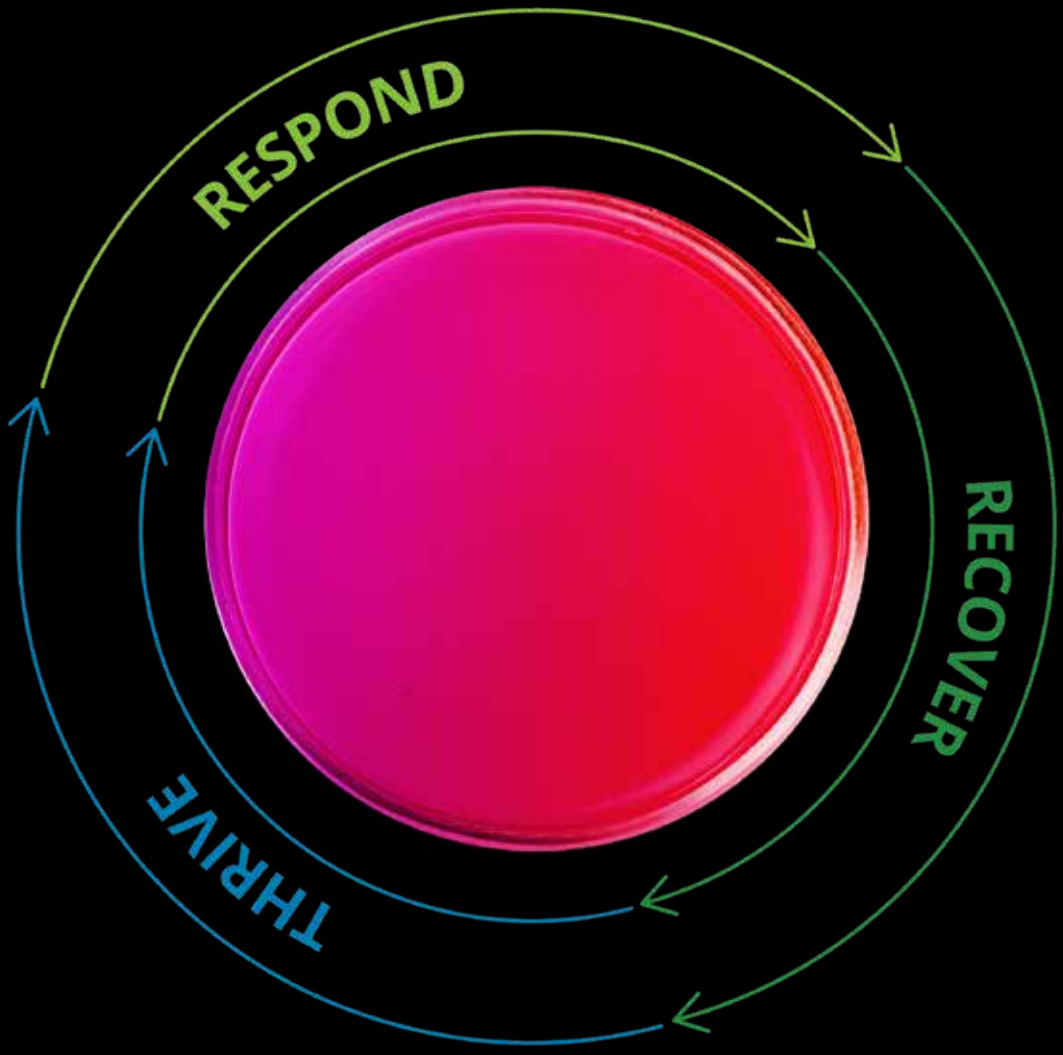
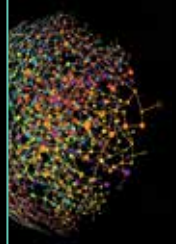
Deloitte.



Cyber
Consideraciones de Ciberseguridad en medio de una pandemia global

CREANDO UN IMPACTO SIGNIFICATIVO
Desde 1845

Lo que estamos viendo ...



A medida que los efectos del coronavirus (COVID-19) se hacen presentes en todo el mundo, las acciones principales de gobiernos y empresas se enfocan, cada vez más, en garantizar el bienestar y la seguridad de sus ciudadanos, colaboradores y clientes.

En este contexto particular, en el que la difusión de información oficial es fundamental para definir las medidas de control y protección que se deben poner en marcha, los cibercriminales han encontrado un nuevo nicho de negocio.

Su nueva forma de operar consiste en hacerse pasar por organismos internacionales de salud (como la Organización Mundial de la Salud y otras organizaciones de atención médica) y otras entidades gubernamentales, a través de campañas de correo electrónico maliciosas, diseñadas invocando el miedo, con la esperanza de desencadenar acciones que les brinden la oportunidad de obtener acceso a sistemas sensibles de información.

