FI$CALIZADOS
Entre los negocios y los impuestos

"Detrás de una gran empresa existe una política de cumplimiento"

CONCANACO SERVYTUR MÉXICO

Seguridad Digital para PYMEs

Mtro. Daniel Medina Cabello
Head of Legal & Compliance

Marzo 2022

FI$CALIZADOS

Entre los negocios y los impuestos

www.concanaco.com.mx

"Detrás de una gran empresa existe una política de cumplimiento"

CONCANACO SERVYTUR MEXICO

Mtro. Daniel Medina Cabello

Abogado, miembro honorario de la Asociación Internacional de Cumplimiento (ICA), profesional certificado en GRC por la Universidad de Manchester (Reino Unido). Con más de 10 años de experiencia en prevención de delitos financieros, cumplimiento normativo y legal, en México, LATAM, Estados Unidos, Reino Unido, Asia y la Unión Europea.

Actualmente es Director Jurídico y de Cumplimiento para Swile en México.

Eso es solo para las grandes corporaciones, ¿no?

Cuando se habla de un programa de un programa de ciberseguridad quizás se piense inmediatamente en **grandes empresas y corporaciones con un gran presupuesto**. No hay nada más lejos de la realidad.

Cualquier empresa, por pequeña que sea y me atrevo a decir, incluso aquellos profesionales independientes, necesitan urgentemente diseñar una estrategia de seguridad digital **por el simple hecho de estar conectados a internet y ser parte de la híper-digitalización**.

¿Qué información fluye?

Registros contables, nombres de clientes, quizás la receta secreta de nuestro producto estrella, información personal, proveedores, y muchas cosas más viven digitalizadas en nuestros dispositivos móviles, tabletas y ordenadores. **Diariamente a través de nuestro módem de internet se intercambian cantidades inimaginables de datos** que contienen también nuestro historial de búsquedas, conversaciones, sitios visitados y en general, toda la información que es intercambiada con nuestro proveedor de internet.

Todos estamos conectados

Este pequeño vistazo a nuestra realidad digital pone de manifiesto que **todos, sin importar el tamaño de nuestra actividad económica**, tenemos una responsabilidad legal y ética para asegurarnos que la información, el bien más preciado del siglo XXI, sea debidamente almacenada, resguardada y protegida.

¿Por dónde empiezo?

Está claro que no todas las actividades económicas son iguales en oferta, dimensión, alcance, cobertura geográfica. **Cada negocio es único y por ende, el análisis que conlleva a diseñar un programa de Ciberseguridad deberá estar hecho a la medida**, atendiendo las particularidades de cada sujeto.

Paso 1: Conoce y entiende tu negocio

- ¿Qué **información** vive aún en papel y cuál se encuentra ya **digitalizada**?
- ¿**De qué tipo de información se trata**, es financiera, legal, propiedad intelectual?
- ¿**Toda la información es mía**, o también tengo información de terceros, por ejemplo empleados, clientes, proveedores, etc.?

Paso 2: Entiende tu situación actual

- **¿En dónde está almacenada esta información?** ¿Está en mi celular? ¿Está en aplicaciones de terceros como Whatsapp, Facebook? ¿Se encuentra en mi computadora? ¿Se hacen respaldos de esta información, por ejemplo, al usar un proveedor de almacenamiento en la nube (G Drive, Exchange, Dropbox, etc.)?
- **¿Está debidamente protegida la información?** ¿Tiene contraseñas únicas y mecanismos de autenticación seguros, como el Factor de Doble Autenticación (2FA, por sus siglas en inglés)?

- **¿Cuál es el Plan de Continuidad del Negocio en caso de que pierda acceso a la información?** ¿Qué sucede si pierdo mi contraseña o bien, hay un acceso mal intencionado? ¿Hay un correo electrónico adicional o un número de teléfono de respaldo en caso de que no pueda acceder a mi cuenta? ¿Hay contactos de confianza establecidos?
- **¿Soy consciente de las amenazas actuales en materia de seguridad de la información?** ¿Conozco las últimas tendencias o por lo menos, las formas de operar tradicionales de los delincuentes informáticos? ¿Podría decir que yo y mi negocio tenemos los conocimientos mínimos necesarios para hacer frente a un robo de identidad, fraude o vulneraciones mal intencionadas a nuestra información?

