RECOMENDACIONES DESDE LA PERSPECTIVA DE TECNOLOGÍA

Pese a vivir en un mundo interconectado, hay situaciones inesperadas como crisis ambientales o sanitarias a nivel mundial que ponen a prueba cualquier músculo tecnológico de las compañías. La situación con el COVID-19, por ejemplo, ha hecho que las empresas, buscando proteger y cuidar su talento humano, encuentren grandes oportunidades en la tecnología para garantizar la continuidad de su operación.

Para ello, la conectividad remota es una excelente alternativa, pero es necesario tener algunos cuidados para no poner en riesgo a la organización. A continuación, describimos algunos retos y/o riesgos que enfrentamos al trabajar de manera remota.

TECNOLOGÍA:

RIESGO / RETO: Habilitar el trabajo remoto.

1. Implica brindar acceso a herramientas de colaboración, como correo electrónico, video y teleconferencia, herramientas de ofimática, carpetas y archivos compartidos.

DESCRIPCIÓN:
Teniendo en cuenta las medidas de control tomadas para prevenir y contener el COVID-19, es importante que tus colaboradores, proveedores, aliados, clientes y demás interesados puedan interactuar a través de canales virtuales, de tal forma que se promueva el autoaislamiento sin afectar la operación normal de la Compañía, o por lo menos, mitigando considerablemente la afectación.

RECOMENDACIONES:
Usa servicios, canales de comunicación y herramientas que se puedan consumir desde Internet y desde cualquier dispositivo, que sean confiables y tengan todos los mecanismos de seguridad en acceso (autenticación y perfilación) y de confidencialidad de la información (encriptación de datos y de canales de comunicación).

2. Brindar acceso a aplicaciones y procesos automatizados de negocio.

DESCRIPCIÓN:
Para la operación de las compañías, normalmente los empleados, proveedores y demás interesados, requieren acceder a aplicaciones tales como ERP, CRM, aplicativos transaccionales, entre otros. Para que el trabajo y la operación remota funcione, se debe dar acceso a estas aplicaciones, pero teniendo en cuenta que ya no van a estar dentro de las instalaciones y dentro de las redes y los sistemas de comunicaciones propios de la compañía.

RECOMENDACIONES:

- En caso de que las aplicaciones estén publicadas y puedan ser accedidas desde Internet, realiza la conexión desde sitios seguros (espacios en los cuales las conexiones a Internet son seguras y privadas).
- En caso de que las personas no cuenten con servicio de Internet en sus hogares, la Compañía debería ofrecer alternativas como la asignación temporal de planes de datos a través de líneas celulares, módems móviles, entre otros (teniendo en cuenta que estas líneas son la forma más rápida y segura de habilitar estas conexiones).
- En caso de que las aplicaciones no estén publicadas en Internet, se debe garantizar que el acceso remoto se dé con todos los protocolos de seguridad que estos casos demandan (activación de VPN o redes privadas virtuales para las personas que van a acceder de manera remota). La información y los datos que se guardan en las aplicaciones y sistemas de las compañías son un activo estratégico que debemos cuidar incluso en momento de crisis. Debemos dar acceso remoto sin descuidar los elementos de seguridad que sean pertinentes.
- Nota: hay aplicaciones que, por su diseño, no pueden ser accedidas desde Internet. Estas aplicaciones sólo pueden accederse de manera remota usando herramientas que permiten simular la conexión a la red interna, como si el usuario estuviera dentro de las instalaciones de la compañía. En caso de que se cuente con este tipo de aplicaciones y ellas requieran ser accedidas en un escenario de trabajo remoto, se debe adquirir y habilitar este tipo de tecnología de simulación o virtualización para poder dar acceso.

