asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

FELABAN

clab 2016

XVI CONGRESO LATINOAMERICANO
DE AUTOMATIZACIÓN BANCARIA

LIMA-PERÚ 14 - 16 SEPTIEMBRE

Prevención y procedimientos en casos de fraude interno

Foresenics

Módulo 1
El dia anterior

Un mal en aumento….

Los ataques informáticos han crecido en el Perú, que el año pasado ocupó el quinto lugar en Latam en número de incidentes. Un porcentaje importante, el 70% de ataques a bancos se concreta en complicidad con un mal trabajador.

Un ataque informático, un fraude interno o investigar la actividad de un miembro de la organización tiene como clave al documento digital.

Muchos de nuestros asistentes que son especialistas en seguridad de la información o trabajan en el sector de IT de su banco, lo saben. Otros, abogados, agentes comerciales oficiales de atención al público, quizás no tanto.

Les invitamos a todos a recorrer juntos algunos conceptos esenciales.

En el principio: documento digital, naturaleza y caracteres

Es frágil

Es perenne

Se duplica solo

Es complejo

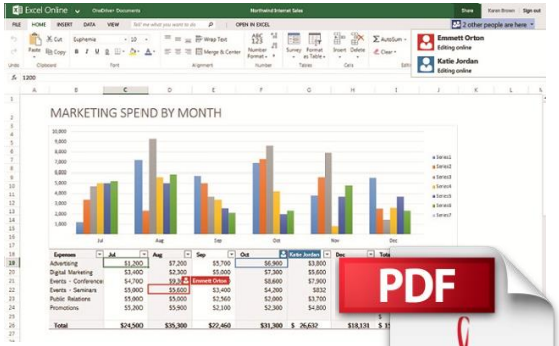
Se altera sin que se vea

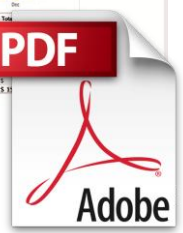
Siempre se sabe si se altera

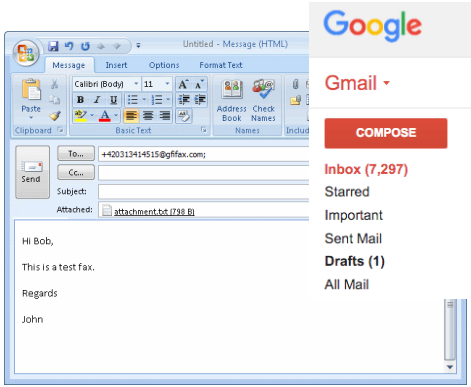
Todas las fuentes de información (y objeto de ataques)

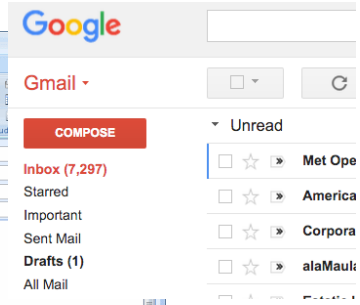
- Teléfonos celulares
- Presentaciones
- Fotocopiadoras
- Cámaras
- Videos- y mucho más
- Emails
- Página web
- Data base
- Hard drive
- Programas
- Servidores!

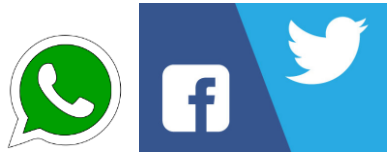
Todo esto es documento electrónico











Desde el principio: Datos Personales, marco legal

Hay dos tipos de bases de datos para la Ley 29.733:

- Base de datos de Titularidad Pública conformadas por datos pertenecientes a organismos públicos (Fuerzas Armadas, de inteligencia o policiales)

- Base de Datos de Utilidad Privada que son recopiladas por personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos de carácter personal.

Definiciones

Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no (puede ser en papel), cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos con domicilio legal, delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley.

Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos

Más definiciones...

Datos personales: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

Titular de los datos: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley.

