Estado Actual de la Ciberseguridad 2020

Junio 2020

Con la colaboración de:

Deloitte. AECI

Con la participación de la:

OEA | Más derechos para más gente

Contenido

ESTADO ACTUAL DE LA CIBERSEGURIDAD
ECUADOR 2020

La ciberseguridad está en el Top 5 de los riesgos globales según el Foro Económico Mundial, dejando al descubierto la necesidad de que las organizaciones desde su planeación estratégica incluyan proyectos de seguridad alineados a los objetivos de la gestión estratégica del negocio.

Debido a su importancia, La Revista IT ahora, en conjunto con la Consultora Deloitte y la Asociación de Ecuatoriana de Ciberseguridad, AECI, desarrollaron el sondeo el Estado Actual de la Ciberseguridad 2020 Ecuador en el que participaron líderes de IT y Seguridad de la Información se revisan aspectos claves relacionados con la Estrategia / Gobierno, Prevención, Vigilancia y Respuesta de las empresas ecuatorianas.

Pariendo del estudio realizado por Deloitte , en 2028, denominado Tendencias de Cyber Riesgos y Seguridad de la Información en Ecuador la evolución que han tenido las empresas ecuatorianas en sus iniciativas de ciberseguridad y seguridad de la información ha tenido avances importantes.

Solamente, para presentar uno de ellos, para el 90% de empresas participantes la consideran que la ciberseguridad es un riesgo a nivel organizacional, además existe una concientización sobre la necesidad de incorporar estructuras formales de ciberseguridad. La transformación digital y las tecnologías emergentes que las organizaciones adoptan empujan una mayor demanda de servicios de ciberseguridad.

El Estado Actual de la Ciberseguridad Ecuador 2020, es una guía que presenta los niveles de madurez de la ciberseguridad, gestión de seguridad, e inversión que dará a los líderes de Seguridad de la Información y de IT, las pautas necesarias para tomar decisiones de ciberseguridad para sus organizaciones.

Roberth Chávez,
Gerente Senior de Asesoría en Riesgos - Cyber en Deloitte Ecuador

Vivimos tiempos complejos como país y a nivel mundial por la pandemia del coronavirus Covid-19, que está dejando una huella muy profunda a todo nivel.

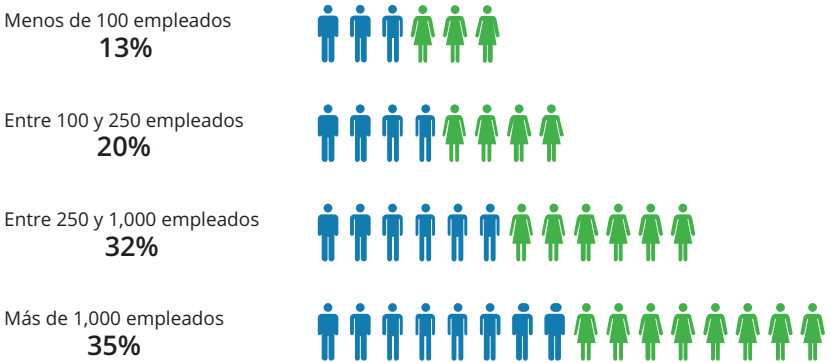
Mientras enfocamos nuestros esfuerzos en combatir esta pandemia, es importante que las organizaciones no bajen la guardia, ni descuiden el frente expuesto a ciberamenazas, ya que todo lo que vivimos actualmente, podría ser aprovechado por algún atacante con fines maliciosos para intentar obtener acceso a sus activos de información o controlar recursos tecnológicos de manera no autorizada.

Deloitte e IT Ahora, en colaboración con la Asociación Ecuatoriana de Ciberseguridad (AECI), conscientes de la situación que atraviesa la humanidad a nivel global, y preocupados por conocer cómo están nuestras contramedidas, controles o salvaguardas de ciberseguridad en la actualidad, realizaron un sondeo para medir aspectos claves con respecto a este ámbito en el territorio local.

