MOORE

SEGURIDAD DE LA INFORMACIÓN

Webinar Moore Colombia – Cyte Colombia
Abril 2020 | V1.0

CONTENIDO

PANELISTAS

Conoce más sobre la experiencia de nuestros expertos.

Adriana Piñango
Gerente de Consultoría Empresarial y TI

MOORE COLOMBIA

Ingeniera de Sistemas
CISA – ITIL 4

Cuenta con más de 10 años de experiencia profesional enfocada en el diseño, ejecución y gestión de proyectos de auditoría de Tecnología de la Información bajo estándares NIA y PCAOB, y aseguramiento razonable bajo estándares ISAE3000 / ISAE3402. Ha desarrollado proyectos de consultoría para la mejora de procesos de negocio, tecnología, control interno de TI, cumplimiento regulatorio, gestión integral de riesgos, seguridad de la información e implementación SOX.

Los proyectos desarrollados le dan amplio conocimientos en diversos sectores económicos como financiero, educativo, alimentos y bebidas, farmacéutico, oil and gas, salud, retail, entre otros.

Cuenta con alta experiencia en sistemas de información complejos como SAP ECC - S/4HANA, Oracle, Dynamics y herramientas de administración de usuarios para la gestión de riesgos a nivel de accesos y segregación de funciones.

CYTE COLOMBIA

Ingeniero de Sistemas
Magister en ingeniería de sistemas y computación y Master of Science

Director del centro MOX de computación avanzada y Director de la especialización en seguridad de la información de la Universidad de los Andes.

Criptógrafo por formación. Experto en seguridad de la información con experiencia en aseguramiento de procesos y reingeniería de procesos con tecnologías
innovadoras.

Especialista en el desarrollo de servicios de seguridad y soluciones de acuerdo a las necesidad de las compañías y el mercado Colombia donde se encuentran importantes empresas del sector financiero, oil & gas, energía, entre otros.

Milton Quiroga
Socio fundador CYTE Colombia

Webinar

SEGURIDAD DE LA INFORMACIÓN

23 ABRIL 2020

- ✓ Ciberseguridad.
- ✓ Riesgo Operacional.
- ✓ Infraestructura crítica.
- ✓ Contingencia Tecnológica a causa del COVID-19

Hablando de Seguridad de la Información y la importancia de comprender la diferencia entre lo que si es y lo que no es.

Así mismo hablamos sobre la Ciberseguridad e identificar los detalles en la relación que establece con la gestión del riesgo operacional y sus derivados.

Por otro lado, no podemos olvidar la dependencia con la gestión de la infraestructura crítica y como todos estos elementos se conjugan para apoyar a nuestras organizaciones frente a las contingencias predecibles y no predecibles.

¡Consigue la Presentación completa!

LEER MÁS

NUESTRAS RECOMENDACIONES

- ✓ **El origen de un ciberataque no siempre es específico ni delimitado a las características que conocemos, el cibercrimen evoluciona constantemente..** como consecuencia de los “silos” organizacionales y la no-coordinación de esfuerzos, se tiende a implementar soluciones de continuidad como centros alternos sin cuidar los análisis de infosec; lo que nos duplica la exposición a vulnerabilidades. Por no considerar de manera coordinada los aspectos de riesgo operacional, un control para resolver un riesgo de disponibilidad, incrementa los riesgos de confidencialidad / integridad. Todo esto se resuelve abordando de manera integrada los aspectos de riesgo operacional, y dejando a un lado la obediencia ciega a los códigos de práctica que con frecuencia son dañinos.

- ✓ **Los elementos caóticos del mundo que habitamos no pueden controlarnos y dejarnos desprotegidos en la gestión de riesgos..** la tendencia nos lleva a concluir que el origen de las amenazas infosec es normalmente humano, y típicamente el modelamiento de amenazas de ciberseguridad tiene que pasar por modelar comportamientos caóticos, pero esto no debe condicionarnos, la clave está en conocer nuestra organización y los riesgos que se desprenden de la misma, desde su concepción estándar de mercado, pasando por los tipos de sistemas de información que usa y las particularidades de la operación.
  Desde este conocimiento es menos complejo identificar la metodología de gestión de riesgos que nos funciona, siempre que garantice “completitud” y “repetibilidad” en la identificación de amenazas. Como ejemplo, hemos usado con bastante éxito la metodología Octave® del Computer Emergency Response Team.