Datos sensibles: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

Datos personales: cuándo no preocuparse por fraude o pérdida

Las buenas nuevas:

- Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
- Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.
- Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para s.u desarrollo o cumplimiento.
- Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico

Cuando somos responsables. Casi siempre…

1. Sea efectuado en un establecimiento ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento.

2. Sea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento.

3. El titular del banco de datos personales o quien resulte responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional; y

4. El titular del banco de datos personales o quien resulte responsable no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento.

Prevención. Documento de seguridad.

La normativa del país y las buena prácticas han establecido la obligación de contar con Documentos de Seguridad.

La Ley peruana establece que para cumplir con la garantía del tratamiento de datos personales, debe contarse con un código de conducta que establezca las normas internas de protección de datos personales con el contenido previsto por el artículo 31 de la Ley, e inscrito según lo previsto por los artículos 89 a 97 del Reglamento de la Ley ante la Dirección General de Protección de Datos Personales.

Que, a su vez, ha elaborado la Directiva de Seguridad, en la que se proponen unos criterios atendiendo a las características de la información y los tratamientos para clasificarlos en uno de los cinco niveles definidos, con el fin de orientar a las organizaciones en cuáles son las características mínimas de las medidas que deben aplicar en cada caso.

Prevención. Manejo de la información digital

Siguiendo las recomendaciones de las normativas de Seguridad de Datos Personales, podemos recomendar:

- Documento con funciones y obligaciones del personal.
- Clasificación de archivos de acuerdo a la sensibilidad de los mismos.
- Registro de incidentes de seguridad.
- Procedimientos para efectuar las copias de respaldo y su recuperación

Prevención. Manejo de la información digital (cont.)

- Procedimientos de identificación y autenticación de los usuarios.
- Control de acceso de usuarios a datos y recursos.
- Medidas de prevención para impedir amenazas de software malicioso:
  - Instalar, ejecutar y actualizar software de detección y reparación de virus.
  - Verificar, antes de su uso, la inexistencia de virus en archivos recibidos de la web, correo electrónico y otros orígenes inciertos.

Prevención: Política de Usos de herramientas Digitales

Redacte en el Código de Conducta un contenido relativo a la **Política de Usos de herramientas Digitales**.

- En él debe constar la facultad de monitoreo y control de las herramientas digitales provistas o cuyo acceso es provisto por el empleador.
- Debe ser aplicable a todo el personal de manera uniforme.
- Debe estar suficiente y reiteradamente notificado a todo el personal, desde su ingreso mismo.
- Distinga claramente las casillas personales de las cooperativas.
- Regule la navegación por la web en horario de trabajo y desde un ordenador o celular de la empresa.

Prevención. Saber cómo está la empresa en seguridad informática

Test de penetración:

- Ataque simulado realizado de manera controlada.
- Permite identificar vulnerabilidades en sistemas informáticos, equipos tecnológicos y capacitación del personal. (Un ejemplo para no seguir: Mossack-Fonseca)
- Anticiparse a los problemas para solucionarlos antes de que suceda un incidente de seguridad.

Módulo 2. Dia dos: el incidente

Notifique, aunque no quiera...

Si el ataque es externo, o existe una presunción que involucró pérdida de datos personales de sus clientes, notifíquese de inmediato.

Luego viene el control de daños, de la mano del grado de cuidado que Ud. tuvo para evitar lo que ocurrió.

Hágalo, no sume problemas.

Protocolo inicial. Control de daños e identificación de fuentes

1. No altere la evidencia
2. Analice con cuidado su derecho a intervenir
3. Identifique las fuentes
4. Cuide la cadena de custodia, preserve su prueba
5. Análisis de la evidencia: las herramientas, los protocolos
6. Back up y scanner no son las mejores opciones

Sentido común. Le sobra, pongalo en practica.

Guardar para probar no es hacer backup – ni se le parece.

Establezca responsables y responsabilidades de la preservación.

Avise a los custodios para que no deterioren la evidencia.

Póngase en contacto con un especialista y no contamine nada!

Evite reasignar computadoras y celulares.

Ataques a los sistemas propios o a un servidor externo

Sistemas propios y herramientas del cliente: PCs, Celulares, laptops. Responsabilidades ante terceros.

Cuando la información está en un servidor externo y éste es quien fue atacado. Responsabilidades ante terceros- lo vemos con más extensión más adelante.