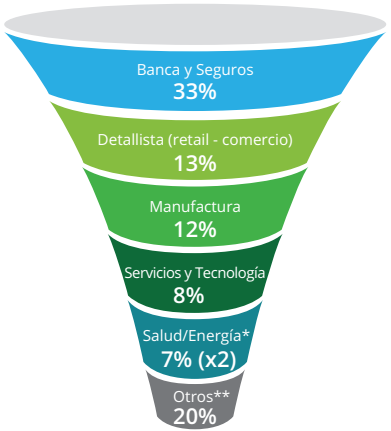
El sondeo consistió en 10 preguntas distribuidas entre las siguientes áreas:
ESTRATEGIA / GOBIERNO, PREVENCIÓN, VIGILANCIA Y RESPUESTA.

Obtuvimos respuesta de alrededor de 100 empresas entre el periodo de marzo a mayo del 2020, de diferentes industrias, sectores y tamaños por número de empleados. Presentamos los resultados finales de la encuesta.

Tamaño por número de empleados



Por industria / sector

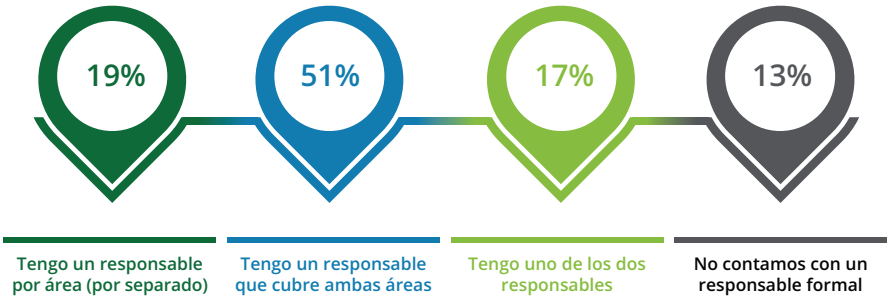


* Ambas industrias obtuvieron la misma participación.
** Se consideran: Educación, Turismo, Telecomunicación, Automotriz y Sector Público / Gobierno

ESTRATEGIA Y GOBIERNO

Uno de los principales indicadores de la madurez de la ciberseguridad en Ecuador es contar con responsables del área de ciberseguridad, pero es importante diferenciar que la gestión de seguridad de información es mucho más amplia y abarca información sin importar el formato, mientras que ciberseguridad se enfoca en información que es vulnerable a través de tecnología de información y comunicaciones (ICT por sus siglas en inglés). Específicamente la ciberseguridad se enfoca en información digital y cualquier otro elemento que no sea información pero que se gestione, opere o maneje a través de tecnologías de información y comunicación (ej. equipo de telecomunicaciones, dispositivos IoT, etc.).

Estructura del área de Seguridad de Información y Ciberseguridad en la organización



Tomando en cuenta esto, el sondeo identificó que sólo un 20% de los participantes gestionan la seguridad de información y ciberseguridad con responsables diferentes: comparado con años anteriores estas son cifras alentadoras que evidencian la necesidad de contar con una gestión dedicada a ciberseguridad, lo cual se incrementará conforme las organizaciones inicien proyectos de transformación digital.

Un aspecto que también será tendencia es contar con estos responsables bajo la modalidad de servicio u "on-demand" (CISO as a Service) como una forma de contar con asesoría especializada, sin la recarga que personal bajo relación de dependencia crea en las organizaciones.

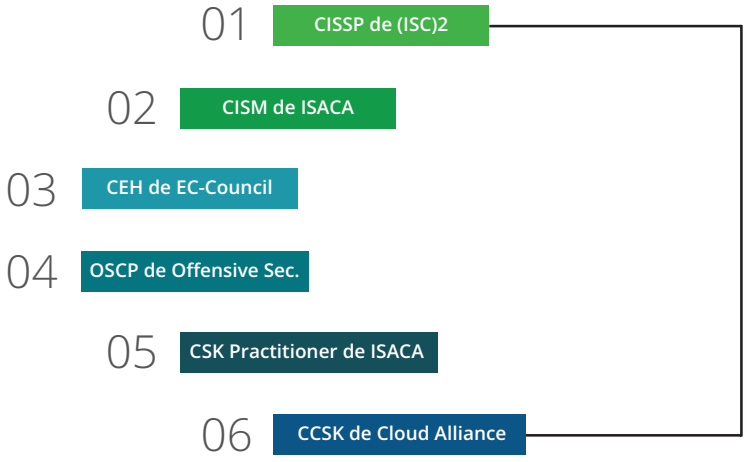
Certificaciones

Otro aspecto importante que nuestro sondeo destaca son aquellas acreditaciones que las organizaciones buscan en aquellos profesionales de ciberseguridad (sean contratados o por servicio).