Paso 3: Conoce tu marco legal

Muchos de nosotros operamos negocios y emprendimientos sin estar conscientes que dicha actividad económica **conlleva una responsabilidad legal.**

En México, los datos personales se encuentran protegidos por la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y su cumplimiento se encuentra supervisado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

En México,en el Código Penal Federal (CPF) se han tipificado conductas que constituyen delitos informáticos. Algunos de los delitos tipificados en México, en los cuales se emplean los sistemas informáticos, electrónicos, Internet, computadoras, programas informáticos como medio o como fin se encuentran: la revelación de secretos, el acceso ilícito a sistemas y equipos informáticos, el acoso sexual, el engaño telefónico, la extorsión telefónica, falsificación de títulos, pornografía, suplantación de identidad, entre otros. Otros delitos en cuya comisión se emplean las Tecnologías de la Información y la Comunicación son el delito de fraude, el robo, el delito equiparado al fraude, entre otros.

Es importante mirar al CPF en dos vías, por un lado la responsabilidad penal de la persona jurídica (Art. 11bis del CPF, fraude) y por el otro como estar conscientes de que dichos delitos pueden convertir al negocio en el sujeto pasivo, es decir, la **víctima**, causándole daños y perjuicios que podrían conducirle a la extinción.

Nuestro marco legal, en resumen, nos exige **contar con las medidas necesarias para salvaguardar y proteger los datos personales** (LFPDPPP), la información que pueda constituir **propiedad industrial** (Ley Federal de Protección a la Propiedad Industrial), así como evitar ser el canal o medio para la **comisión de un delito** (responsabilidad penal de la persona jurídica).

Paso 4: Identifica tus riesgos

Una vez conoces y entiendes tu negocio (Paso 1), conoces tu situación actual (Paso 2) y la responsabilidad legal que tienes (Paso 3), **el siguiente paso es identificar tus riesgos.**