- ✓ **El resultado del análisis de riesgos deberá generar la visual de las posibles vulnerabilidades a las que estamos expuestos en nuestra organización para tratarlas..** y claro que existen metodologías y herramientas, sin embargo, no podemos verlos como elementos independientes, debemos alinearlos de manera que la estrategia de gestión de riesgos alcance el análisis, tratamiento y monitoreo de las vulnerabilidades, y también nos permita mantener la guardia alta frente a nuevos vectores de ataque. Cuando se desarrollan análisis de vulnerabilidades es recomendable el uso combinado de herramientas y el análisis de lo que sucede en el exterior de nuestra organización, para potenciar la capacidad de identificar los eventos de riesgo.

NUESTRAS RECOMENDACIONES

- ✓ **Es vital mantener el foco en la estrategia de la organización, aunque aún identifiquemos silos, no podemos estar desconectados del sentido de existencia (misión / visión)..** la seguridad de la información es un bien común, y las estrategias que se diseñan para gestionarla desde los equipos responsables, no pueden perder de vista la razón de ser de la organización; de otro modo tendríamos que reconsiderar si es acertado el nivel de relevancia que se le da a los activos de TI y en consecuencia, si los riesgos están bien identificados y mitigados por los controles que se establecieron. La contingencia que atravesamos hoy, entre otras cosas, ha demostrado la importancia de los procesos de TI y su conexión con la esencia de la organización.

- ✓ **No podemos perder de vista la seguridad sobre los activos de TI, si nuestras condiciones cambiaron, entonces deben adaptarse nuestros controles..** la base esta en gestionar nuestras políticas y procedimientos, someterlas a las actualizaciones necesarias, y lo más importante, comunicarlas a los funcionarios de la organización de forma clara y objetiva. Uno de los factores de éxito fundamentales en una contingencia es el conocimiento de las personas sobre las actividades que deben desempeñar y de las cuales son responsables. Mantener la operación no significa hacerlo a cualquier precio, por el contrario se refiere a continuar operando con las normas adecuadas y sin tomar riesgos. Algunas actividades pueden ser capacitaciones, comunicaciones con tips relevantes, evaluaciones y campañas de sensibilización al riesgo.

- ✓ **En la actualidad el esquema de ciberseguridad está en una medición constante de eficacia, y en esa línea debemos orientar nuestras estrategias de continuidad, el análisis de riesgos y las soluciones que implementamos..** pero recordemos que no somos elementos aislados, vale la pena conocer qué pasa en Colombia, en la región y en el mundo, en organizaciones como las nuestras, y documentarnos desde fuentes confiables. Algunos puntos de consulta:
  - ✓ http://www.colcert.gov.co/
  - ✓ https://cve.mitre.org/
  - ✓ https://www.us-cert.gov/ncas/alerts/2020

NUESTRAS RECOMENDACIONES

- ✓ **No podemos dejar de comunicarnos, pero si podemos hacer de forma segura..** desde una mirada razonable, no es posible hablar de la seguridad absoluta de una herramienta o sistema de información. Las herramientas de video conferencia son diseñadas para cubrir una necesidad del mercado e incorporan esquemas de seguridad propios, pero también debemos considerar el impacto de factores externos como la configuración segura de la red, la seguridad del navegador desde el cuál se accede a la herramienta y hasta la configuración de seguridad en redes desde el sistema operativo.

