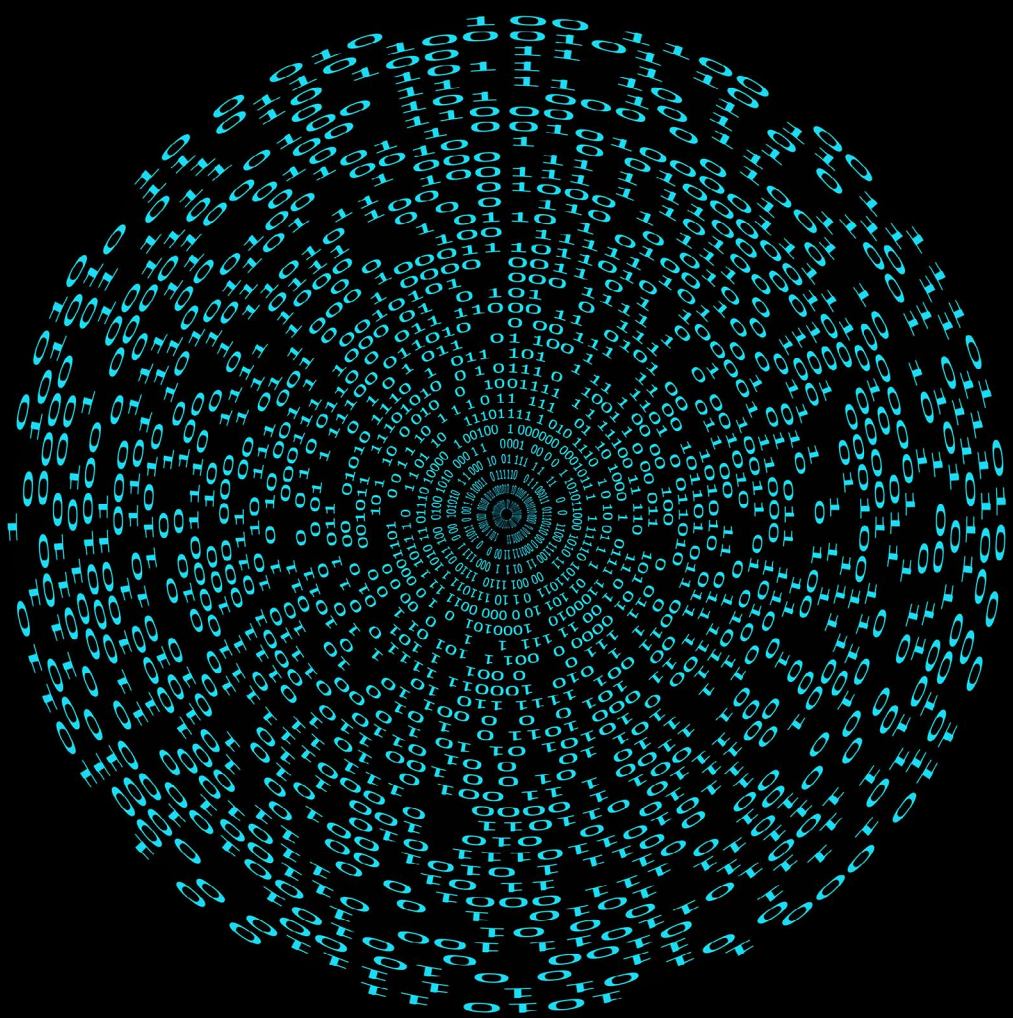
Deloitte.

makros
Cyber Security Expert



Guía de Ciberseguridad para Pymes

Octubre 2020

Introducción

La ciberseguridad es una realidad para las personas y las organizaciones del mundo contemporáneo. Es un concepto que si bien parece complejo, a veces es más simple y necesario de entender. En un escenario digital la seguridad virtual es tan importante como la seguridad real en nuestras comunas o barrios.

La definición del termino **ciberseguridad** "Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".

Esta guía fue preparada en conjunto por el área de Ciberseguridad de Deloitte Chile y Makros, empresa especialista en soluciones de ciberseguridad, y pretende acercar conceptos relevantes para que todas las organizaciones, en un contexto laboral, puedan proteger su capital creativo, económico y financiero.

