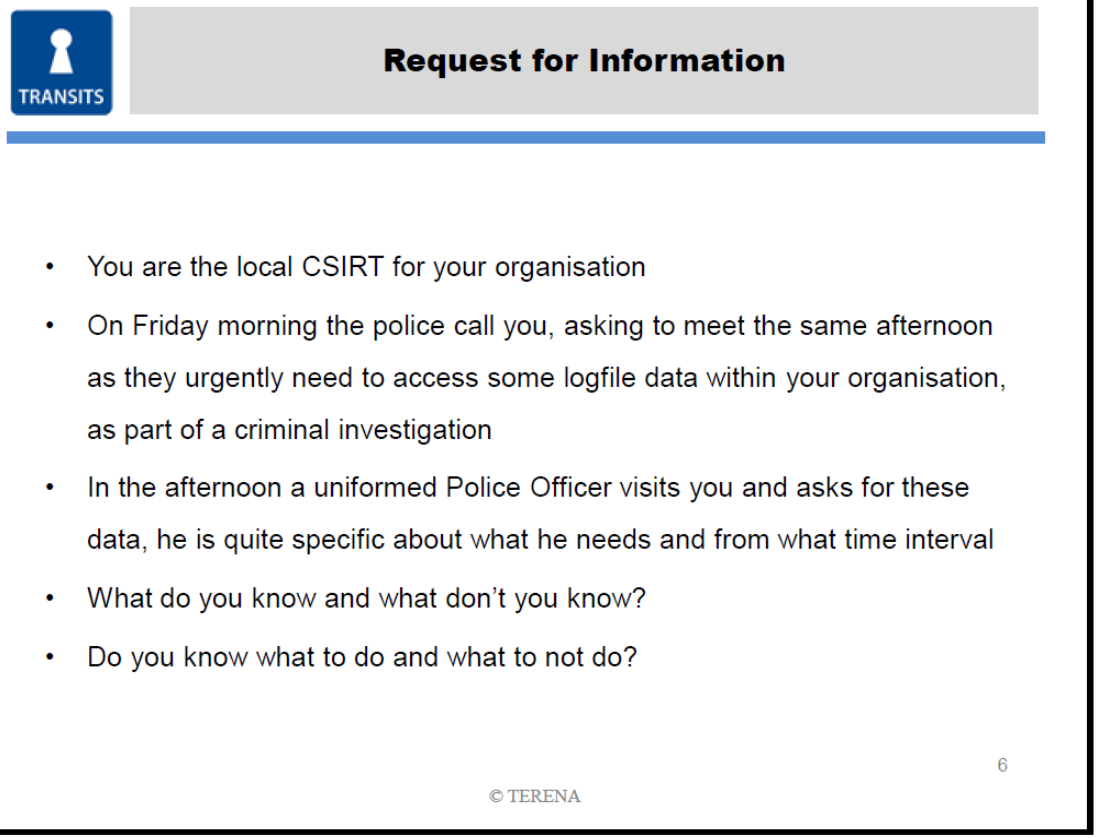
Ley de Comercio Electrónico

Ecuador

- Incluía reformas del anterior Código Penal, entre otras, sobre:
  - infracciones informáticas
  - divulgación fraudulenta de información
  - obtención no autorizada de identidad o datos de seguridad
  - falsificación electrónica
  - daños informáticos
  - uso de las TICs para robo de bienes
  - derecho a la intimidad

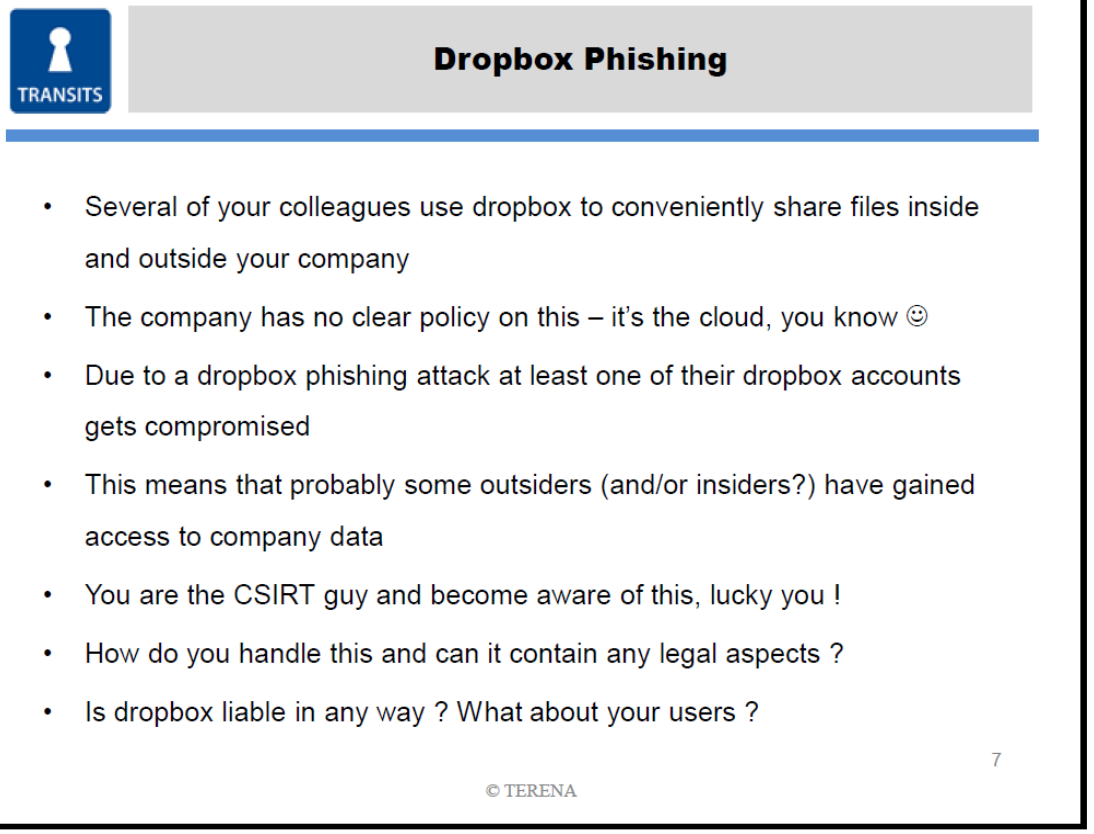
Ejercicios

1.



Ejercicios

2.



Ejercicios

3.

TRANSITS

Abuse by a Colleague

- You are the CSIRT of the Phone Company
- An employee of your company with access to communication logfiles is suspected to have checked the call history of his girlfriend to find if she has been cheating on him
- You think you may need to access his work computer and e-mail to gather evidence, and technically you, or IT, can do this
- Are you allowed to do this by your company policies ?
- What safeguards are there both for your colleague and you?
- Is it possible that you may break the law by doing this?
- Will any evidence gathered stand up in court if needed?

Ejercicios

4.

TRANSITS

Botnet Remedy (Takedown ?)

- You are a very clever CSIRT officer in your university and you find out that many local systems are “owned” by what seems a big international botnet
- You want to remedy the botnet inside but also help to take the botnet down!
- Do you need to report this to the police?
- Does your boss allow you to?
- Does your boss have any clue what the university’s stand is in cases like this?
- Suppose you cooperate with the police – what can you be expected to do and share – and what not to?

Referencias

- INEN (2012) Descripción General y Vocabulario. Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000:2012.

- Stallings, W. (2011) Network Security Essentials 4th edition, New York, US; ISBN:13: 978-1587052460: Prentice-Hall.