  Algunas recomendaciones en la utilización segura de herramientas de videoconferencias son:

  - Utilizar herramientas aprobadas por el área de Tecnología de la compañía
  - Considerar el alcance del soporte que ofrece el proveedor
  - Capacitar al personal en el uso adecuado de las herramientas y los riesgos asociados a dicha tecnología
  - Gestionar las actualizaciones de seguridad
  - Gestionar la seguridad en los entornos de conexión, dentro y fuera de las compañías

REFERENCIAS

Bibliografía:

- A Leader's Guide to Cybersecurity - why boards need to lead and how to do it. Thomas J. Parenty | Jack J. Domet. Harvard Business Review Press. 2019. ISBN-13: 978-1633697997. https://www.amazon.com/Leaders-Guide-Cybersecurity-Boards-Lead/dp/1633697991/ref=tmm_hrd_swatch_0?_encoding=UTF8&qid=&sr=

- Blockchain Revolution - how the technology behind bitcoin and other cryptocurrencies is changing the world. Don Tapscott - Alex Tapscott. 2018. ISBN-13: 978-1101980149. https://www.amazon.com/Blockchain-Revolution-Technology-Cryptocurrencies-Changing/dp/1101980141/ref=tmm_pap_swatch_0?_encoding=UTF8&qid=1587681498&sr=8-3

- Blockchain: The Insights You Need from Harvard Business Review. Catherine Tucker, Don Tapscott, Marco Iansiti, Karim R. Lakhani. Harvard Business Review Press. 2019. https://store.hbr.org/product/blockchain-the-insights-you-need-from-harvard-business-review/10282

- Wicked Problems - Jay Rosen - https://edge.org/response-detail/11091

- The World is Unpredictable - Rudy Rucker – https://edge.org/response-detail/10171

Ciberseguridad y Riesgo Operacional

Uno de los términos más incomprendidos en nuestro medio es quizás la palabra "ciberseguridad". Aún cuando es término referido con frecuencia en Juntas Directivas y circulares del gobierno, en realidad el encargado de estos temas se encuentra con frecuencia sin guías de como abordar su responsabilidad. En esta nota se presenta desde el punto de vista de **riesgo operacional** una posible metodología de trabajo de los aspectos de ciberseguridad en una organización.

cyte
we know-how®

LO DIFUSO DEL TÉRMINO CIBERSEGURIDAD

Por M. Quiroga

En efecto, al parecer, comprar un *firewall*, actualizar el antivirus o contratar hacking ético, cualquier cosa pareciera ser relevante para mostrar gestión en ciberseguridad. En el imaginario colectivo de ciberseguridad en muchas organizaciones aparece desde un atacante solitario en *hoodie* como el de la figura de arriba, hasta un *"terminator"* desplazándose por la carrera séptima disparando a todo lo que se mueva.

En realidad imaginar los escenarios de ciberguerra no re- quiere un esfuerzo tan grande de imaginación y en cambio puede llevar a riesgos y amenazas reales. Basta simplemente con recordar algunas operaciones bélicas en la historia y tratar de imaginar este tipo de operaciones en contextos "ciber".

Operaciones Bélicas

En la Segunda Guerra Mundial el gobierno Alemán con- dujo una audaz operación bélica, conocida como la operación "Bernhard". Para el momento de concebir esta operación, la aviación alemana rutinariamente bombardeaba Londres, sin que el pueblo inglés diera muestras de rendirse. El alto mando ideó una operación capaz de detener la economía inglesa y sin disparar una bala más.. . la operación consistía en inundar las calles londinenses con miles y miles de billetes de y libras esterlinas ¡falsos!

Hitler confiaba en que lo que no conseguía con las bombas, lo iba a conseguir con billetes falsos. . .

Clausewitz decía que "la guerra es un acto de poder para doblegar el enemigo".. . ¿qué más da si no son bombas sino presiones inflacionarias que lleven a la destrucción económica del enemigo? Sun Tzu en "El Arte de la Guerra" escribió: "cien victorias en cien batallas no es lo ideal. Lo ideal es someter al enemigo sin luchar".

Hay otro caso emblemático que es premonitorio de la ciberguerra. . . este caso sucedió en 1982 y se conoció como "la explosión del gasoducto Urengoy–Surgut–Chelyabinsk". Al parecer en estos tiempos de la guerra fría, la antigua Unión Soviética era particularmente habilidosa espiando y robando tecnología de occidente. Narra Thomas C. Reed que la CIA procedió a realizar una operación encubierta en la cual escondió una *bomba lógica* en el software SCADA de control de oleoductos de la compañía Canadiense Telvent®, que luego la KGB soviética hábilmente robó.