Sin embargo, éste no es el único aspecto relacionado con ciberseguridad al que las organizaciones deberán prestar atención. La coyuntura actual ha provocado también que muchas empresas, con el propósito de responder activamente a los riesgos de salud relacionados con el COVID-19, hayan comenzado a migrar su modo de operación regular a uno alterno, basado en la colaboración remota y las oficinas virtuales.

Contar con un enfoque integral y bien estructurado durante un evento extraordinario, como el que actualmente nos encontramos viviendo, permitirá a las organizaciones abordar proactivamente los desafíos cibernéticos.

A continuación, presentamos algunas consideraciones y recomendaciones en materia de ciberseguridad que las organizaciones pueden considerar al momento de definir la estrategia que implementarán para hacer frente al COVID-19.

Consideraciones generales de ciberseguridad en medio de eventos extraordinarios

Los procesos de negocio cambian y hay una mayor demanda hacia los servicios de acceso remoto y colaboración, lo que crea nuevos riesgos | **Se recomienda adaptar las políticas, procesos y controles de ciberseguridad al nuevo escenario de operación**

A medida que la pandemia evolucione, cada vez serán más las organizaciones que necesiten ajustar sus procesos actuales para poder ejecutar la mayor parte de sus operaciones. En respuesta a este cambio, los controles de seguridad de la información relacionados también deben ajustarse y las configuraciones de seguridad correspondientes tendrán que actualizarse.

Durante la pandemia, por mencionar un ejemplo, se registra un acceso remoto masivo de colaboradores, para lo cual, las organizaciones necesitan contar con una mayor capacidad de procesamiento y conectividad. También, requieren abrir o expandir más "interfaces" para acceder a los servicios internos, y habilitar derechos de acceso a datos, a través de una red pública (Internet).

Las empresas no deben eludir ni abandonar las medidas de gestión de riesgos cibernéticos, debido a este contexto particular. El ajuste temporal de las políticas de seguridad y gestión de capacidad de la red harán que la organización pueda hacer frente, de manera efectiva, a las amenazas que plantea el nuevo escenario de operación.

A medida que las organizaciones recomiendan que los empleados trabajen de forma remota, aumenta el uso de dispositivos móviles y el acceso remoto a los sistemas empresariales centrales | **Se recomienda fortalecer la gestión de acceso a la identidad organizacional y el monitoreo y correlación de eventos**

Los riesgos cibernéticos aumentan al realizar trabajo remoto o desde casa (home office). Las medidas proactivas pueden mejorar la experiencia de los usuarios y su seguridad al momento de trabajar bajo este esquema. Los dispositivos que no cuenten con la protección necesaria podrían provocar la pérdida de datos, violaciones de privacidad y sistemas víctimas de *ransomware*.

Las organizaciones deberán:

- **Implementar una capa consistente de autenticación multifactor (MFA) o una autenticación progresiva según la criticidad de las solicitudes de acceso.**
- **Garantizar que los procesos de gestión de identidad aseguren todas las identidades de terceros con acceso a la red de la compañía.**
- **Tener una visión integral de las identidades privilegiadas dentro de sus entornos de TI, incluido un procedimiento para detectar, prevenir o eliminar cuentas huérfanas.**
- **Refinar la granularidad del monitoreo de seguridad y enriquecer el monitoreo en escenarios de operación remota.**
- **Hacer seguimiento a la operación de las funciones de gestión de ciberseguridad, identificar cuáles de éstas puedan llegar a estar fuera de servicio y los retrasos que se presenten en la respuesta de seguridad.**

Las crisis, a menudo, reducen los niveles de alerta y protección de los usuarios finales y llevan a los ciberdelincuentes a aprovecharse de esta situación y operar bajo esquemas maliciosos | **Se recomienda aumentar la conciencia ante el surgimiento de nuevas amenazas**

Durante la pandemia, los colaboradores de las diversas organizaciones reciben, de manera constante, una gran cantidad de información de fuentes internas y externas al respecto. Esto puede provocar una presión psicológica, que reduzca su estado de alerta e impacte en su nivel de respuesta hacia amenazas como ataques de ingeniería social o *phishing*.

Las campañas de *phishing* relacionadas con el COVID-19, en las que los cibercriminales se hacen pasar, por ejemplo, por organizaciones de salud acreditadas, están en aumento. Por esta razón, es importante que las organizaciones permanezcan atentas a mensajes fraudulentos relacionados con esta pandemia.

Los ciberdelincuentes pueden enviar correos electrónicos con archivos adjuntos maliciosos o enlaces a sitios web fraudulentos, para engañar a las víctimas y conseguir que revelen información confidencial o realicen donativos a organizaciones o causas fraudulentas. Ataques como estos pueden propagarse de manera rápida y extensa en toda una red empresarial, provocando el robo de identidad y la presentación de reclamos de pagos y programas de beneficios falsos.