Investigación del incidente

Se impone preservar la documentación que será investigada.

Para identificarla, habrá que recurrir a las facultades derivadas del documento de seguridad.

Una vez identificada la documentación, hay que preservarla íntegramente. **Solo una porción será útil**

Lo que sirve: correos electrónicos

Investigacion de incidente: hay límites.

- Límites legales: privacidad, uso de correos corporativos y personales
- Límites legales: propiedad de las herramientas. Facultad de controlar los elementos de trabajo
- Límites jurisprudenciales: privacidad, otra vez. Facultad previa del empleador, publicidad de esa facultad.
- Redes sociales: una cuestión especial…

Un dictamen. Enunciado.

En Septiembre de 2014, , la Comisión de Trabajo y Seguridad Social aprobó un polémico dictamen que regula el uso de medios informáticos en los centros de trabajo públicos y privados y que ha generado la reacción de algunos sectores.

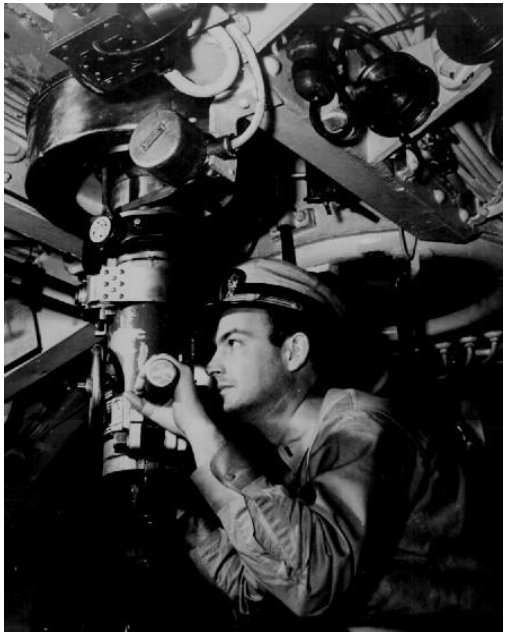
El artículo 3 de este documento especifica: “Los medios informáticos en el centro de trabajo son de titularidad del empleador, independientemente de su asignación al trabajador, y su uso no genera una expectativa razonable de privacidad o secreto”

El dictamen. Reacciones inmediatas.

Antes que nada: derecho a la privacidad o a la expectativa de privacidad?

- Celulares: dónde estoy y a qué hora estoy.
- Redes sociales: dónde almuerzo, con quien y el menú…
- Privacidad en Facebook: alguien la entiende?
- GPS: por dónde voy. Cada día de mi vida.
- Usinas de búsqueda: que compro y que deseo comprar.
- Correo electrónico y correo tradicional. No es lo mismo.
- Supervisión estatal.
- Reconocimiento facial: hoy te vi.

Control y monitoreo: principio general



Cuando el empleado usa el correo de la empresa, en horario de trabajo, para realizar un acto desleal, y fue avisado previamente de la facultad del empleador de monitorear la cuentas corporativa, su derecho a la privacidad parece retroceder.

Cuando un empleado entra en una red social y postea contenidos relacionados con su trabajo, compartir es un verbo que no se lleva bien con privacidad

Control y monitoreo: tres preguntas y una respuesta.

Puedo controlar la navegación de mis empleados?
No siempre, habrá que consultar la Política de Uso de herramientas digitales de de la empresa. Habrá que contar con su consentimiento - constante.

Puedo controlar el correo electrónico de mis empleados?
No siempre, es el caso de la pregunta anterior…

Puedo controlar el celular de mis empleados?
Seguimos en la misma

Fuente del incidente: Un clásico, Phishing.

Phishing = *ir a la pesca*.

Robo de datos con ingeniería social.

- Mantener alertas a los empleados y clientes.
- Realizar simulacros controlados.
- Prevenir y prepararse para control de daños

Bajo fuego: Phishing. Ejemplos reales

Attention Beneficiary,
Based on our investigation of your payment, we want to find out if you're still alive or did you sign any deed of assignment with (Mrs. Grace Jackson.) to receive your fund, reply to us:
Your Full Names.....
Your Home/Office Address.....
Your Tel Phone And cell phone.....
Your Occupation.....
Your Age/Sex.....
The nearest Airport To Your Country.....
A Copy Of Your Identity.....
This is because $5.6 Million has been approved in your favor for payment so get the above information to us fast and unfailingly today or your fund will be released to Mrs. Grace Jackson.