Esta *bomba lógica* causó que un tiempo después el oleoducto en mención explotara con una violencia equivalente a 3 kilotones.

En ambos casos aquí mencionados, se trató de actos bélicos, que sin embargo no fueron actos militares en el sentido tradicional. Es decir se trató de ataques contra infraestructura del adversario y que sin embargo no involucraron balas o bombas. . . Esos son precisamente los escenarios más frecuentes de ciberguerra, ataques "a través de bits" que persiguen un fin político. Es decir, si se dice que la guerra es una extensión de la política, la ciberguerra es simplemente un nuevo ámbito de la guerra

La ciberguerra busca producir una parálisis estratégica del aparato productivo del enemigo. Las armas de ciberguerra son simplemente armas de interrupción masiva.

El resto de la historia reciente de ciberguerra no es pertinente profundizar más en este espacio: una secuencia temporal que quizás inicia con ciberarmas como Stuxnet (2010), Havex (2013), BlackEnergy (2015), CrashOverride (2016), Triton – Trisis (¿2018? ¿2019?). . .

Solo resta resaltar un fenómeno curioso y poco comprendido. Las armas de ciberguerra pasan a la delincuencia común muy rápidamente. Por ejemplo, la tecnología de Stuxnet (https://en.wikipedia.org/wiki/Stuxnet) una ciberarma empleada contra Irán, a los pocos meses pasó a delincuencia común, encarnada en malware como Duqu y Flame

Sin embargo, es importante precisar que no es razonable suponer que las hostilidades a que estamos expuestos son escenarios "ciber" puros. Es claro que un escenario serio de ataque incluye actos no necesariamente "ciber": históricamente una bala y un asesinato selectivo siempre ha sido un recurso bastante socorrido de efectividad comprobada (CNET)

Es decir, el modelamiento de amenazas de escenarios "ciber", en realidad se trata de un espectro continuo de amenazas que debe incorporar adversarios como gobiernos extranjeros, empleados desleales, competencia deshonesta y espionaje industrial, delincuencia común, delincuencia organizada y también por supuesto seguridad física.

Resiliencia Operacional y Riesgo Operacional

Los acuerdos de Basilea definen un lenguaje común de gestión de riesgos para el sector financiero, que sin embargo puede ser adecuadamente extendido para cualquier organización.

Estos acuerdos de Basilea definen el riesgo operacional como el riesgo resultado de procesos de negocio internos fallidos o inadecuados, o de personas o de tecnología o de eventos externos.

Estos conceptos son particularmente de interés, toda vez que se trata de un marco de trabajo ampliamente conocido en varios sectores económicos (hasta la misma Superintendencia Financiera tiene una circular de "Riesgo Operacional") y por lo tanto se trata de términos compartidos, toda vez que ciertamente las amenazas de ciberseguridad están estrechamente vinculadas al riesgo operacional.

Es decir, una hipótesis de trabajo propuesta en este texto se formula así: **una organización es "resiliente" en ciber- seguridad si es "resiliente" ante eventos de riesgo operacional.**

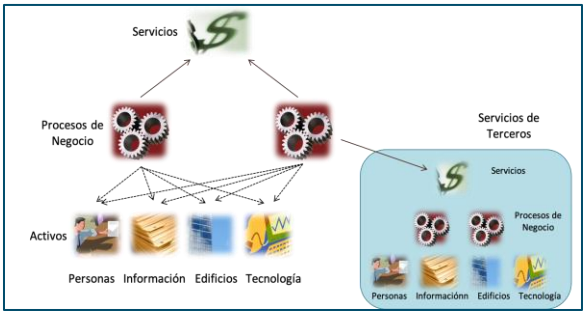
Resiliencia y Riesgo Operacional

Conceptualmente una organización está formada por una jerarquía de Servicios, Procesos de Negocio y Activos, similar a la mostrada a continuación en la siguiente figura.