Nicolás Corrado
Socio Líder de Cyber
en Deloitte

Marcelo Diaz
CEO de Makros

Existen 5 principios fundamentales para toda empresa **-independiente de su tamaño-** que debieran seguirse:

1.- Identificar
No se puede cuidar lo que no sabemos que tenemos. Entonces, el primer paso es identificar. ¿Cuántos computadores tiene mi organización? ¿Cuántos son propios? ¿Cuántos son del colaborador (Byod)? ¿Tenemos cámaras de seguridad? ¿Existen sensores de aperturas de puertas? ¿Accesos controlados por huella y todo aquel dispositivo que sea posible conectar a internet (IoT)? ¿Nuestra información (facturas, OC, guías, patentes, inventos, sistemas, etc.) dónde esta almacenada? ¿En la nube o en algún computador o servidor dentro de mi empresa? Después de hacer este primer ejercicio de identificación podemos pasar el paso siguiente.

2.- Proteger
Identificamos todo lo que debemos proteger, ¿entonces qué hacemos ahora? Cada sistema cuenta con alguna medida de protección (también tendremos que evaluar los riesgos), y aun cuando estos sistemas parezcan no tener una protección, existen estrategias que se pueden abordar para poder dar protección a lo que identificamos anteriormente. Antimalware (solía ser antivirus, pero ahora es mucho mas complejo), Parches o actualizaciones (ese mensaje que hace que nuestro computador nos diga qué debemos reiniciar, por qué hay que actualizar el sistema operativo), Firewall (ok, la palabra ya es más compleja, pero es lo que nos entrega el proveedor de Internet de una forma básica o más avanzada y evita que entren a nuestra red).

3.- Detectar
Hemos establecido algunas medidas de protección de nuestros activos, que a veces nos parecen ser más molestosas que productivas (aquí vendrá después una decisión de invertir en protección o contar con servicios profesionales), estas medidas comenzaran a entregar alertas, porque el malware y los ciberdelincuentes no descansan, y esperemos que aquellas soluciones que protegen nuestros sistemas detecten los ataques, y por supuesto nos alerten. Sin embargo, es importante poder interpretar estas alertas ya que en muchas ocasiones son indicios de que podemos estar frente a algún tipo de evento de ciberseguridad que podría amenazar nuestro patrimonio digital. Aquí debemos pasar al siguiente paso.

4.- Responder
¿Cómo reaccionar? Tendremos a mano el contacto de alguien que nos ayude, o contaremos con servicios profesionales que nos puedan asesorar en situaciones como estas. Hay que sentirse seguros pero es necesario además preguntarse regularmente cómo enfrentar este tipo de crisis. Podría haber situaciones límites donde, por ejemplo, un virus informático podría dejarte sin acceso a todos los archivos de tu organización.

5.- Recuperar
Si nada funcionó o lo hice cuando ya era tarde o el atacante fue más astuto, solo queda recuperar. Frente a un evento de ciberseguridad las preguntas claves son: ¿Respaldamos nuestra información? ¿podemos reconstruir nuestros datos con almacenado? ¿Estamos preparados para recuperar? Es necesario terminado este proceso de sacar lecciones y aprendizajes para el futuro.

Este ciclo de 5 pasos debiera ser una hábito que permita aprender y mejorar en ciberseguridad.

Tu casa también es tu oficina, ¡Protégela!

La tecnología nos permite continuar con nuestras «tareas de oficina» cuando llegamos a casa. Abrir el correo electrónico de la empresa, realizar un pedido a uno de nuestros proveedores o actualizar la lista de clientes son solo algunas de las tareas corporativas que podemos realizar cómodamente desde nuestro hogar. Hasta aquí, todo parece una ventaja, pero, ¿y si hablamos de la seguridad? ¿Tomamos en casa las mismas precauciones que en la oficina? ¿Realmente conocemos todas las medidas de seguridad que necesitamos?

Tome nota siga y estos consejos

¿Cómo teletrabajar de manera segura?

- No entregues tus datos al primero que te los pida. El principio de la duda es el que debiera prevalecer, a veces somos muy confiados.
- Protege tu equipo y tus dispositivos móviles con credenciales de acceso y diferencia tus cuentas personales de las profesionales. Recuerda utilizar siempre contraseñas robustas y utiliza el doble factor de autenticación siempre que sea posible.