Pero el aumento de presión psicológica no solo impacta en este sentido. Este fenómeno también puede provocar que los colaboradores sean más propensos a cometer errores en el manejo de procesos o tengan comportamientos no seguros, como compartir información privada o credenciales de acceso.

Por lo anterior, se recomienda ejecutar acciones de concientización con mensajes, con los siguientes lineamientos:

- **Tener cuidado al manejar cualquier correo electrónico con asunto, archivo adjunto o hipervínculo relacionado con COVID-19, y desconfiar de las súplicas, textos o llamadas de las redes sociales relacionadas con COVID-19.**
- **Utilizar fuentes confiables, como sitios web legítimos del gobierno para obtener información actualizada y basada en hechos sobre COVID-19.**
- **No revelar información personal o financiera en el correo electrónico, y no responder a solicitudes de correo electrónico para esta información.**

Un mayor riesgo de fuga de datos confidenciales o privados debido a su exposición en entornos no seguros | **Se recomienda gestionar las conexiones remotas**

Las oportunidades de acceso remoto y colaboración a través de redes y dispositivos no corporativos han aumentado y en la situación actual los empleados pueden sentirse tentados a utilizar estos medios en vez de los corporativos. Esta situación podría exponer datos confidenciales en redes no corporativas, redes sociales y/o plataformas de terceros que no cuentan con las medidas de protección apropiadas.

Asimismo, en los últimos años han entrado a los hogares muchos dispositivos de red inteligentes pero con funciones de seguridad débiles. Las numerosas debilidades de seguridad de estos dispositivos plantean riesgos que han sido advertidos por diferentes agencias de seguridad los cuales cobran mayor relevancia e impacto bajo una operación remota "masiva". Algunos de estos dispositivos también generan riesgos derivados de una configuración estándar no segura, la ausencia de mantenimiento o soporte por parte del proveedor, la falta de actualizaciones de seguridad y posibilidades de acceso desconocidas por el usuario.

Las empresas deben identificar y clasificar los requisitos de conexión remota, identificar los riesgos relacionados y confirmar rápidamente el umbral de seguridad del negocio permitido bajo esta situación. Al mismo tiempo, deben evitar la aceptación de una gran cantidad de excepciones que socavan el nivel de gestión y control de seguridad de la información. En especial cuando estas excepciones sean debido a necesidades de negocio secundarias.

La transformación digital permite a las organizaciones desarrollar sistemas y medidas de seguridad para evitar la intrusión y el acceso a sistemas críticos | **Se recomienda contar con un plan de recuperación cibernética**

En la era cibernética actual, que se caracteriza por una mayor transformación tecnológica, el uso de la nube y mayores capacidades de red, el panorama de amenazas digitales continúa en aumento. En este contexto, los ciberdelincuentes buscan atacar sistemas operativos y capacidades de respaldo, de manera simultánea, bajo un esquema de operación altamente sofisticado, que puede provocar un riesgo importante para cualquier empresa.

Las organizaciones pueden mejorar su postura de defensa y preparación para los ciberataques con una buena higiene cibernética, una estrategia de respuesta a incidentes y el diseño e implementación de soluciones de recuperación cibernética, las cuales permitirán mitigar el impacto de los ciberataques. Un programa de resiliencia cibernética viable expande los límites de los dominios de riesgo tradicionales para incluir nuevas capacidades, como servicios de apoyo a los colaboradores, herramientas de comunicación y colaboración remotas, y una bóveda de recuperación.

Consideraciones de ciberseguridad dependientes de la situación de la compañía

1. Para las empresas que no han implementado soluciones de colaboración y acceso remoto y no tienen oficinas remotas a gran escala

- **Evaluar** el alcance y el modelo de colaboración empresarial remota en función del tamaño de la compañía y las características de la industria.
- **Seleccionar** herramientas de colaboración razonables adecuadas para escenarios comerciales específicos. Para ello tener en cuenta:
  - *Las características de seguridad de la plataforma o el software de oficina remota.*
  - *Las condiciones de propiedad de los datos y protección de la privacidad establecidos en el acuerdo de uso / cooperación*
  - *Las certificaciones de seguridad de la industria.*
  - *Otras características relacionadas: portabilidad, disponibilidad, escalabilidad, entre otros.*
- **Clarificar** el alcance del acceso a servicios de oficina por parte de terceros, definir los límites de integración con sistemas de terceros y fortalecer el control de acceso de seguridad a datos confidenciales.
- **Mejorar** el monitoreo de seguridad y la protección de los servicios y sistemas de información de la empresa, y, de ser necesario, reorganizar los roles de análisis y respuesta a ataques de ciberseguridad.