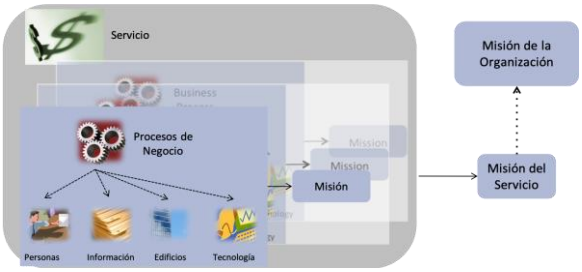
En ella podemos ver los Servicios de la organización, es decir aquel conjunto de actividades que realiza una organización para fabricar un producto o ofrecer un servicio a un cliente. Estos Servicios son elaborados en una serie de Procesos de Negocio, que a su vez se apoyan en un conjunto de Activos para su operación.

Estos Activos pueden ser -en general- de tres tipos: activos de tipo Personas que tienen que ver con la gente a cargo de operar el proceso de negocio, los activos de tipo Información que tienen que ver con los datos y conocimiento que le permiten a la organización operar el proceso, los activos de tipo Edificios que tienen que ver con oficinas, bodegas y plantas de fabricación donde reside el proceso y finalmente los activos de tipo Tecnología que tienen que ver con el software, hardware, sistemas SCADA y equipos de automatización y en general la tecnología en la que se basa el proceso para operar.

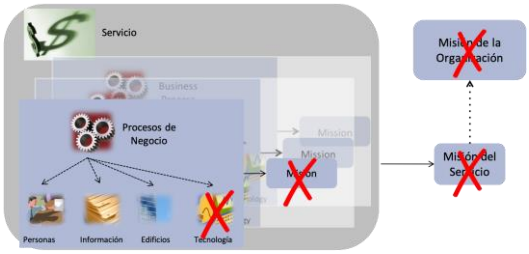
Con frecuencia y -cada vez más- las organizaciones se basan en terceros para operar sus Procesos de Negocio. Estos terceros resultan vitales hoy en día, ya que le permiten a las organizaciones concentrarse en sus competencias más importantes y dejar aquellas actividades no-vitales a terceros expertos. Por supuesto, también los terceros tienen la jerarquía de Servicios, Procesos de Negocio y Activos que tipifican en general una organización, como se muestra a continuación en la figura de abajo.



Así cada **Servicio** que ofrece una organización está basado en una serie de **Procesos de Negocio**, con su propia "**misión**". Cuando se unen estos servicios individuales obtenemos colectivamente la Misión de la organización, como se muestra a continuación en la siguiente figura.

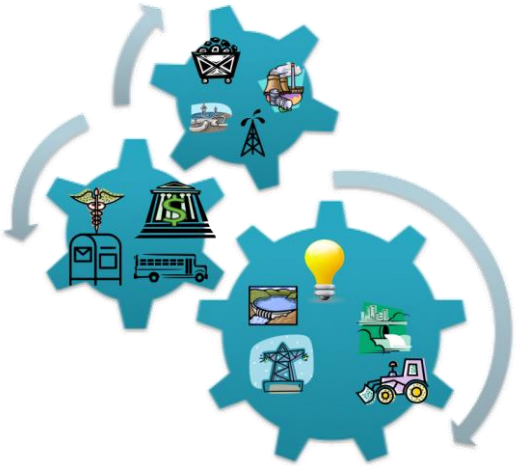


Ahora bien, si un **Activo** sensible de la organización, digamos un activo de tipo **Tecnología** falla, los **Procesos de Negocio** que apoya fallarán en consecuencia y por lo tanto es posible que algún(os) Servicio(s) fallen también, desencadenando incluso, lo que podría constituir una falla completa de la empresa para cumplir su **Misión** organizacional, como se muestra a continuación en la figura de abajo.



Es decir, **la gestión de ciberseguridad de una organización tiene que ver con preservar la misión organizacional, mediante la gestión de la resiliencia de los activos de soporte de los procesos de negocio, aún ante escenarios adversos de amenazas de gobiernos extranjeros, empleados desleales, competencia deshonesta y espionaje industrial, delincuencia común, delincuencia organizada y seguridad física.**

Si consideramos nuestro país y todo su aparato productivo como un gran mecanismo de relojería, podemos imaginar cómo los servicios que ofrece una organización son incorporados en los procesos de negocio de otra organización y de otra en otra y así sucesivamente todos los sectores de la economía están íntimamente conectados de manera que resultan ser codependientes entre sí.