- Mantén los sistemas operativos y las aplicaciones actualizados, tanto los que usas profesionalmente como a nivel usuario. Instala software de repositorios oficiales y nunca olvides disponer de un antivirus.
- Encripta todo dispositivo donde almacenes información para proteger los datos de tu empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.
- Realiza copias de seguridad periódicas de todos tus equipos o al menos aquellos que sean criticos para la operación del negocio (Gerentes, Servidores con Datos de Facturacion, entre otros) para garantizar la continuidad del negocio en caso de que ocurra cualquier incidente de seguridad o cualquier otro posible desastre (robo o pérdida del dispositivo, avería, etc.).
- Comprueba regularmente que estas copias pueden restaurarse. Es recomendable al menos una vez al año probar que lo que respaldamos lo podemos recuperar.

Si necesitas acceder a la información almacenada en los equipos de la empresa, evita el uso de aplicaciones de escritorio remoto. Estas herramientas pueden crear puertas traseras (backdoors) a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y, por lo tanto, permitir el acceso a los equipos corporativos por parte de alguien no autorizado.

Además, al utilizar este tipo de aplicaciones aceptamos ciertos términos y condiciones de uso que podrían otorgar algún tipo de privilegio a las mismas sobre nuestros equipos e información.

En lugar de las aplicaciones de escritorio remoto, **conéctate a tu empresa de forma segura a través de una red privada virtual o VPN** (sigla en inglés: Virtual Private Network). De este modo, la información que intercambiamos entre nuestros equipos viaja cifrada a través de Internet.

Documéntate sobre las diferentes opciones para elegir una VPN segura y que mejor se adapte a tu organización.

Si en casa disponemos de conexión Wifi, debemos asegurarnos de que la configuración sea correcta y segura, en la medida de lo posible intenta separar la conexión, de manera de dar acceso a TV u otros aparatos de una forma y a tus equipos o los de tu empresa en una red distinta. Así evitaremos que un ciberdelincuente pueda conectarse a ella y robar nuestra información o la de nuestros clientes.

Si utilizas dispositivos móviles (smartphones, tablets, equipos portátiles, etc.) para acceder a tu información corporativa, **instala aplicaciones de administración remota.** En caso de robo o pérdida, te permiten localizarlo o realizar un borrado de los datos si fuera necesario.

Si no dispones de una VPN, cuando viajes evita el uso de redes wifi públicas (hoteles, cafeterías, aeropuertos, etc.), utiliza las conexiones 4G/5G en su lugar y accede a servicios que utilicen comunicaciones seguras (SSL, HTTPS, etc.).

Si tu casa a veces también es tu oficina, ahora ya sabes cómo protegerla.

Ruta Pyme Segura

Toda la información que maneja un negocio tiene valor, no solo para el empresario, sino también para otros, como la competencia o los cibercriminales. Empieza por identificar el capital digital de tu empresa. ¿Cuáles son los datos más importantes que almacena tu negocio? Puede ser cualquier cosa, desde tu propiedad intelectual hasta información sobre los clientes, inventario, información financiera, etc. ¿Dónde guardas todos estos datos? Una vez que tengas las respuestas a estas preguntas, podrás empezar a pensar en los riesgos a los que tus datos están expuestos.