Certificaciones como CISSP y CISM se destacan entre las que más confianza generan al momento de contratar un profesional de ciberseguridad:

Es interesante notar que, si bien la ciberseguridad se enfoca en un ámbito más operativo, las certificaciones que más confianza generan (CISSP y CISM) tiene un fuerte componente gerencial / estratégico, puesto que la gestión de ciberseguridad no puede ser ajena al resto de la organización y se debe tomar en cuenta su alineación con objetivos estratégicos, así como la optimización de costos.

Certificaciones que generan más confianza al contratar un profesional en ciberseguridad

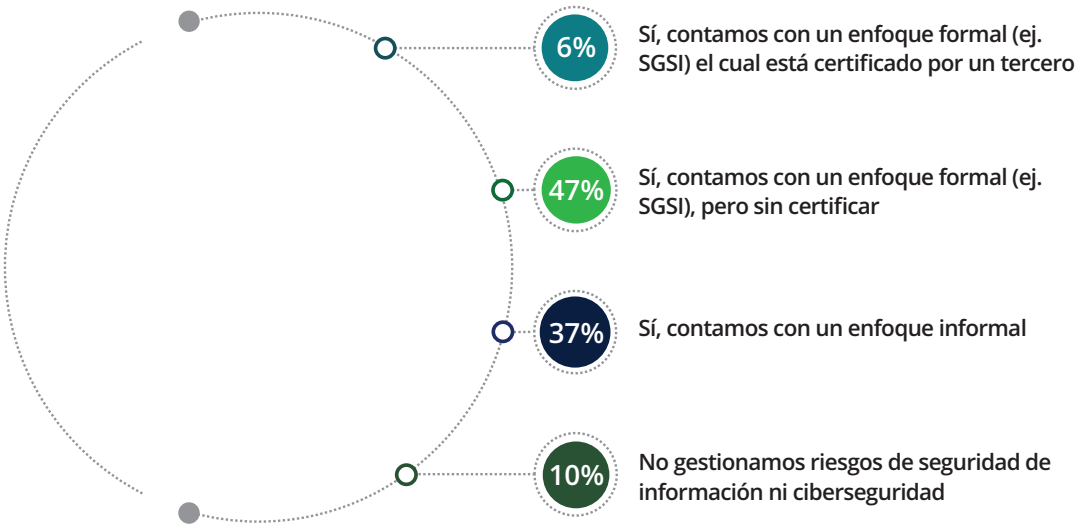


Un aspecto no mostrado en la ilustración es que un 19 % de los participantes afirmaron que ninguna certificación les genera confianza: algo que podría tender a aumentar en el futuro dado que está cada vez más probado que una certificación no necesariamente asegura la competencia de los profesionales de ciberseguridad, o ¿tal vez los costos asociados a su mantenimiento podría ser otro factor influyente? Mantener certificaciones respetables y en buen estado puede tener un costo de entre USD 500 y 1000 anuales dependiendo del número de certificados del profesional.

Enfoque para administrar riesgo

Como parte de la Estrategia y Gobierno, consultamos a las organizaciones si contaban con un enfoque formal para gestionar riesgos y es importante destacar que el 90% de los participantes afirman contar con un enfoque, formal o informal, para gestionar riesgos de ciberseguridad o seguridad de información:

Enfoque utilizado para administrar riesgos de seguridad de información y ciberseguridad

