ISEC LEGAL

Ventura Daniel Bustos
Martin Vila
Isec.legal@isec-global.com

A quien le hago caso?

Ingeniero TODO SEGURO
Vs
Abogado Dr Siempre LA GANO

Que pasa si el Director nos pregunta ...

Es legal revisarle los mails a los empleados?

Es prueba LEGAL la firma de CONVENIOS de CONFIDENCIALIDAD del Personal?

Qué tengo que hacer si SOSPECHO de un usuario?

Qué pasa si encuentro Pornografía Infantil en una PC de un usuario?

Si recibimos un mail con injurias, extorsión, etc., QUE TENGO QUE HACER?

Y si soy Administrador y me denuncian por Invación a la Privacidad de la Gente?

Los logs, sirven de prueba legal?

Qué hago con la Ley de Habeas Data?

Hay otras Leyes?

Y si no hay ley que hago?

Si soy Director o Gerente, soy responsable por lo que hagan mis empleados?

Hay alguien preso por esto?

Qué puedo hacer para prevenirme?

Qué hago si YA ME PASO???

Qué HACEMOS entonces????

PRIMEROS PASOS

Entender la Relación entre RIESGOS y DELITOS / Inconductas Informáticas

Lo primero que tenemos que reconocer que muchos Problemas se convierten no solo en RIESGOS de NEGOCIOS sino también en CONTINGENCIAS LEGALES para la Compañía y sus FUNCIONARIOS

Y a veces los Ingenieros NO entendemos bien si un DELITO INFORMATICO es ...

Matar al jefe mediante un GOLPE preciso y certero en la cabeza con una NOTEBOOK
(si no, no se consideraria informatico).

Destruir el mp3 de su compa;ero de trabajo asi se termina de una vez la CUMBIA en la oficina.

Leerle el registro del CHAT a su esposa a la noche cuando llega para ver si es verdad que sale con el Profesor de Salsa.

Algunos ejemplos:

- **Acceso no autorizado:**
  - El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario.

- **Destrucción de datos:**
  - Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.

- **Infracción de los derechos de autor:**
  - Copia, distribución, cesión y comunicación pública de los programas.

- **Infracción del copyright de bases de datos:**
  - El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los archivos contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

- **Interceptación de e-mail:**
  - En este caso, se propone una ampliación de los preceptos que castigan la violación de correspondencia y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

- **Estafas electrónicas:**
  - La proliferación de las compras vía Internet permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

- **Transferencias de fondos:**
  - Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

- **Espionaje:**
  - Se han dado casos de accesos no autorizados a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.

- **Espionaje industrial:**
  - También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

- **Terrorismo**:
  - La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha sido aprovechado por grupos terroristas para remitir consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

- **Narcotráfico**:
  - Existen mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

- Otros delitos:
  - Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, etc.

- **Usos comerciales no éticos**:
  - Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

- **Usos particulares no éticos**:
  - Emplear los recursos informáticos para distribuir obscenidades, insultos, etc.

- **Publicación no autorizada**:
  - Poner a disposición de usuarios determinada información cuyo acceso puede no estar permitido o que requiera autorización previa o erogación económica. Ejemplo de esto es e intercambio gratuito de música. Esto puede ocurrir al conectar un servidor a Internet o el envío a través de correos electrónicos.

- **Acceso a la información privada de las personas:**:
  - Puede darse a través de la publicación de información personal residente en bases de datos y/o en registros de monitoreos de los sistemas, o por la intercepción de los correos electrónicos enviados por Internet.

Y donde esta el RIESGO concretamente???

El primer RIESGO:

"Solo se que no se nada"

COMO HAGO DE TODO ESTO

UN PROCESO DE GESTION

ORDENADO Y CONTINUO ???

Paso 1

ENTENDER EL PROBLEMA

CAPACITACION

CONCLUSION 1:

PREGUNTEMOS A LOS QUE SABEN

Siempre es IMPRESCINDIBLE definir las políticas de seguridad con el ASESORAMIENTO y la APROBACION FORMAL del área de LEGALES de la COMPAÑIA

CONCLUSION 2:

Hay que CONOCER CUALES SON LAS CONTINGENCIAS LEGALES
Para luego definir si
Una POLITICA DE SEGURIDAD
Podemos o no aplicarla

CONCLUSION 3:

Tendremos que TRABAJAR EN FORMA CONJUNTA los INGENIEROS con los ABOGADOS en estos temas