Comprende y gestiona tus riesgos

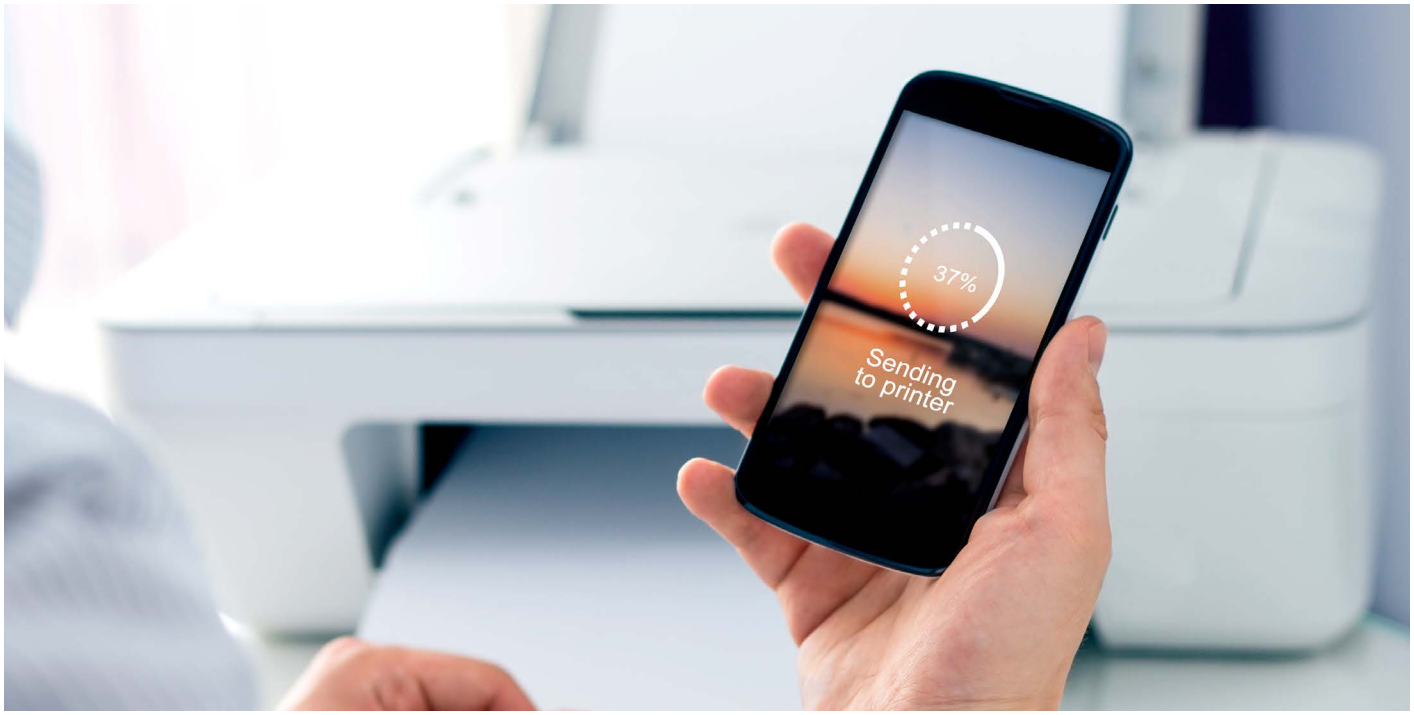
- Decide quién o quiénes serán los responsables de gestionar los riesgos de seguridad TI (Tecnología de la Información) en tu empresa.
- Elige qué nivel de riesgo estás dispuesto a aceptar.
- Elabora una Política de Seguridad que describa, paso a paso, qué estás dispuesto a hacer para gestionar los riesgos. Revísala al menos cada año para asegurarte que se ajusta a tus riesgos reales.
- Distribuye las responsabilidades de seguridad TI entre tus colaboradores y asegúrate que comprenden y asimilan su importancia.

Actualiza tu software (configuraciones seguras)

- Haz un inventario con todos tus activos de tecnologías de la información (instalaciones, equipos, hardware, software, etc.) para ser consciente de lo que tienes y de su valor.
- Actualiza sistemas operativos, softwares, firewares, etc. con parches y actualizaciones periódicas. Puedes activar la opción de «actualización automática» durante la
- instalación de muchos paquetes de software.
- Asegúrate de que tienes licencias de todo el software instalado.
- Revisa, periódicamente, las debilidades de tus sistemas mediante un análisis de vulnerabilidades (para empezar, puedes utilizar alguna herramienta gratuita) o, si tu equipamiento es más complejo, con una herramienta de pentesting (o test de penetración).
- Al menos hazlo una vez al año o cuando realices algún cambio importante de hardware o software.

Protege tu red

- Protege tu red contra ataques externos e internos.
- Comprueba si el dispositivo que conecta tu organización a Internet, el router que te ha proporcionado el proveedor de Internet (ISP del inglés: Internet Service Provider), incluye Firewall, que van a permitir controlar las conexiones de red del acceso a Internet. Si no es así, instala uno que incluya esta funcionalidad para tus equipos.
- Sigue las instrucciones del fabricante para mantenerlo bien configurado y actualizado. Permanece alerta de los mensajes que te vaya indicando.
- Consulta con un experto si sospechas que tu red ha sido comprometida o si observas una actividad poco habitual.
- Restringe el acceso a internet full.



Instala defensas contra malwares

- Utiliza en todos los equipos de la empresa un antimalware (algo más que un antivirus), o un paquete de seguridad con esta funcionalidad. Evita los gratuitos.
- Utiliza todas las prestaciones (antivirus, antispyware) que te ofrezca el paquete, aunque para ello haya que cambiar algunos hábitos. Asegúrate de que el escaneado se realiza al menos cada día y configura la herramienta para que se actualice automáticamente.
- Permite exclusivamente el uso de CD, DVD, USB, tarjetas SD o cualquier tipo de memoria flash que proporcione tu administrador de sistemas. Vigila su uso, dónde están, quién los tiene y qué contienen.
- Asegúrate que permitan cifrado y de que son escaneados para detectar malware cada vez que se usen. Muchos paquetes antimalware tienen la opción de analizar los dispositivos y medios extraíbles.