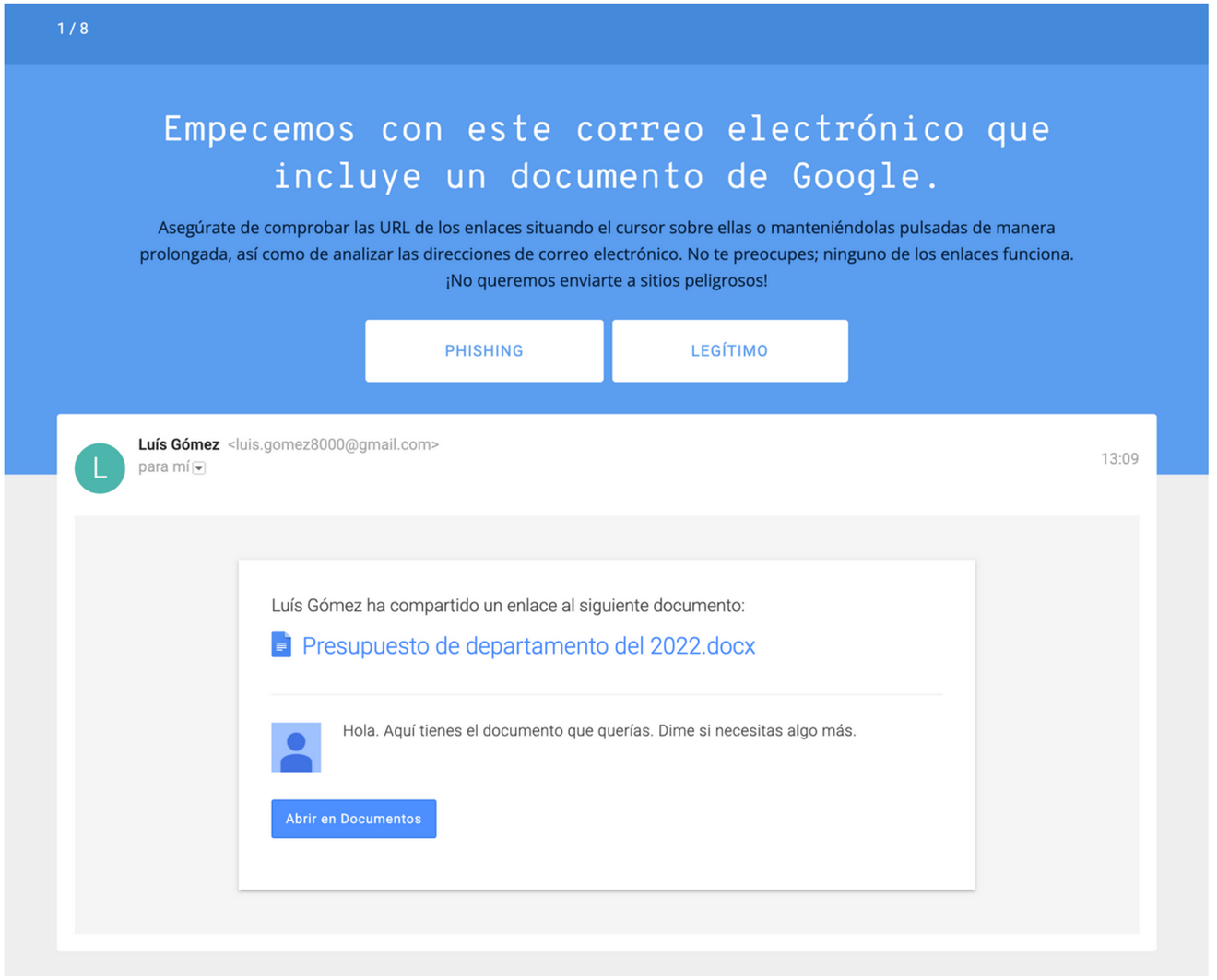
Resulta fundamental destacar que el desconocimiento de un riesgo no implica su inexistencia, sino que por el contrario, significa la aceptación total y ciega del mismo, así como de sus consecuencias. Esto quiere decir que el ejercicio de identificar los riesgos debe ser minucioso, detallado, transparente y a su vez, documentado (en caso de que sea necesario presentar evidencia ante algún tercero, incluyendo el INAI o el Ministerio Público).

Para identificar los riesgos en materia de seguridad de la información es importante hacernos las siguientes preguntas:

- ¿Qué **plataformas** utilizo para resguardar la información y cómo se protege el acceso a las mismas?
- ¿En qué **dispositivos** se almacena, le pertenecen dichos dispositivos al negocio, al empleado o al dueño?
- ¿Qué tan **segura** es la plataforma y el dispositivo para evitar ataques maliciosos? ¿Han habido **noticias** sobre infiltraciones no autorizadas en esa plataforma, o bien, robo de datos personales?
- ¿Tengo **sitio de internet**, se resguarda allí información? ¿Se hen hecho pruebas de penetración para ver si son resilientes a ataques informáticos?

- ¿Tengo un **inventario** en dónde se incluya el tipo de información que posee mi negocio, el hardware en donde está resguardada, así como el software?
- ¿Hay un inventario de **permisos**, indicando qué persona y en función de qué requisitos, puede tener acceso a determinada información?
- ¿Cuento con un **registro de accesos a la información de la empresa**, verificar día y hora, información consultada, acciones realizadas (imprimir, descargar, copiar, modificar, alterar, destruir, etc.)?
- ¿**Ha habido cursos, capacitaciones o de índole similar**, al interior de mi negocio, con el fin de estar al día con las últimas amenazas a la seguridad de la información? Por ejemplo, valdría la pena preguntarse, ¿saben mis empleados como identificar un correo de suplantación de identidad? ¿Saben qué hacer o a quien reportar estos casos?

Se pueden utilizar **herramientas en línea gratuitas** como: https://phishingquiz.withgoogle.com/ para medir el riesgo de vulnerabilidad ante ataques de phishing.


