

# La ciberseguridad durante la pandemia de COVID-19

**Resiliencia a la pandemia:** No es demasiado tarde. Su organización puede tomar medidas proactivas ahora para adaptarse a las cambiantes necesidades del negocio ante una pandemia y a fin de garantizar la continuidad de sus operaciones comerciales.



## Prepare al personal y promueva su bienestar

- ▶ **Establezca expectativas:** Reconsidere la exigencia de "siempre disponible" y establezca metas y expectativas claras.
- ▶ **Establezca canales de comunicación:** Estos mantienen la sensación en empleados y clientes de estar siempre conectados y coordinados.
- ▶ **Rastree, monitoree y actualice:** Las actualizaciones evitan la propagación de información errónea, el pánico y la disminución de la productividad.
- ▶ **Capacitaciones de sensibilización:** Brinde capacitación a los empleados para protegerse contra la ingeniería social de parte de hackers que intenten explotar el actual escenario de COVID-19.



## Aproveche la tecnología para ampliar las capacidades del negocio digital

- ▶ **Amplie capacidades de trabajo remoto:** Mejore la infraestructura de trabajo remoto para respaldar mejor las operaciones de negocio.
- ▶ **Planifique la respuesta y la continuidad del negocio:** Revise los planes de respuesta y contingencias, como canales de comunicación alternativos para empleados (por ej., celulares, redes sociales).
- ▶ **Comunicación y redes seguras:** Establezca plataformas que permitan a los empleados trabajar de forma remota en las actividades diarias.
- ▶ **Tecnología para autoservicio:** Establezca plataformas de autoservicio como chatbots y/o IVR (Interactive Voice Response) para la gestión de incidentes.



## Priorice la ciberseguridad

- ▶ **Verifique la seguridad de datos y backup:** Revise las necesidades de seguridad de los datos de los empleados remotos, actualice las políticas, los procedimientos y comunice las prácticas de manejo de datos.
- ▶ **Asegure la infraestructura virtual:** Revise y fortalezca la seguridad de la infraestructura, tales como las VPNs y la infraestructura de escritorio virtual.
- ▶ **Refuerce la seguridad de PCs y equipos móviles:** Implemente o mejore las PCs/laptops y la seguridad de los dispositivos móviles para monitorear y responder a las ciberamenazas.
- ▶ **Mantenimiento de terceros:** Obtenga actualizaciones periódicas de sus proveedores de servicios de seguridad; Revise los SLA según sea necesario.



Una pandemia no es un evento aislado y los períodos de enfermedades pueden venir en 2 o 3 oleadas, entre 3 y 12 meses de diferencia. Es probable que la duración total de una pandemia sea de 12 a 18 meses.

Fuente: Canadian Centre for Occupational Health and Safety

Una pandemia puede resultar en un posible ausentismo del personal que exceda el 40% por largos períodos.

Fuente: Gartner



## ¿Cómo puede ayudarle EY?

### 1 Evaluación y plan de impacto COVID-19

Una evaluación rápida de los impactos, riesgos y la resiliencia organizacional ante el COVID-19. La evaluación se centra en aspectos operativos, tecnológicos, de ciberseguridad, financieros, laborales y tributarios para proporcionar recomendaciones priorizadas y un plan de estabilización inmediato para abordar los riesgos e impactos.

### 2 Comando de operaciones ante crisis

EY comprende que sus procesos de negocio y su fuerza laboral se verán afectados como resultado del COVID-19. Con nuestra presencia global y el conocimiento en una amplia gama de servicios de gestión de crisis, EY puede implementar centros de comando de negocios virtuales para apoyar a sus equipos. EY también puede convocar a especialistas para ayudarle ante la escasez de personal especializado en áreas estratégicas de su negocio.

### 3 Manteniendo la ciberseguridad

Cuando los miembros clave de su equipo cibernético o TI no puedan realizar sus tareas debido a enfermedad o necesitan cuidar a sus seres queridos, EY puede proporcionarle profesionales capacitados y experimentados para ayudar a mantener proyectos, ejecutar servicios y brindar orientación profesional para continuar operando su programa de seguridad cibernética.

### 4 Capacitación y sensibilización sobre Seguridad & Privacidad

A medida que las organizaciones recurren al teletrabajo, se enfrentan al desafío de capacitar rápidamente a gerentes y empleados sobre roles y responsabilidades relacionadas con la protección de tecnología y datos. EY puede crear e implementar rápidamente un programa de capacitación, junto con las políticas necesarias para ayudar a su organización a proteger las joyas de la corona en estos momentos de crisis.

## Contactos



**Jorge Acosta**  
Socio Líder de Consultoría  
Jorge.Acosta@pe.ey.com



**Elder Cama**  
Socio de Consultoría  
Elder.Cama@pe.ey.com