

Seminario red iberoamericana de protección de datos
Montevideo

DENTONS

La protección de datos personales en un nuevo contexto de riesgo Problemáticas y estrategias

3 noviembre 2015

Introducción

- El contexto de riesgo
 - Riesgo – principales vulnerabilidades
- Estrategias
- Tácticas
 - Evaluación del riesgo
 - Desarrollo de políticas claras y accesibles
 - Gobernanza útil y eficaz a todo nivel
 - Respuesta a los incidentes
 - Intrusiones
 - Quejas
- Los temas del día
- En resumen

El contexto de riesgo actual - Algunas estadísticas

1. La frecuencia

- FireEye encuentra que el 97% de las empresas estadounidenses han sufrido una intrusión en 2014

2. La complacencia

- Una encuesta de ICSPA revela que 80 % de la empresas encuestadas no conocen su riesgo

3. El valor competitivo

- Encuestas de negocios muestran que el 46 % de los encuestados han dejado o evitado una empresa que ha sufrida un intrusión

Riesgo - principales vulnerabilidades

- La ciber-seguridad cibernética, por
 - Delegación excesiva a los administradores de TI
 - La subestimación del riesgo

Re: Hack attacks hit home: « The kind of thing that CEOs get fired for »
Theresa Tedesco, *National Post*, 2.2.2015

- El error humano, por
 - La falta de littératie digitales
 - Falta de supervisión
- La indiscreción de los empleados, por
 - Formación basada en normas y no en la ética
 - Control de acceso insuficiente

Sitio web Dentons...

Estrategias

- La seguridad es una cuestión organizacional, no solo de la TI
- Reside en un ecosistema de medidas
 - Físicas
 - Tecnológicas
 - Administrativas

Objetivo : Coordinado e integral

Tácticas

1. La evaluación de riesgo ambiental e interno
2. El desarrollo de un conjunto de políticas adecuadas
3. La adopción de una estructura de gobernanza para garantizar el cumplimiento
4. Mecanismos de respuesta a los incidentes

Objetivo : Protección correspondiente al riesgo

1. Evaluación del riesgo

1. Medio Ambiente: tendencias clave

2. Interno

- Controles físicos: es el acceso a áreas repositórios de datos personales controlado?
- Los controles técnicos: son las medidas de seguridad (cifrado, codificación, etc...) correspondientes a la sensibilidad de los datos?
- Controles administrativos: existen directorios de datos, restricciones de acceso, asignación de responsabilidades, formación del personal para la protección de datos?

➤ **Objetivo: implementar un ecosistema de protección**

Re: Rapport spécial au Parlement, CPVP, Enquête sur la perte d'un disque dur à EDSC, 25,3.2014

2. Desarrollo de políticas claras y accesibles

- Para los empleados,
 - Sobre la base de la ética
 - Adaptadas a las tecnologías del trabajo
 - Acompañadas de formación
 - Incluyendo plan de respuesta temprano a incidentes

➤ **Objetivo : El empleado es responsable de la protección de datos**

- Para los usuarios,
 - Accesibles y prominentes
 - Adaptadas a la organización
 - Acompañadas de remedios
 - Con opciones claras y efectivas de consentimiento

➤ **Objetivo: El usuario controla sus datos**

3. Gobernanza útil y eficaz a todo nivel

- El C.A: el deber de vigilancia

Re: The Dangers of Ignorance in the Boardroom. Prof. Errol Mendes, Frontline Security 2014 (Vol 9, No 3)

- El C.D. y la alta dirección : el deber de gestión
- El funcionario designado públicamente: i) políticas y medidas de protección, ii) garantizar la aplicación y el informe, iii) abordar las cuestiones y quejas, iv) coordinar la respuesta a incidentes
- Inventario de los bases de datos
- Colaboración vida privada y TI
- Gerentes: supervisar la implementación de las políticas
- Empleados: hacer cumplir las políticas como inherente al servicio al cliente

Re: Un programme de gestion de la protection de la vie privée : la clé de la responsabilité, CPVP, 2012

➤ **Objetivo : integración al mandato de la organización**

4 Respuesta a los incidentes

4.1 Intrusiones

- Aplicación de un plan de respuesta anticipada
 - Convocación del Comitado de respuesta
 - Evaluación del alcance de la intrusión y la lesión
 - Medidas correctivas
 - Decisión relativa a la notificación
 - Despliegue de la estrategia de comunicación
 - Asignación de responsabilidades
 - Seguimiento hasta la resolución jurídica y técnica
 - Recurso a un especialista si es necesario

➤ **Objetivo: Protección en la respuesta**

*Re: A day in the life of privacy issues for corporate counsel.
web sitio Dentons*

4.2 Quejas

- Asistencia al demandante como inherente al servicio cliente
- Reconocimiento de temas sensibles de la protección de la privacidad
- Junto con el regulador, en su caso
 - Transparencia
 - Buena fe
 - Humildad
- Evaluación compasiva y realista del alcance del incidente
- Recurso a un especialista si es necesario

➤ **Objetivo : resolución sin queja**

Los temas del día

- ¿La publicidad en línea o privacidad?
 - Informe de Investigación de Canadá sobre Google, enero 2014 y sobre Bell de abril 2015
- ¿El control o la nube?
 - ISO/IEC 27018 ofrece ambas cosas
 - Seguridad en la nube
 - Un marco normativo que garantiza el control por parte del cliente
- ¿BYOD?
 - Política clara de utilización de dispositivos personales por los empleados

➤ **Objetivo: control individual sobre su respeto de datos**

En resumen

La practica demuestra elementos básicos de éxito:

1. Un enfoque multidisciplinario
2. Gobernado por un marco organizacional concerado
3. Basado sobre la realidad de riesgo
4. Apoyado sobre un ecosistema de medidas de protección
5. Acompañado de remedios

Gracias

The Dentons logo consists of the word "DENTONS" in white, uppercase, sans-serif font, centered within a purple arrow-shaped graphic that points to the right. This graphic is set against a black rectangular background.

Dentons Canada.

99, Bank

Oficina 1420

Ottawa (Ontario)

K1P 1H4

Canada