Gestiona el acceso a tus sistemas (privilegios de usuario)

- Para controlar el acceso a los sistemas y equipos utiliza nombres de usuario y contraseñas seguras.
- Asegúrate de que los empleados utilizan contraseñas seguras y que no las apuntan en papel o las comparten con otros usuarios.
- Limita los privilegios de administración de sistemas a quienes realmente sean administradores.
- Asegúrate de que los empleados sólo tengan acceso a las carpetas que necesiten para su trabajo.
- Mantén los datos sensibles (contabilidad, nóminas, clientes) separados y vigilados.
- Controla los elementos extraíbles (pendrives, discos duros u otros dispositivos externos)

Monitorea tus redes y servicios

- Para detectar posibles fallos de hardware o actividad inusual en tu red o en los dispositivos que se conectan a Internet, es indispensable monitorizarlos, para empezar, puedes utilizar alguna herramienta gratuita de monitorización o de análisis de protocolos.

- Si dispones de una red compleja deberías plantearte utilizar herramientas comerciales de control de tráfico de red que incluyen análisis de tráfico, uso de IP, etc.

- Asegúrate que los empleados avisen al responsable de seguridad ante cualquier actividad inusual que detecten y de que se disponen de los planes y experiencia para actuar ante estos eventos.

Enseña buenas prácticas (sensibilización y formación de usuarios)

- Asegúrate que todos los colaboradores conocen y aplican la Política de Seguridad definida y de que se insiste en su importancia en el protocolo de admisión de nuevos empleados.

- Incluye el cumplimiento de la Política como una clausula en los contratos.

- Recuerda, periódicamente, a los colaboradores, las buenas prácticas de seguridad, especialmente cuando cambia la Política o los riesgos.

- Si tu empresa utiliza Redes Sociales asegúrate de que los colaboradores están al tanto de cómo se deben comportar en las mismas cuando representan a la empresa y de que existen documentos que no se pueden compartir (sensibles o sujetos a propiedad intelectual).

Controla los dispositivos móviles de los colaboradores

- El uso de dispositivos móviles privados o corporativos (teléfonos, tablets) siempre debe tener la aprobación del responsable de seguridad.

Como mínimo se debe asegurar que:

- Tienen un antimalware instalado y actualizado.
- Usan PIN, contraseña u otro sistema de autentificación.
- Están cifrados.
- Podemos rastrearlos y borrarlos remotamente en caso de pérdida o robo.
- Los empleados informarán, inmediatamente, al responsable de seguridad en caso de pérdida o robo para que los datos puedan ser eliminados a la brevedad.

Gestiona los incidentes y la continuidad del negocio

- Cualquier evento, como un ataque de malware, pérdida o corrupción de datos, robo de portátiles, catástrofe, fallo crítico u otro que interfiera con la actividad normal del negocio es un incidente.

