

MARSH INSIGHTS

COVID-19: Ciberseguridad y resiliencia

COVID 19, una amenaza con multitud de facetas: 5 letras y 2 números, estos son los caracteres que están afectando a nuestras vidas.

Todos estamos a título personal y a nivel empresarial, haciendo frente a nuevos retos ante una realidad nunca antes vivida.

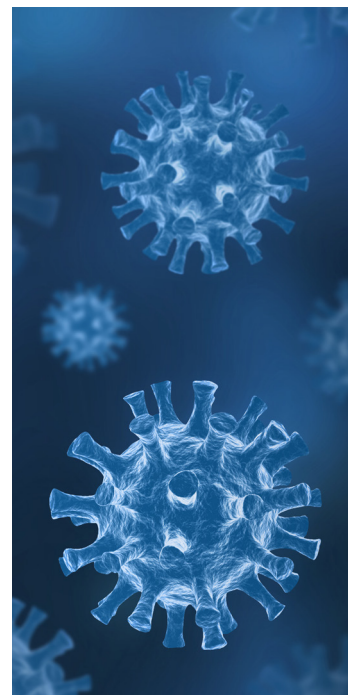
La interrupción de la actividad, el reenfoque de prioridades o el masivo teletrabajo han supuesto grandes riesgos operacionales para las organizaciones, que ha puesto a prueba los planes de contingencia y continuidad de los negocios en estas semanas de crisis y confinamiento. Ahora conviene encontrar un momento para detenerse y analizar esta situación desde una perspectiva estratégica para robustecer la resiliencia de la empresa en el corto, medio y largo plazo.

PRIMER RETO

La interrupción o adaptación de las principales actividades del negocio

Algunas organizaciones están afrontando una reducción de su actividad, otras un sobredimensionamiento de la demanda de sus productos o servicios y, finalmente, otras han podido adaptarse a la situación y realizar nuevas y distintas tareas productivas (por ejemplo, iniciando la fabricación de gel desinfectante, material sanitario, etc.) siendo especialmente relevantes – desde una perspectiva de ciberseguridad – el aumento de la actividad en el comercio online, tráfico en las redes e interconectividad.

La forma abrupta en la que ha habido que abordar esta situación ha provocado, en muchos casos, que las organizaciones se hayan centrado menos en supervisar la ciberseguridad. Los departamentos de IT están en una situación delicada; su trabajo está sometido a una presión adicional al tener que garantizar que el negocio pueda seguir desarrollándose en remoto, a la vez que velar por la seguridad de los sistemas de información y los accesos y procesos en remoto. Los cibercriminales son muy conscientes de esta situación, y están centrando sus esfuerzos en aprovechar esas vulnerabilidades



DESDE MARSH, COMO LÍDER GLOBAL EN CONSULTORÍA DE RIESGOS Y SEGUROS, LE PODEMOS AYUDAR.

PONEMOS A SU DISPOSICIÓN NUESTRO RECONOCIDO EQUIPO DE PROFESIONALES EXPERTOS EN LA RESILIENCIA DEL NEGOCIO Y MEDIACIÓN DE SEGUROS PARA RIESGOS CIBERNÉTICOS.

y atacar a aquellas empresas u organizaciones gubernamentales, cuya actividad se está viendo afectada, para lanzar ciberataques con motivaciones principalmente económicas, pero también políticas.