Best Regards,
Mr. Ebere Williams
Chairman, Investigation and Debt Settlement Committee.

Bajo fuego: Phishing. Ejemplos reales

BBVA net Office
Todas las cuentas deben ser actualizados antes del 14-04-2016 con el nuevo sistema de seguridad por teléfono.
Su cuenta no se ha actualizado y nos vimos obligados a suspender temporalmente el acceso en línea.
Para actualizar tu cuenta y tener una mayor seguridad bancaria, por favor haga clic en el siguiente enlace:

www.bbvanet.banca25.com

Bajo fuego: Phishing. Ejemplos reales

Estimado Cliente de Apple,,

Tu ID de Apple se ha desactivado temporalmente por razones de seguridad!!!

Alguien acaba de intentar iniciar sesión en tu cuenta de Apple de otra dirección IP. Por favor, confirme su identidad actual o su cuenta se desactivará debido a la preocupación que tenemos por la seguridad e integridad de la comunidad de Apple.

Para confirmar su identidad, le recomendamos que vaya a Comprobar ahora >

Saludos,
Apple

Bajo fuego: Phishing. Estar alerta

Mensajes de:

- Bancos y tarjetas de crédito
- Medios de pago: PayPal, ...
- Redes Sociales
- Páginas de Ventas: MercadoLibre, eBay, Amazon
- Servicios: Outlook, Apple, Gmail

Investigación: Preguntas antes de empezar

- Cuáles documentos quiero usar y que quiero probar con ellos?
- Dónde están?
- En qué plazos puedo acceder?
- Quién, cuándo y cómo puede acceder?
- Y lo más importante, otra vez: tengo el derecho de acceder a la información?

El tiempo de las entrevistas. Después...

No se anticipe ni se apresure. Primero atienda la prueba digital. Identifiquela y sobre todo preservela.

Ya habrá tiempo para las entrevistas.

Al final del dìa, nadie suele inculparse en ellas. Salvo en Hollywood...

Ya identifique- queda preservar. Preservación de evidencias digitales internas.

La certificación de la prueba digital, por medio de un acta notarial, es un acto necesario para darle validez al documento electrónico y certeza al modo en el que se lo identificó.

Sin embargo, le fe pública debe estar acompañada por la certeza técnica.

Tecnología y formalismo coinciden en un mismo procedimiento.

El acta tendrá eficiencia a la hora de probar, si la integridad del documento fue resguardada

Participación del notario o escribano

- Un concepto nuevo que se hace familiar: la cadena de custodia.
- El notario y su rol.
- Un acta autosuficiente.
- Cómo y cuándo presentar el acta.
- Diferencias: lo que debemos preservar está al alcance- o no lo está.

Resguardo de prueba digital: buenas prácticas

- Registre fecha y hora de toma y uso de la información
- Inspeccione el medio de almacenaje y saque fotos
- Registre herramientas informáticas utilizadas. Use bloqueadores de escritura para acceder a información de discos y pendrives
- Calcule el “hash value” para cada elemento
- Proteja la prueba: haga varias copias y guárdelas por separado
- Determine cada persona que física o electrónicamente acceda a la data
- Trabaje sobre copias forenses

Data y metadata: en correo electrónico

Email Informativo-Microsoft

EM

Eventos microsoft
miércoles, 23 de septiembre de 2015, 1:51 p.m.
To: Gabriel Paradelo

Gracias por tomar mi llamada. El motivo del correo es para confirmarle que gracias a la retroalimentación que recibimos a través de las encuestas de satisfacción, hemos implementado varias de sus sugerencias en servicios y beneficios de Microsoft Partner Network, por lo que le estamos llamando para actualizarlo y asegurarnos que los conoce porque USTED nos lo sugirió.