Y en este gran concierto de servicios, procesos de negocio y activos. . .
. . . una falla en un activo en un proceso de negocio, en un servicio crítico de la organización **X**. . .
. . . una falla orquestada por un adversario como un gobierno extranjero, un empleado desleal, un competidor deshonesto o delincuencia común / organizada. . .
. . . puede hacer que la organización **X** no pueda cumplir su misión y además desencadenar una serie de fallas en toda la economía que incluso pueda afectar nuestra viabilidad como sociedad civilizada.

Este tipo de organizaciones que ofrecen servicios de los que dependemos vitalmente como sociedad son conocidas como infraestructura crítica y en cualquier escenario de ciberseguridad es muy importante tenerlas presente, toda vez que este tipo de organizaciones deben incorporar en sus operaciones todo el modelamiento de amenazas y análisis de riesgos que les permitan ser resilientes ante escenarios de ciberguerra.

En general los gobiernos han hecho algunos trabajos de identificación de **infraestructura crítica** y hay algunos trabajos de mesas sectoriales que han sido bastante claros identificando el "**qué**"... Sin embargo, en muchas ocasiones, tener claro el "**qué**", no necesariamente lleva al "**cómo**".

Precisamente el "**cómo**" se puede encontrar en el modelo de gestión de resiliencia del *Software Engineering Institute de Carnegie Mellon University*.

Modelo Gestión de Resiliencia (CERT-RMM)

El Modelo de Gestión de Resiliencia (CERT-RMM) define un esquema de mejora continua de procesos que le permite a una organización conseguir Resiliencia Operacional (i.e. Resiliencia ante eventos relacionados con Riesgo Operacional).

Este modelo incluye un conjunto específico de actividades diferentes, agrupadas en torno a 26 grupos (conocidos como *Process Areas*), junto con un mecanismo de medida y auto-evaluación basado en los modelos de *madurez / capacidades* que han sido tan transformadores para muchas industrias, especialmente la industria del software.

En estos 26 grupos de proceso aparecen por ejemplo, actividades relacionadas con:

- Gestión de Riesgos,
- Gestión de Continuidad,
- Gestión de incidentes,
- Gestión de Activos,
- Gestión de logs, monitoreo y mediciones,
- Seguridad en el ciclo de vida del software,
- Gestión de terceros,
- Gestión de identidades,
- Gestión de acceso,
- Gestión de vulnerabilidades.

Junto con una serie de automedidas para mejora continua en términos de niveles de capacidad (Nivel 0 - Realizado, Nivel 1 - Administrado, Nivel 3 - Definido), que buscan que la organización sea capaz de operar de una manera predecible, aún en momentos de stress como los causados por eventos de ciberseguridad.

Sin embargo, el beneficio más importante del modelo CERTRMM consiste en que define una serie de actividades completas que incorporan todos los aspectos de riesgo operacional y ciberseguridad de una organización, junto con un mecanismo claro de **medición** de esfuerzos, que le permiten a la Alta Gerencia responder con certeza las siguientes preguntas:

- ¿Cuál es el estado actual de preparación de la organización en temas de ciberseguridad?
- ¿Qué tan efectivo ha sido el dinero que se ha empleado en la preparación de ciberseguridad?
- ¿Es la organización capaz de operar de manera predecible ante un evento de ciberseguridad?
- ¿Qué planes de mejora son los más adecuados para la organización a corto, mediano y largo plazo y por qué?
- ¿Cómo puedo incorporar la estrategia de ciberseguridad en mis planes de mejoramiento continuo de procesos?
- Si mi rol es vigilar los esfuerzos de ciberseguridad de un grupo de organizaciones, ¿Cómo puedo definir un mecanismo de evaluación y medición simple y objetivo y que además le entregue valor a las organizaciones vigiladas?

PARA MÁS INFORMACIÓN:

Consúltenos en info@cyte.co acerca de las preguntas que pueda tener acerca del uso de estas metodologías para mejora
de sus procesos de negocios.

www.cyte.co

+57 (1) 745-0272

Calle 24 No. 7-43 Of. 704. Edificio Siete 24.