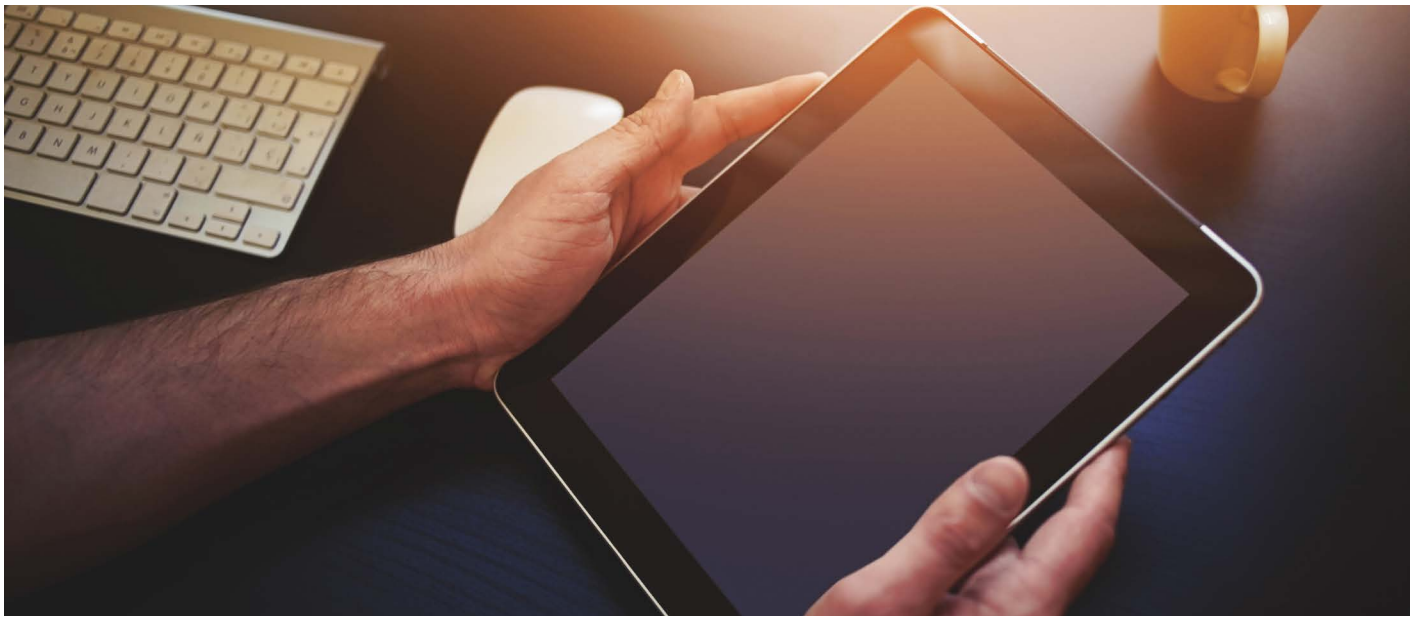
- Decide, redacta y aprueba, qué hacer y qué no hacer en caso de que suceda.

- Prueba que este plan funciona.

- Obtén ayuda y experiencia, externa si fuera necesario, para tratar con los incidentes.

- Si no dispones de ella, identifica a quién puedes llamar.

- Para aprender de la experiencia registra cada incidente, sus causas, las dificultades para recuperarse y cómo prevenirlo en el futuro.



Recomendaciones de ciberseguridad en tu empresa

Puesto de Trabajo
Mantén tu escritorio limpio de papeles que contengan información sensible.
Bloquea la sesión de tu equipo cuando no estés en tu escritorio.

Dispositivos
No modifiques la configuración de los dispositivos de tu empresa.
No instales aplicaciones no autorizadas.
No conectes dispositivos USB no confiables.

Uso de Equipos No Corporativos
No manejes información corporativa en equipos públicos.
Si accedes al correo corporativo desde tu equipo personal no descargues ficheros al equipo.

Fugas de Información
No facilites información sensible si no estás seguro de quién es el receptor de la misma.
Destruye la información sensible en formato papel. No la tires al basurero.
No mantengas conversaciones confidenciales en lugares donde pueden ser oídas por terceros.

Gestión de Credenciales
No compartas tus credenciales de acceso (usuario y contraseña).
No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal.
No dejes tus credenciales en lugares visibles.

Navegación
Evita acceder a páginas web no confiables.
No pinches en enlaces (links) sospechosos.

Protección de la Información
Realiza copias de seguridad de aquella información sensible que sólo esté alojada en tus dispositivos.

Viaje seguro
Procura no transportar información sensible en dispositivos extraíbles. Si lo haces, encripta la información.

Contacta a nuestros expertos

Nicolás Corrado
Socio Líder de Cyber en Deloitte
nicorrado@deloitte.com
+56227298665

Marcelo Díaz
CEO Makros
mdiaz@makros.cl
+56223349334

Oficina central

Rosario Norte 407
Las Condes, Santiago
Chile
Fono: +56 227 297 000
Fax: +56 223 749 177
deloittechile@deloitte.com

Regiones

Av. Grecia 860
Piso 3
Antofagasta
Chile
Fono: +56 552 449 660
Fax: +56 552 449 662
antofagasta@deloitte.com

Alvares 646
Oficina 906
Viña del Mar
Chile
Fono: +56 322 882 026
Fax: +56 322 975 625
vregionchile@deloitte.com

Chacabuco 485
Piso 7
Concepción
Chile
Fono: +56 412 914 055
Fax: +56 412 914 066
concepcionchile@deloitte.com

Quillota 175
Oficina 1107
Puerto Montt
Chile
Fono: +56 652 268 600
Fax: +56 652 288 600
puertomontt@deloitte.com

Deloitte.

www.deloitte.cl