SEGUNDO RETO La superficie de ataque

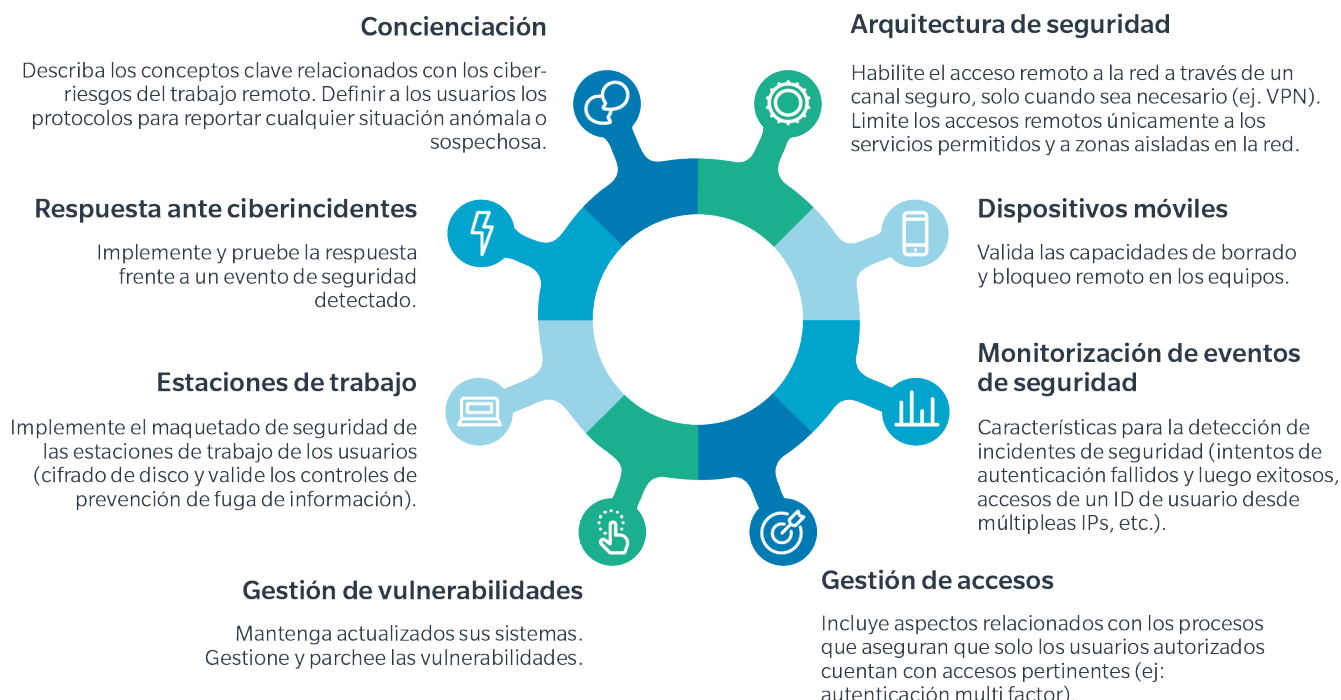
Con motivo de las campañas “Quédate en casa” y de distanciamiento social que se han puesto en marcha para reducir los efectos del COVID-19, muchos profesionales tienen que trabajar desde sus domicilios, lo que da lugar a varias situaciones:

- Por un lado, las infraestructuras IT están a pleno rendimiento para poder sostener la continuidad del negocio. Las organizaciones tienen que tener en cuenta los riesgos asociados a la ciberseguridad que ello conlleva, pero también si sus infraestructuras IT son lo suficientemente robustas como para soportar la carga de trabajo que desean tener.

- El teletrabajo incrementa el riesgo de cumplimiento normativo relativo a las políticas y procedimientos de privacidad (por ejemplo, con el uso de dispositivos personales que almacenan información confidencial sin ser encriptados, etc.). Como consecuencia, la información confidencial o de carácter personal protegida que trata una empresa quedan expuestas ante posibles vulneraciones de privacidad o accesos no autorizados a los sistemas.

A todos nos preocupa en estos momentos el incierto futuro al que nos enfrentamos, y los comités de gestión de crisis COVID-19, que trabajan en proteger y mantener la actividad de la empresa, deben de considerar los riesgos cibernéticos junto al resto de riesgos operaciones y de gobierno corporativo que están en juego.

Consejos en materia de ciberseguridad en el teletrabajo para atravesar la crisis del COVID 19



¿Dispongo de un Seguro Cyber? ¿Qué ocurre con mi próxima renovación?

El mercado asegurador está prestando gran atención a factores adicionales de riesgo que están aflorando en esta crisis, y las compañías de seguros serán cada vez más minuciosas en su análisis y a la hora de revisar la resiliencia de sus clientes, preguntando por las medidas adoptadas ante un generalizado teletrabajo y las políticas o nuevas realidades de uso de dispositivos personales (“bring your own device”, por sus siglas en inglés BYOD). Las aseguradoras están revisando sus cuestionarios y proponiendo reuniones telemáticas antes de la contratación de seguros Cyber o de su renovación con preguntas dirigidas a ampliar información sobre los accesos remotos, VPNs, seguridad, o el uso de autenticación multifactor.