Usted cuenta con:

Recursos de ventas y marketing que puede usar descargando los logos, campañas, flyers, promociones e incentivos que tenemos para usted de Windows 10, Azure, Office 365, CRM Online, entre muchos otros. Ingrese a https://readytogo.microsoft.com/es-la/paginas/campaignfinder.aspx para descargarlos.

➢ Centro de soporte, servicios en la nube y horas de asesoría con los ingenieros y soporte técnico de Microsoft que le ayudarán a resolver todas sus dudas.

➢ Encuentre aquí los números telefónicos de soporte:

- **Presione las siguientes opciones**: #3 para Socios de Microsoft Partner Network, luego: #1 Programas de Socios, #2 Preguntas de Nube, #3 Soporte Técnico, #4 Licenciamiento.

➢ Entrenamientos, capacitaciones y recursos comerciales y técnicos que puede tomar en línea que le ayudarán a diferenciarse de la competencia y ofrecer el mejor servicio a sus clientes. Ingrese aquí para tomar los cursos y capacitaciones.

Todo esto y más está 100% incluido en su membrecía como socio de Microsoft.

Lo invito a suscribirse a nuestro boletín semanal, ingresando a la siguiente liga www.aka.ms/latamnl y dar clic en suscribir para acceder a todos los anuncios y novedades de MPN para poder crecer su negocio.

Gracias por su tiempo y Gracias por ser un socio de Microsoft. No olvide que su satisfacción, con el apoyo e información que le brindemos es nuestra prioridad.

```
Delivered-To: gparadelo@expertizen.com.ar
Received: by 10.58.252.234 with SMTP id zv10csp469754vec;
        Wed, 15 Aug 2012 07:19:43 -0700 (PDT)
Received: by 10.224.28.7 with SMTP id k7mr41148546qac.56.1345040383229;
        Wed, 15 Aug 2012 07:19:43 -0700 (PDT)
Return-Path: <delivery@mx.sailthru.com>
Received: from mx-64-34-47-136.sailthru.com (mx-64-34-47-136.sailthru.com. [64
        by mx.google.com with ESMTP id eplsi2157575qab.8.2012.08.15.07.19.43;
        Wed, 15 Aug 2012 07:19:43 -0700 (PDT)
Received-SPF: pass (google.com: domain of delivery@mx.sailthru.com designates
Authentication-Results: mx.google.com; spf=pass (google.com: domain of deliver
smtp.mail=delivery@mx.sailthru.com; dkim=pass header.i=@businessinsider.com
Received: from nypl-jmailer1.sailthru.com (nypl-jmailer1.sailthru.com [64.34.5
        by mx-64-34-47-136.sailthru.com (Postfix) with ESMTP id F2AF2E540A
        for <gparadelo@expertizen.com.ar>; Wed, 15 Aug 2012 10:19:42 -0400 (ED
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; t=1345040383;
        s=sailthru; d=businessinsider.com;
        h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type:List-ID:Li
        bh=xhWglCvWsTQuYuNAfRnbItQvO8JNRgLBwE+0HwsZ5EM=;
        b=PyHFcrGZFAcyluHHE5UGTC6AV/1Q0JLF8gWyQFmkYb16XDmMc74RMnkYau0FcA4N
        o8+aaOnJFV43+pIdnEDwbk8vPiQlzjvaEnRzV3udzWKmHTL/8kiY1QXN1/1VY7qLUf4
        VsAeJ4nUUqdmAuEXm80rXDOZr26X0QEFaLupVmlE=
Date: Wed, 15 Aug 2012 14:19:42 +0000 (UTC)
From: Business Insider <newsletter@businessinsider.com>
To: gparadelo@expertizen.com.ar
Message-ID: <20120815141942.502bafe2dd6a49ad79000118@sailthru.com>
Subject: Instant Alert: Pinterest Goes Nuts With Mobile App Releases
```

