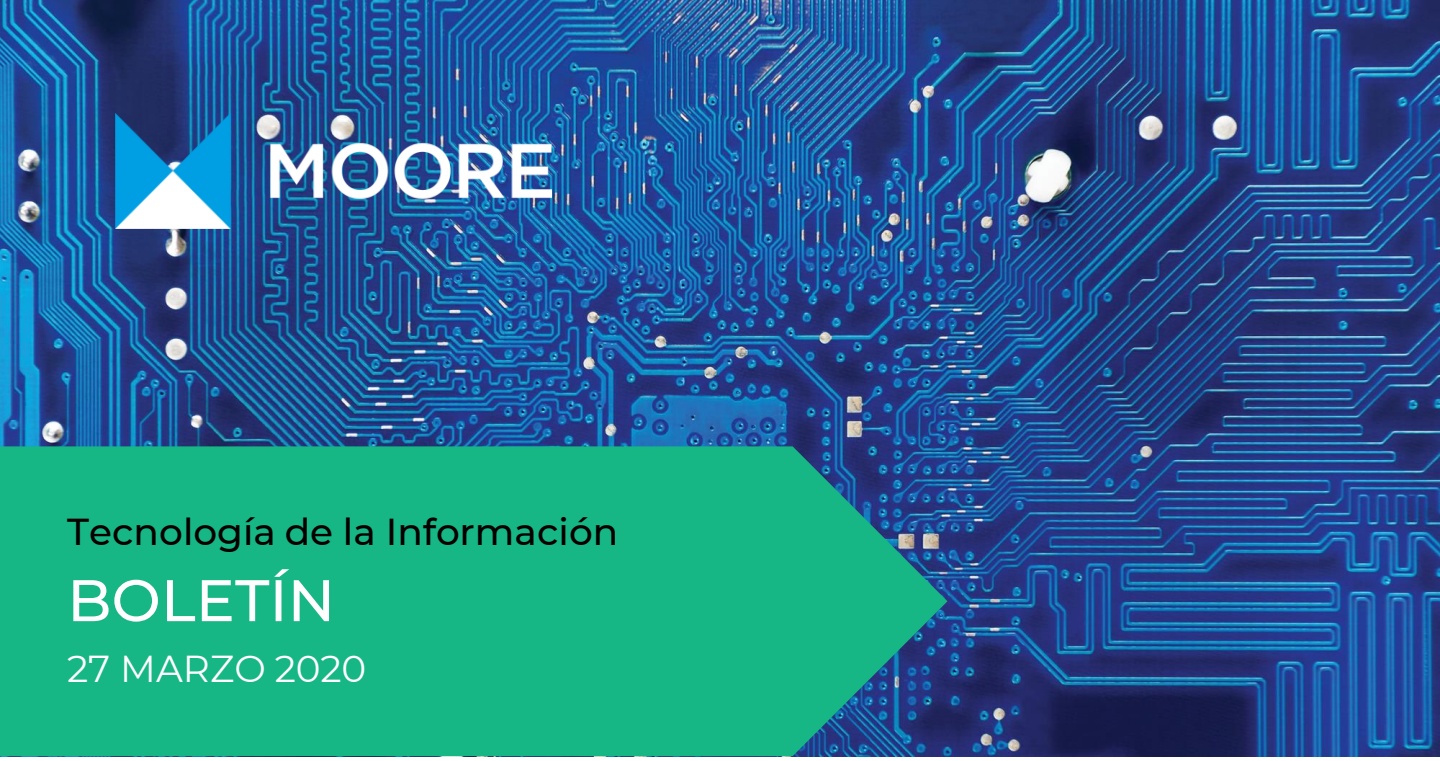

MOORE

Tecnología de la Información

BOLETÍN

27 MARZO 2020

¡RESILIENCIA ORGANIZACIONAL, UN COMPROMISO DE TODOS!

En los últimos días mundialmente se ha tenido que responder a la llegada del coronavirus (COVID-19), poniendo en la mesa de juego todas las estrategias para reducir el impacto que genera este evento a nivel económico, gubernamental y con una connotación mayor en la vida diaria de todos los habitantes del planeta. A medida que se ha venido desarrollando el virus hemos notado como en los países donde surgió inicialmente se vieron obligados a parar fábricas, oficinas y demás espacios colectivos con el fin de reducir la expansión en la población y concentrar todos los esfuerzos en la contención y eliminación del virus en las personas afectadas.