En estos momentos disponer de un buen seguro de Cyber resulta crítico, pues su cobertura actuará ante una brecha de seguridad como una última barrera de defensa que protegerá la cuenta de resultados y los activos de la empresa.

LOS SEGUROS DE CYBER RESPONDEN PRINCIPALMENTE ANTE:

- la paralización de actividad que se puede derivar por ejemplo de un “ransomware” o ataque de denegación de servicio; o
- Las actuaciones regulatorias a las que una empresa puede tener que enfrentarse debido a una vulneración de privacidad en materia de datos de carácter personal; o
- las reclamaciones de responsabilidad civil por incidentes de seguridad o privacidad que afectan a clientes; y
- adicionalmente cubre los costes extras de tener que acudir a profesionales externos, facilitando el acceso inmediato a empresas cualificadas para la inmediata respuesta ante la crisis con ayuda forense, legal, de IT y comunicación especializada, todo ello a cargo de la aseguradora.

Pero el seguro Cyber, siendo fundamental, es un instrumento clave de protección ante incidentes de seguridad que estratégicamente una empresa siempre querrá evitar o minimizar trabajando en su resiliencia.

Protejamos lo que nos mantiene resilientes en el actual entorno de teletrabajo generalizado.

Le recomendamos mantener una actitud proactiva con un claro enfoque en las siguientes prioridades:

TECNOLOGÍA

- **Validación del entorno de teletrabajo**
Verifique en contraste con su normativo de referencia los riesgos de ciberseguridad en el teletrabajo, y sino dispone de él priorice su elaboración.
- **Testeo de la ciberseguridad**
Realice un análisis técnico para verificar tanto los controles de ciberseguridad establecidos como la capacidad de ciberresiliencia, acudiendo a profesionales externos en busca de apoyo profesional independiente y cualificado.

PERSONAS

- **Concienciación considerando el cambio de entorno (de la oficina al hogar)**
Lleve a cabo iniciativas de formación para preparar a sus empleados frente a ataques de ingeniería social (phishing, vishing, etc.), validando su grado de concienciación, valorando el apoyo de especialistas para la mayor efectividad en esta crítica misión de concienciación del empleado, como eslabón de protección más débil ante este riesgo.

FINANZAS

Las organizaciones deben de poder priorizar el análisis de los riesgos cibernéticos que afectan a su organización (incluyéndolos su mapa de riesgos, cuantificación de escenarios, valorando su probabilidad e impacto para tener claridad acerca de la validez de su cobertura). En esta labor, resulta recomendable buscar apoyo en firmas de consultoría de riesgos especializadas, que combinen en su propuesta de valor capacidades en el área de mediación de seguros junto a especialistas en ciberseguridad y resiliencia. El trabajo con sus consultores de riesgos y seguros no debe de quedar en el análisis del riesgo y la búsqueda de una óptima solución aseguradora, pues donde su apoyo puede resultar igualmente crítico es en la gestión del propio incidente para la mejor defensa de sus intereses en la notificación y gestión del siniestro ante las aseguradoras.

CONTRATACIÓN DE PÓLIZAS Y PREPARACIÓN DE LA RENOVACIÓN

En las actuales circunstancias es aconsejable agilizar el proceso de compra de una cobertura de seguro Cyber, y anticipar los procesos de renovación cuando ya disponga de póliza. Le recomendamos abordar una revisión de la suma asegurada y de las condiciones técnicas de su póliza con su mediador que le apoye en un adecuado flujo de información con su aseguradora para obtener términos y condiciones optimizados en coste y coberturas.

Para más información sobre nuestros servicios en apoyo de su ciberseguridad y resiliencia ante al COVID 19, por favor no dude en contactar con nosotros:

SARA MUÑOZ RUBIO

Marsh JLT Specialty
Directora Riesgos Tecnológicos y Cibernéticos
sara.munozrubio@marsh.com

NELIA ARGAZ DURANGO

Marsh Risk Consulting
Directora de Ciberseguridad y Resiliencia del Negocio
nelia.argaz@marsh.com.

