Introducción

- En los despachos de abogados se maneja muchísima información y en gran parte esta es de carácter privado o confidencial. Desde la experiencia de INCIBE se introducirá a las posibles ciberamenazas y los riesgos a los que se está expuesto.

¿Realmente mi despacho necesita de la ciberseguridad?

- A partir de un caso personal (infección por malware) se indicará la importancia de conocer a qué riesgos está expuesto una empresa en este caso un despacho y la necesidad de "saber de ciberseguridad" para prevenir pérdidas o el activo más importante: la información.
- Posibilidad de cierre del despacho por la falta del activo
- Conclusión: se ha de mejorar la ciberseguridad

¿Conoces los riesgos que pueden afectar a tu despacho?

- Existen numerosas situaciones y riesgos a los que estamos expuestos y que si no se conocen, difícilmente van a poder ser subsanados o gestionados:
  - Empleados descontentos
  - Problemas de hardware
  - Ataques dirigidos
  - Etc.

¿Es necesario subcontratar servicios de ciberseguridad/TIC?

- Casi todas las empresas contratan o subcontratan servicios TIC ¿pero conocen las cuestiones más importantes a la hora de contratar servicios de ciberseguridad?
- Elementos básicos para confiar en la ciberseguridad de un proveedor (NDA, SLA, etc.)

Plan director de seguridad (PDS): cómo nos puede ayudar

- Por dónde empezamos el plan
- Cómo lo implementamos
  - Explicación de las fases del plan
- ¿El plan es suficiente para no preocuparse de nada más?

Protección del puesto de trabajo: recomendaciones para desempeñar nuestras sinergias con la tecnología con seguridad

- Los "alrededores" de nuestro escritorio (post-it's, información confidencial, smartphones, papelera, etc.)
- Crear contraseñas seguras
  - Robustas
  - Una para cada servicio
  - Doble factor cuando sea posible
  - Buenas prácticas
- Aplicaciones seguras
  - Actualizaciones

- Software legal
- Información portátil (pendrives, etc.)
  - Fuga de información (pérdida o robo)
  - Cifrado de archivos
  - Propagación de malware

Necesito que la información de mis clientes esté segura ¿Cómo se consigue?

- Políticas de seguridad para:
  - Información importante
  - Datos personales o confidenciales
  - Cómo se accede a la información

Si trabajas desde casa o accedes a servicios de tu despacho remotamente, tienes que conocer a qué te expones y cómo protegerte

- Acceso desde el Smartphone o Tablet
  - Proteger el dispositivo con contraseña
  - Cifrar los archivos en tránsito
  - No instalar aplicaciones que no sean necesarias
  - Usar MDM en la medida de lo posible
- Trabajando desde casa
  - Trabajar desde un dispositivo seguro teniendo los mismos cuidados que en la oficina
  - Usar servicios que sean seguros (la nube) y en caso de duda, cifrar los archivos.

Tengo mucho miedo a los ransomware. Si me secuestran los ordenadores del despacho estoy perdido. ¿Cómo podemos hacer frente a estos problemas?

- Plan de contingencia
  - Copias de seguridad (cómo, cuándo y dónde), apagones, incendios, etc.
  - Revisión del plan
- Gestión de riesgos
  - Identificar los activos y las amenazas
  - Evaluar y gestionar los riegos
  - Acciones a tomar

Los datos y la LOPD

- Aspectos básicos
  - Derechos ARCO
- La AGPD
- Tengo una web con información sobre mi despacho y un formulario donde los usuarios pueden hacerme preguntas, pero ¿Estoy cumpliendo con todos los requisitos que exige la ley?

Crear cultura en ciberseguridad en los despachos: los usuarios son la parte más importante

- ¡Que no te engañen! Ingeniería social
- Formación y concienciación de los empleados

¿Qué servicios de ciberseguridad me puede ofrecer INCIBE para proteger mi despacho?