Linked.in/miltonq

cyte
we know-how®

TIPS DE CIBERSEGURIDAD PARA TRABAJAR DE FORMA SEGURA DESDE CASA

RECOMENDACIONES DE ARMANINO LLP – FIRMA MOORE

La propagación de COVID-19 ha cambiado el proceso de TI para muchas organizaciones, siendo los empleados trabajando desde casa, a una escala mucho mayor que nunca, el cambio principal. Pasar de trabajar en un entorno de TI confiable de una organización a trabajar de forma remota a través de redes domésticas o públicas puede crear riesgos de seguridad que antes no se tenían en cuenta.

Los ataques de phishing y malware que utilizan COVID-19 como asunto y en el contenido han aumentado significativamente. Los atacantes aprovechan al máximo el miedo y el interés público que rodean esta pandemia. Estas personas nefastas están utilizando diversas tácticas para comprometer las credenciales de los usuarios, la información de pago y otros datos que pueden monetizarse.

A continuación, compartimos algunos consejos para ayudar a los usuarios a mantenerse seguros cuando se conectan en línea desde sus casas:

- Asegúrese de que la conexión Wi-Fi de su hogar sea segura utilizando el cifrado WPA2, el cual se recomienda para las redes domésticas. Si bien la mayoría de las redes Wi-Fi están protegidas correctamente con WPA2, es posible que algunas instalaciones o equipos más antiguos no lo estén, es decir, que usen encriptación WEP, lo que permite que alguien con herramientas básicas de piratería acceda a su red.

- Tenga cuidado al abrir y hacer clic en enlaces a correos electrónicos sobre COVID-19. Puede pasar el mouse sobre los hipervínculos en los correos electrónicos para verificar que van al sitio previsto.

Si no está seguro del remitente, trate esto como un intento de phishing. Notifique a su servicio de asistencia de TI de inmediato.

- Si accede a los datos confidenciales de la empresa de forma remota a través del almacenamiento en la nube (por ejemplo, Dropbox, BOX o One Drive), asegúrese de seguir el procedimiento de su empresa para acceder a los datos.

- Asegúrese de seguir la estrategia de respaldo de su organización guardando archivos importantes en ubicaciones cubiertas por su política de respaldo de TI. Los archivos importantes deben ser respaldados constantemente. En el peor de los casos, si se convierte en víctima de ransomware, sus datos se pueden recuperar del almacenamiento de respaldo.

- Asegúrese de utilizar una conexión segura a su entorno de trabajo a través de una red privada virtual (VPN). Una VPN proporciona mayor seguridad al encriptar la línea de comunicación entre su dispositivo y su red de trabajo.