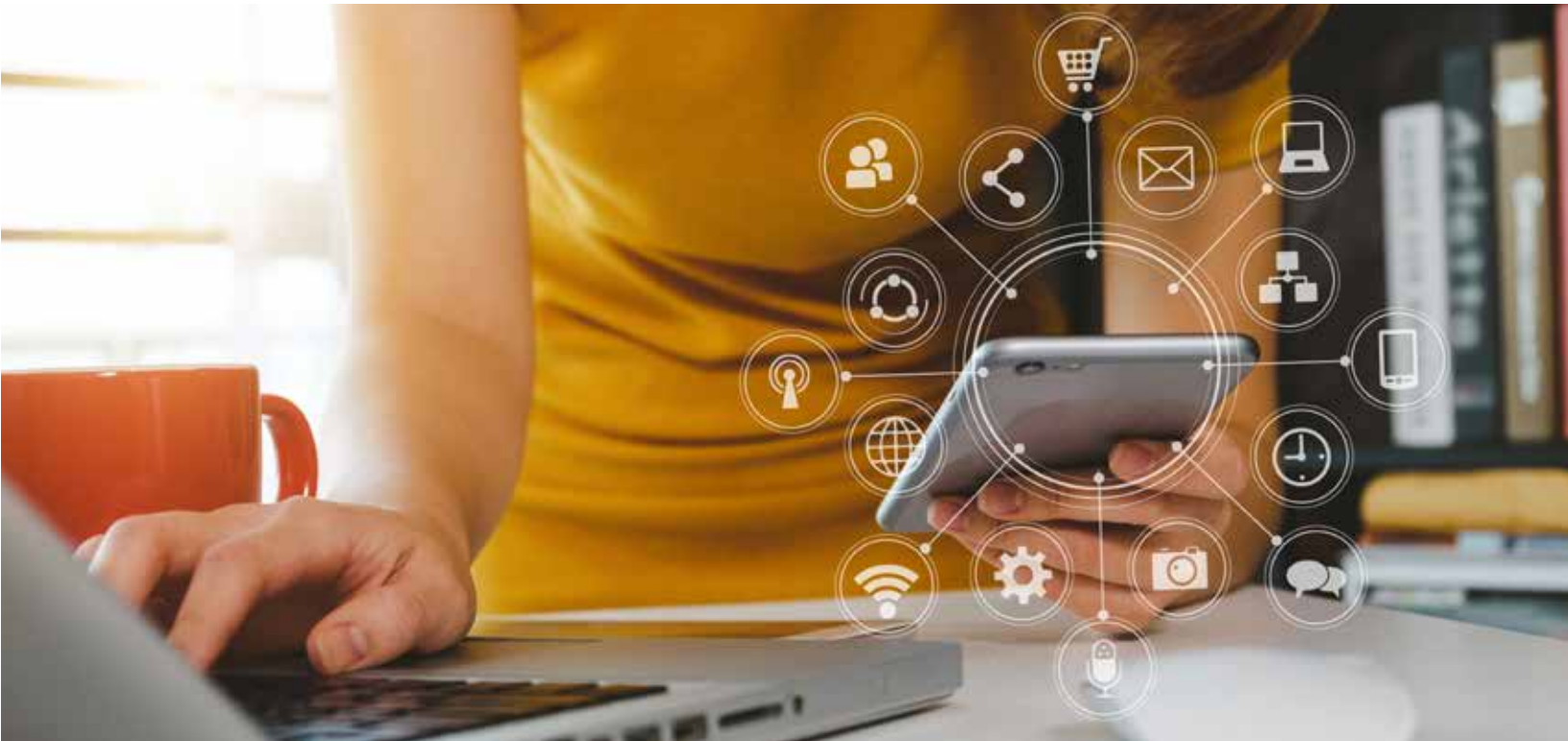
RIESGO / RETO: Información y comunicación.

DESCRIPCIÓN:

En momentos de crisis, la información, la comunicación y sus flujos internos y externos son un factor relevante y determinante que deben ser gobernados y gestionados eficazmente dentro de las organizaciones. Los aspectos tecnológicos no se escapan a esta premisa y, por el contrario, al ser la tecnología un habilitador relevante como medio de transmisión de información, se debe considerar su control y su modelo de gobierno.