Es por esto por lo que las empresas han tenido que transformar su modelo de operación tradicional; generando nuevas estrategias que le permitan desarrollarse de manera remota de forma parcial o total para disminuir el impacto que implica no afectar el desarrollo de la operación sin exponer la vida de nuestros colaboradores.

A continuación, presentamos los desafíos tecnológicos a los que se están enfrentando nuestras empresas:

- Desplegar correctamente la contingencia de TI sin afectar la seguridad de nuestra información, dado que las compañías requieren dar acceso remoto a sus sistemas a colaboradores y terceros, sin embargo, deben considerar un panorama integral de riesgos a los que se enfrentan al permitir el acceso remoto mediante internet. En estos casos un análisis de riesgos tecnológicos permitirá a las compañías definir medias de seguridad efectivas que le permitan mantener segura la operación.

- En algunos casos permitir el acceso remoto de manera permanente y libre requiere que se tenga una buena configuración en la capa de acceso de nuestros sistemas usando un modelo robusto de autenticación de varios factores el cual permita controlar el acceso a los sistemas únicamente al personal autorizado. En estos casos se recomienda implementar en los sistemas tecnologías MFA (Métodos de autenticación multifactorial) para verificar la legitimidad de los usuarios que acceden.

- La comunicación desde diferentes sitios remotos debe estar apalancada por un modelo que garantice la conectividad de los colaboradores desde sus casas ya que la intermitencia en la conectividad podría generar demoras y reprocesos. Si bien este aspecto no depende netamente de las compañías, ya que seguramente la conexión desde cada uno de los hogares de los colaboradores es proporcionada por ellos mismos. Se ha visto que los gobiernos locales están exigiendo compromiso a los prestadores de internet presentes en los países garantizar la conectividad y estabilidad de las conexiones de internet a cada uno de sus clientes. Incluso en casos como Colombia algunos proveedores han aumentado la velocidad de las conexiones y han generado tarifas cómodas para incentivar la adquisición de este tipo de planes.

- Monitorear de manera permanente toda la infraestructura tecnológica que soporta la operatividad para evitar pérdidas de disponibilidad de los sistemas. En este tipo de situaciones las compañías también se convierten en un objetivo tentador para los ataques cibernéticos. Así mismo el uso de sistemas de monitoreo IPS e IDS los cuales aumentan la seguridad de la red ya que detectan y previenen ciberataques.

- Definir y desplegar correctamente las herramientas que pueden llegar a representar una ventaja tecnológica si se implementan dentro de la organización. En este caso es importante tener identificado con claridad las necesidades de la compañía desde cada uno de sus procesos. Considerando dentro herramientas utilitarias para hacer meetings virtuales, plataformas de correo electrónico oficial para enviar y recibir información y definir rutas compartidas para compartir información. Todo lo anterior utilizando protocolos seguros como HTTPS, certificados digitales, servicios SFTP y cifrado fuerte TLS.

- Adoptar esquemas de computación en la nube para facilitar la administración de los sistemas y aumentar el porcentaje de disponibilidad en caso de que las situaciones de riesgo relacionadas a la epidemia se materialicen y limiten la ejecución de cierto tipo de actividades en los centros de datos.

Otros desafíos no tecnológicos a tener en cuenta:

- Organizacionalmente se deben definir lineamientos que estructuren y organicen el esquema de comunicación que se va a adoptar para la modalidad de trabajo remoto con el fin de garantizar un correcto y efectivo seguimiento a la ejecución de tareas y actividades. Adicionalmente la forma en la que se puede solicitar a poyo adicional en caso de que se requiera.

- Las gerencias de las diferentes áreas deben estar en la capacidad de adaptar los procesos internos a la modalidad de trabajo remoto dentro de lo posible para evitar exponer a los colaboradores a situaciones físicas que faciliten el contagio del virus.

- Desarrollar campañas de concientización a los colaboradores para que dentro de su labor diaria acaten todas las recomendaciones sanitarias que sean compartidas por los organismos estatales encargados.

- Medir y reconocer esfuerzos adicionales que se deben generar para fortalecer el control y la continuidad de la operación.

- Identificar aliados estratégicos con los cuales podamos generar dinámicas de apoya para poder sopesar todos los elementos disruptivos que surgen en estos momentos de pandemia.

- Desarrollar campañas de higiene psicológica para este tipo de situaciones de emergencia lo cual generan estrés y preocupación a todas las personas.

La implementación de estrategias que estén alineadas con buenas practicas de seguridad permitirán a la empresa fortalecer los procesos core del negocio, obtener resultados positivos ante contingencias a la par que cuida de su personal.