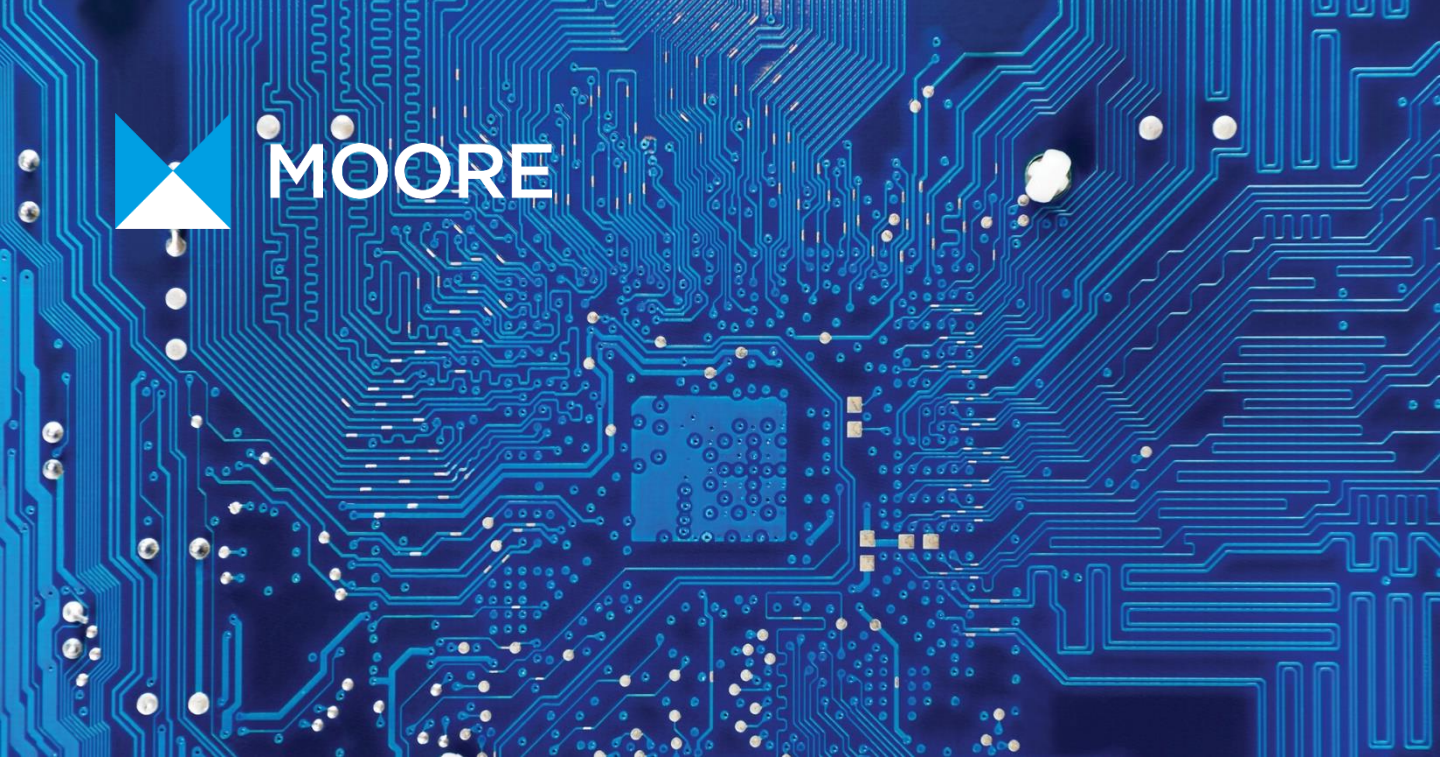
- Verifique si tiene instaladas herramientas de cifrado. El cifrado ayuda a evitar el acceso no autorizado a los datos en los dispositivos. Los datos se codifican de una manera que dificulta que las personas no autorizadas puedan descifrarlos. Esto puede ser especialmente importante en caso de pérdida o robo del dispositivo, ya que ayuda a evitar que extraños accedan a sus datos sin la clave de cifrado.

- Utilice una contraseña de fuerte protección y autenticación. Las contraseñas seguras contienen al menos ocho caracteres e incluyen números, símbolos y letras mayúsculas y minúsculas. Cambiar las contraseñas regularmente también es importante.

- Si su empresa ofrece el uso de autenticación multifactor (MFA), aproveche esta tecnología, ya que le otorga una capa adicional de protección a su información.

Desafortunadamente, la seguridad del usuario remoto desde el hogar no se reduce solo con seguir un conjunto de pautas. Las protecciones pueden variar de una situación a otra, y usar su mejor juicio y criterio se vuelve crucial. Al ser más consciente de dónde y cuándo acceder a los datos de la compañía, y cómo hacerlo de manera segura, puede ayudar a garantizar que la información confidencial de la compañía esté siempre protegida.

Este artículo fue escrito por Armanino LLP, una firma independiente asociada con Moore Global Network. © 2020. Todos los derechos reservados. Usado con permiso.



¡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 apoyo 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.

Para más información visite:
www.moore-colombia.co

Síganos en redes sociales:
@Moore_Colombia

CONTACTOS

Si quieren saber mas sobre nuestras soluciones, herramientas y acompañamiento que podemos aportar a su empresa, no duden en contactarnos.

MOORE

ADRIANA PIÑANGO LATUFF
apinango@moore-colombia.co

PAOLA SERRANO ROMERO
gestioncomercial@moore-colombia.co

cyte
we know-how®

MILTON QUIROGA
mquiroga@cyte.co

ALFRED ESCOBEDO
aescobedo@cyte.co


MOORE