1 / 8
Empecemos con este correo electrónico que incluye un documento de Google.
Asegúrate de comprobar las URL de los enlaces situando el cursor sobre ellas o manteniéndolas pulsadas de manera prolongada, así como de analizar las direcciones de correo electrónico. No te preocupes; ninguno de los enlaces funciona. ¡No queremos enviarte a sitios peligrosos!
PHISHING
LEGÍTIMO
Luís Gómez <luis.gomez8000@gmail.com>
para mí
13:09
Luís Gómez ha compartido un enlace al siguiente documento:
Presupuesto de departamento del 2022.docx
Hola. Aquí tienes el documento que querías. Dime si necesitas algo más.
Abrir en Documentos

Paso 5: Plan de acción

Una vez identificados los riesgos, el siguiente paso es diseñar un plan de acción y una estrategia para mitigar los mismos. Dependiendo de la organización y su tamaño, se pueden llevar a cabo metodologías especializadas en materia de evaluación de riesgos, sin embargo, lo más importante para el caso de las pequeñas y medianas empresas (PyMEs) es **dar especial atención y prioridad a los riesgos que puedan poner en riesgo la existencia del negocio**, es decir, aquellos que puedan conducir al cierre de operaciones, como son: multas elevadas por parte de la autoridad (INAI), a investigaciones penales, a robo de propiedad industrail crítica para el funcionamiento del negocio, robo de base de datos como clientes (LFPDPPP), etc. **Estos riesgos críticos son los que deberán de ocupar la atención inmediata de toda la organización para diseñar un plan de remediación a la medida.**

Algunos ejemplos de mitigantes en esta etapa son:

- **Abandonar el uso de dispositivos personales y cambiar a aquellos proporcionados o aprobados por la compañía** (ejemplo de "aprobados" sería hacer una política de Trae Tu Propio Dispositivo [BYOD, por sus siglas en inglés] que no representa un impacto económico para el negocio, pero que fija las normas y los estándares de seguridad que deberán seguir los empleados al usar sus dispositivos personales para asuntos del trabajo, responsabilidad legal, así como cláusulas en caso de que la relación laboral concluya).

- **Cambiar a plataformas y/o dispositivos más seguros**, así como monitorear constantemente a través de aplicaciones gratuitas como Google Alerts en caso de que se presenten eventos críticos que pongan en riesgo la información.
- **Educar y proporcionar herramientas** a todo el negocio para que puedan proteger a la organización. Algunas herramientas pueden ser antivirus, herramientas de gestión de contraseñas (por ejemplo 1-Password), entre otras.

- **Si la operación de tu negocio lo permite, es importante que cuentes con un área especializada en Tecnologías de la Información** o por lo menos, tengas a un Consultor independiente que, con base a tus necesidades, pueda ayudarte a resolver cualquier contingencia y cobrar sólo por eso, sin necesidad de tener una carga patronal fija. Asesórate y rodeáte de un experto en el que puedas confiar.

Paso 6: La ciberseguridad es un proceso sin fin

No por haber realizado los pasos anteriores significa que tu organización ya está por siempre segura de cualquier amenaza cibernética. **Tu organización deberá de llevar a cabo este ejercicio por lo menos 1 vez al año** y cada vez que sea necesario debido al uso de nuevas herramientas, plataformas o el surgimiento de eventos críticos en materia de seguridad de la información.

La seguridad de la información es un proceso sin fin, en constante mejora y en un ciclo de iteración infinito.

Conclusión

La seguridad de la información es responsabilidad de todos, no solamente como una responsabilidad legal al emprender un negocio, sino también una responsabilidad moral y solidaria ante la sociedad, puesto que la vulneración de datos personales puede afectar a múltiples familias y personas quienes verán afectados su patrimonio e integridad.

A su vez, estoy convencido de que habrá personas y familias que dependen de que nuestro negocio marche de forma adecuada, por lo que una estrategia de seguridad digital nos protege a nosotros, a nuestras familias y en general, a la sociedad.

FI$CALIZADOS

Entre los negocios y los impuestos

CONCANACO SERVYTUR MEXICO

"Detrás de una gran empresa existe una política de cumplimiento"

Vía redes sociales de
CONCANACO SERVYTUR

www.concanaco.com.mx

CONCANACO
SERVYTUR
MEXICO

www.concanaco.com.mx