La información contenida en este documento es privada y confidencial y tiene únicamente validez a efectos informativos. Está destinada al uso exclusivo del destinatario y solo puede ser utilizada para la finalidad para la que se ha realizado. Todos los derechos de propiedad intelectual, con independencia de que estén o no registrados, de todas y cada una de las informaciones, contenidos, datos y gráficos que se incluyen en el documento pertenecen a Marsh, S.A. Mediadores de Seguros (en adelante Marsh), y el destinatario no obtendrá, ni deberá tratar de obtener, ningún derecho sobre la titularidad de dicha propiedad intelectual. Queda terminantemente prohibido que el documento se reproduzca, distribuya, publique, transforme y/o difunda, total o parcialmente, con terceras personas, físicas o jurídicas, públicas o privadas (incluidos los consultores y asesores del destinatario), sea con fines comerciales o no, a título gratuito u oneroso, sin el previo consentimiento por escrito de Marsh. Este documento se ha realizado ateniendo al propósito que figura en su objeto y está basado en la experiencia y comprensión de Marsh, no siendo válido para cualquier otro fin que no sea el especificado. Se trata de información que no ha podido ser contrastada por Marsh, y por tanto, sin que ésta sea responsable de su integridad, veracidad o exactitud, de modo que no asume responsabilidad alguna por los eventuales errores existentes en ella, ni por las discrepancias que pudieran encontrarse entre distintas versiones de la misma. Ha sido redactado en la fecha de su firma y no refleja hechos o circunstancias que ocurrieron o de los cuales Marsh se enteró con posterioridad. En consecuencia, Marsh no tiene obligación de actualizarlo. El alcance del documento se circunscribe a aspectos relativos a la materia de seguros y en su realización no se ha valorado ningún documento, ni información relacionada con otras materias, citando a título enunciativo y no limitativo las siguientes: medioambientales, financieras o contables, cuestiones actuariales, legales, tecnológicas, de ingeniería o asuntos técnicos. La ausencia de observaciones sobre cualquier asunto (o la ausencia de cualquier asunto en el documento) no debe interpretarse como un comentario u opinión implícita. El documento no pretende ser una explicación exhaustiva o análisis completo de la información proporcionada. El documento pretende ser leído en su totalidad y no en partes. Por ello, Marsh recomienda que dicho documento no sea considerado de manera aislada para la toma de decisiones relativas a la asunción de riesgos. Todas las manifestaciones en materia fiscal, contable o jurídica que pudieran incluirse en el documento, deben entenderse como observaciones generales basadas únicamente en nuestra experiencia en seguros y cobertura de riesgos y no pueden considerarse asesoramiento fiscal, contable o jurídico, el cual no estamos autorizados a prestar. Todas estas materias deben examinarse con asesores adecuadamente cualificados en el correspondiente campo. Por dicho motivo, Marsh no asumirá la responsabilidad que pueda existir, bien por el contenido de dichas observaciones generales que pudieran haberse incluido, bien por la falta de análisis de las implicaciones legales, comerciales o técnicas de los documentos e información puestos a nuestra disposición.

MARSH, S.A. MEDIADORES DE SEGUROS, Correduría de Seguros y Reaseguros (en adelante, MARSH), con domicilio social en Paseo de la Castellana, nº 216, 28046 Madrid y con N.I.F. A-81332322. Se encuentra inscrita en el Registro Mercantil de Madrid en el Tomo 10.248, Libro: 0, Folio: 160, Sección: 8, Hoja: M-163304, Inscripción: 1 y en el Registro de la Dirección General de Seguros y Fondos de Pensiones con la clave nº J-0096 (Correduría de Seguros) y la clave nº RJ-0010 (Correduría de Reaseguros). Tiene concertados los Seguros de Responsabilidad Civil y de Caución, según se establece en la normativa sobre la distribución de seguros aplicable.

Este documento es material de marketing. Copyright © 2020 Marsh - Reservados todos los derechos