2. Para empresas con acceso remoto flexible y soluciones de colaboración ya implementadas

- **Llevar** a cabo actividades de concienciación y entrenamiento de seguridad de la información y ciberseguridad en aspectos relacionados con el modelo de colaboración remota de los empleados.
- **Realizar** un seguimiento oportuno de accesos sospechosos y situaciones anormales.
- Los departamentos de TI y seguridad deben ejecutar los planes de seguridad para oficinas remotas en escenarios especiales y repasar los procesos de respuesta de emergencia correspondientes.
- **Centrar** la atención en garantizar instalaciones de servicio que proporcionen aceso remoto y colaboración de forma segura, tales como: capacidad, disponibilidad y seguridad de los servicios VPN, seguridad de los servicios de correo electrónico y acceso a los datos almacenados en la red interna, entre otros.
- **Revisar** y de ser posible, mejorar, las medidas de protección de seguridad de los servicios e interfaces de acceso remoto (que incluyen, entre otros, autenticación multifactorial, la eliminación oportuna de privilegios de acceso remoto y el monitoreo sobre los servicios de acceso remoto) y los planes de emergencia correspondientes para mejorar la flexibilidad de los servicios de red.
- **Fortalecer** las capacidades de monitoreo y análisis de seguridad de toda la red de la empresa, prestando especial atención a los comportamientos de acceso privilegiado.
- **Enfocar** el monitoreo en el uso de datos confidenciales y en los servicios centrales que brindan acceso a estos datos (tales como el correo electrónico, plataformas de operaciones comerciales, entre otros).
- **Dar prioridad** a las soluciones de acceso y oficina remota aprobadas por la empresa, y tratar de evitar el uso temporal de software de terceros para compartir información confidencial.
- **Realizar** oportunamente copias de seguridad de los datos en la nube y proporcionar varias versiones de copias de seguridad históricas.

3. Otros escenarios de riesgo de seguridad para observar

Ciberseguridad en oficinas corporativas desatendidas:

- **Reforzar** las restricciones de acceso físico a las oficinas.
- **Organizar** el monitoreo de seguridad física en el sitio.
- **Definir** esquemas para responder de manera oportuna a condiciones anormales en el lugar.
- **Establecer** un sistema de servicio remoto para que el personal en servicio realice el monitoreo en tiempo real de la sala de computadoras, la red, los sistemas, las condiciones de operación de las aplicaciones, el uso de recursos.
- **Apagar** equipos innecesarios de red periférica y nodos en la oficina.

Protección de datos privados de los empleados:

- En respuesta a los requisitos de control de pandemia, las empresas deben controlar estrictamente el acceso, transmisión y uso de dichos datos en el proceso de estadísticas de información de salud y gestión de empleados para asegurar un alcance limitado de conocimiento.
- Establecer el nivel de protección de datos clínicos y médicos y evitar el uso de plataformas de terceros para su almacenamiento o transmisión.

Conclusión

Conforme mejore la pandemia y la rutina de trabajo vuelva gradualmente a la normalidad, las compañías tendrán que eliminar las excepciones, reglas especiales, planes temporales o entradas que se habilitaron durante la fase de oficina remota. Asimismo, deberán llevar a cabo un inventario y una actualización de las operaciones de seguridad de la red, establecer nuevamente las medidas adecuadas para la operación rutinaria y regresar a la gestión de la seguridad, bajo la filosofía de cero confianza.

En un contexto como el actual, será crucial que las estrategias cibernéticas estén alineadas a las funciones del negocio, las operaciones, la continuidad comercial / la resiliencia técnica y la gestión de crisis. Los planes de las organizaciones tendrán que contemplar métodos únicos que les permitan conocer los riesgos a los que su red puede estar expuesta, detectar amenazas avanzadas y descubrir brechas sistémicas en el proceso de respuesta ante posibles incidentes.

El equipo de profesionales de **Deloitte** tiene la capacidad para ayudar a las organizaciones a prepararse estratégicamente para responder, recuperarse y transformarse ante los incidentes cibernéticos de alto impacto que podrían interrumpir gravemente las operaciones, dañar su reputación y destruir o mermar, de manera significativa, su valor.

Contactos

Andrés Gil
Socio Líder Regional
Socio Argentina, Bolivia y Paraguay
angil@deloitte.com

Samuel Ardila
Socio Colombia
slardila@deloitte.com

Adriana Berlingeri
Socia Ururguay
aberlingeri@deloitte.com

Andrés Casas
Socio Costa Rica
ancasas@deloitte.com

Christiam Garratt
Socio Perú
cgarratt@deloitte.com

Santiago Gutiérrez
Socio México y Centroamérica
sangutierrez@deloittemx.com

Deloitte.