RECOMENDACIONES:

Centraliza la información oficial en un único responsable (persona o equipo de trabajo). La única información legítima y veraz será la que esté avalada por este único ente responsable.



RIESGO / RETO: Seguridad.

DESCRIPCIÓN:

Los estados de alerta y los momentos de crisis son aprovechados normalmente por personas u organizaciones maliciosas que realizan ataques cibernéticos a las compañías. Algunos de estos ataques se hacen aprovechando vulnerabilidades en los sistemas y en la infraestructura tecnológica. Otros se hacen aprovechando los momentos de miedo y confusión para que las personas, sin saberlo, entreguen sus credenciales y sus claves de seguridad.

RECOMENDACIONES:

- Refuerza las campañas de uso adecuado del correo y otras herramientas de trabajo virtual como video y teleconferencia, herramientas de ofimática, carpetas y archivos compartidos, recalcando:
  - » No abrir correos, enlaces o archivos adjuntos dentro de correos de personas que no sean contactos habituales o sean de origen sospechoso. Tener especial cuidado con aquellas comunicaciones que fomenten el miedo y la incertidumbre.
  - » Nunca entregar usuarios, claves, credenciales o elementos de seguridad que sean personales. Ninguna entidad oficial solicita estos datos.
- Mantén, a través de políticas y buenas prácticas, la actualización permanente de los sistemas de seguridad como:
  - » Antivirus.
  - » Cortafuegos.
  - » VPN.
  - » Sistemas de autenticación y perfilación de usuarios.
  - » Sistemas de acceso remoto
  - » Virtualización de servicios informáticos.

- Implementa políticas y procedimientos constantes de mantenimiento y actualización de licencias y de infraestructura (nuevas versiones, actualizaciones, parches sean o no de seguridad, entre otros) en aspectos como:
  - » Sistemas operativos de red, de bases de datos, de servidores y estaciones de trabajo y computadores personales.
  - » Software comercial o software que sea de propiedad intelectual interna de la compañía.
  - » Herramientas de automatización (procesos y tareas).
  - » Archivos digitales.
  - » Software e infraestructura de telecomunicaciones y redes de datos.

RIESGO: Cuidar aspectos financieros y económicos.

DESCRIPCIÓN:
Momentos coyunturales como pandemias, crisis ambiental, orden público, entre otros, pueden derivar en otros tipos de crisis como la financiera y económica. En estos momentos, también debemos actuar en consecuencia y tomar medidas que mitiguen los efectos al interior y al exterior de las compañías (por ejemplo, con nuestros aliados, proveedores y clientes).

RECOMENDACIONES:

- En momentos de crisis económica, algunas variables macro y microeconómicas pueden presentar alta variabilidad (como la TRM). Si tenemos en cuenta que buena parte del acceso a la tecnología depende de esta variable, es pertinente hacerse cargo de ella. Algunas recomendaciones para esto son:
  - » Si la TRM es favorable para los intereses de tu compañía, trata de aprovechar esta situación adelantando las inversiones y los gastos en moneda extranjera de tecnología que tengan previstas.
  - » Si la TRM es desfavorable para los intereses de tu compañía, mitiga los efectos tomando acciones como:
    * Aplaza al máximo la compra o inversión en equipos y licencias mientras se controla la crisis.
    * Difiere y amortiza las inversiones en activos y pasivos.
    * Utiliza los mecanismos financieros que sean pertinentes para mitigar las fluctuaciones de la TRM para controlar el efecto de la alta variabilidad.
    * Asigna los recursos y las inversiones en lo que sea prioritario para los intereses de la compañía buscando sostenibilidad y, en casos extremos, supervivencia.
    * Negocia con los proveedores y aliados nuevas formas de pago que sean de beneficio para ambas partes de cara la sostenibilidad.