Data y metadata: en Twitter

Reenvíos, Fecha y hora, aplicaciones involucradas

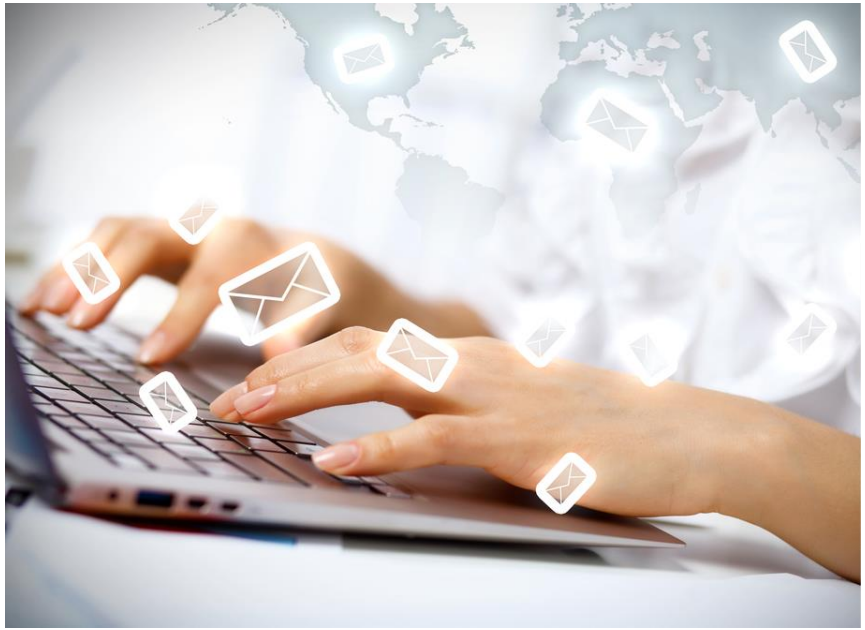
Data y metadata: en Twitter (cont.)

Ubicación

Data y metadata: en Twitter (cont.)

- Ubicación
- Vínculo con otros servicios y usuarios
- Referencias

Correos electrónicos: una fuente muy popular



- Aún son la prueba digital estrella
- Contexto, threading, contexto
- Son complejos, tienen mucha más información de la que imprimimos.
- Servidores y Outlook: parecido pero no igual

Cuándo es prueba el correo electrónico?

- Si yo lo envié, es más difícil utilizarlo como prueba. Sirve de poco:
  - Impresión
  - Correo en copia
  - Mensaje guardado
  - Falta de aviso de rebote
  - Desconocimiento de archivos adjuntos
- Si yo lo recibí, es más valioso como prueba, porque la metadata me respalda

La Web: resguardo de prueba digital

Tanto para el contenido de sitios Web comerciales, blogs, sitios de noticias o redes sociales:

- Descargar data y metadata
- Capturas de pantalla
- Siempre respaldado por un acta notarial

Módulo 3.
El día siguiente y en las nubes

Control de daños. Dentro y fuera de casa

Hasta aquí, hemos considerado una hipótesis en la que el fraude o el ataque involucró solo documentos digitales que se encuentran en las fuentes que son propiedad de la empresa y están en su cercanía física.

La situación cambia si los documentos involucrados están en servidores externos.

Aun con importantes limitaciones, es el caso de muchas instituciones financieras del país.

A partir de ahora, consideremos esa segunda hipótesis.

Control de daños. Dentro y fuera de casa

Todos suben a la nube. A todo esto, que es la nube?: es el alquiler de un disco rígido al que se puede acceder desde Internet. Con perdón de los expertos en tecnología presentes…

Es una novedad que tiene sus riesgos- cuál no?

Dejemos las (muchas) ventajas para los vendedores de servicios en la nube, concentrémonos en las vulnerabilidades:

- Seguridad
- Privacidad

Pero piense lo que piense al terminar, por favor conserve en mente que el negocio no es inherentemente vulnerable y que el 42% de los accidentes de seguridad ocurren fuera de la nube. De hecho, las estadísticas indican que un centro de datos ubicado en una empresa, y no en la nube, es cuatro veces más susceptible de sufrir un ciberataque que un servicio hosteado en la nube.

Antes de correr la hoja: Yo no estoy en la nube, verdad?

En la nube. Yo no!

Todos suben a la nube. A todo esto, que es la nube?: es el alquiler de un disco rígido al que se puede acceder desde Internet. Con perdón de los expertos en tecnología presentes…

Es una novedad que tiene sus riesgos- cuál no?

Dejemos las (muchas) ventajas para los vendedores de servicios en la nube, concentrémonos en las vulnerabilidades:

- Seguridad
- Privacidad

Pero piense lo que piense al terminar, por favor conserve en mente que el negocio no es inherentemente vulnerable y que el 42% de los accidentes de seguridad ocurren fuera de la nube. De hecho, las estadísticas indican que un centro de datos ubicado en una empresa, y no en la nube, es cuatro veces más susceptible de sufrir un ciberataque que un servicio hosteado en la nube.

Antes de correr la hoja: Yo no estoy en la nube, verdad?

Bueno, sí, estoy. Responsabilidades legales.

- Las empresas que tercerizan sus prácticas fundamentales es muy probable que terminen siendo responsables hacia terceros en virtud de las acciones del proveedor del servicio de la nube.
- En caso de que un proveedor de servicios de la nube viole los derechos de un tercero (ej: utilizando incorrectamente información personal), eso generará responsabilidad en los directores de la compañía.
- Asimismo, eso dañará el valor y el buen nombre de la compañía.

Sé lo que hago. Bueno creo que lo sé

Cómo es el esquema legal de responsabilidades? Bueno, por cierto no es el mejor- otra vez, alguien conoce uno mejor? es así:

El responsable o usuario de la base de datos debe garantizar la seguridad y confidencialidad de los datos. El artículo 10 prohíbe registrar datos en bases de datos que no reúnan las condiciones técnicas de integridad y seguridad. (Principio de seguridad de los datos, Ley 18.331)

Naufragio: Directores y Gerentes a los botes

Violación de las leyes, dolo, abuso de poder y culpa grave

Probablemente, la responsabilidad personal más grave que una falla puede acarrear sea la que involucr a los Directores y gerentes de una institución financiera.

En los países sudamericanos, salvo el caso de Colombia, hay una tendencia a atribuir responsabilidad solidaria a los representantes de las sociedades.

No todos, no siempre

- Pero,en principio, dado el carácter colegiado del directorio de las S.A., la Ley le ha impuesto a todos sus integrantes una responsabilidad solidaria e ilimitada, hacia la sociedad, accionistas y terceros por mal desempeño de su cargo.
- Esta conducta no sólo queda configurada por la participación activa de cada director en los hechos generadores de responsabilidad, sino también por una conducta omisiva o negligente, sin la cual el daño podría haber sido evitado.

Una buena práctica

- Directores y ejecutivos deben velar por el cumplimiento de los objetivos tenidos en miras a la hora de decidir la tercerización, al seleccionar al proveedor, así como proveer a la contratación en los términos más adecuados y razonables para la Sociedad.
- **La tercerización importa siempre la delegación de actividades pero no de responsabilidades**.

Negociando el contrato, es decir mitigar el daño...

- Los servicios en la nube no son necesariamente invasivos de la privacidad.
- Pero implican transferencia de información fuera del control de quien contrata el servicio. El procesamiento y almacenaje de esa información puede estar fuera del Uruguay.
- Deje de lado conceptos como jurisdicción, competencia y aplicación de leyes nacionales, en serio.

Negociando el contrato

- La responsabilidad de no violar los derechos de autor es (también) de su empresa.
- Ante un incidente de seguridad, el proveedor no se responsabiliza.
- Los términos y condiciones del servicio están sujetos a modificaciones unilaterales por parte del proveedor.
- Los servidores donde el proveedor aloja la información, de la que su empresa es responsable, pueden estar fuera del país y ser allí legalmente accesibles a Gobiernos y Fuerzas de Seguridad de otros países. Genial !

Resumen ejecutivo.

Mañana a la mañana:

- Diseñe un documento de seguridad, si no lo tiene.
- Chequee su documento de seguridad, si lo tiene.
- Tiene política de uso de herramientas digitales? Si la tiene, notifiquela, caso contrario, créela.
- Contratos de servicios en la nube: que tengan lo que tienen que tener.

Hoy: test de seguridad

Preguntas? Solo contestaremos las que sepamos. Broma!!

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

clab 2016

FELABAN

Gracias!

Dr. Martin F. Elizalde,
melizalde@foresenics.com.ar

Lic. Gabriel Paradelo,
gparadelo@foresenics.com.ar