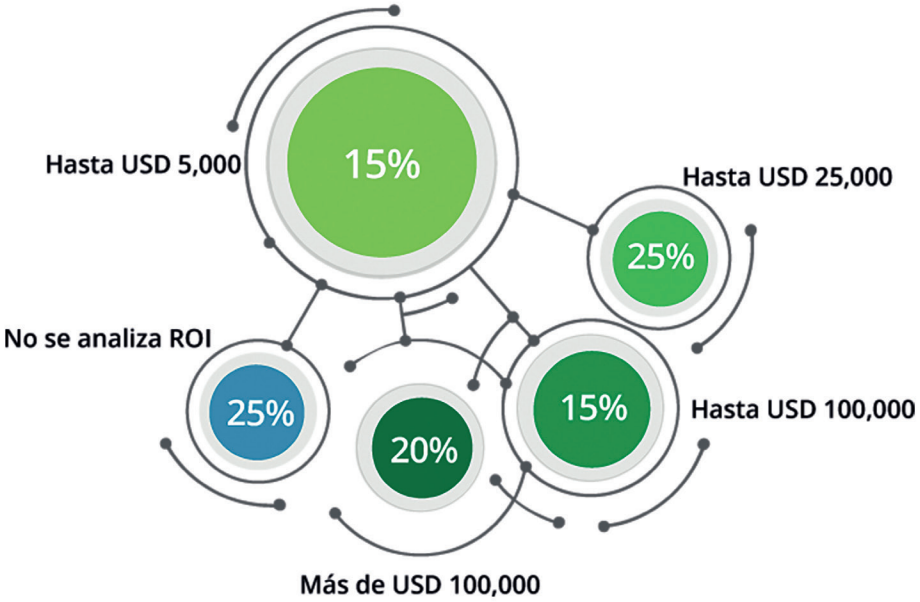


Inversión en ciberseguridad

Inversión en ciberseguridad justificando el retorno de inversión (ROI) ante la Alta Administración

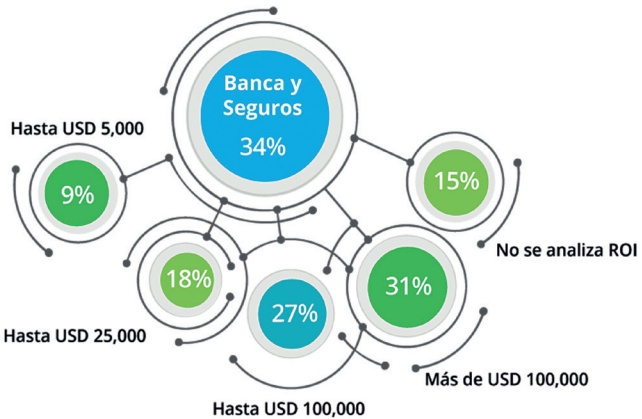
Finalmente, como parte del sondeo, consultamos sobre la inversión justificada en ciberseguridad, y un aspecto relevante es que casi el 40% de los participantes afirman invertir más de USD 25K al año en proyectos de ciberseguridad.

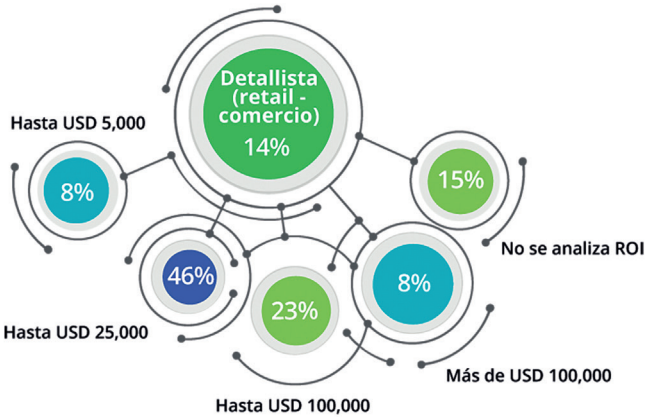
"Con respecto a análisis de retorno de inversión (ROI por sus siglas en inglés), la mayoría de organizaciones que lo realizan están dentro de la industria de Banca y Seguros (5 organizaciones de este segmento afirman no hacerlo): "



Un aspecto destacado es que el sector Banca / Seguros es la industria que mayor inversión justificada realiza en ciberseguridad (desde USD 25K en adelante), seguida del sector Detallista o Retail (entre USD 25K y 100K):

Inversión en ciberseguridad justificando el retorno de inversión (ROI) ante la Alta Administración



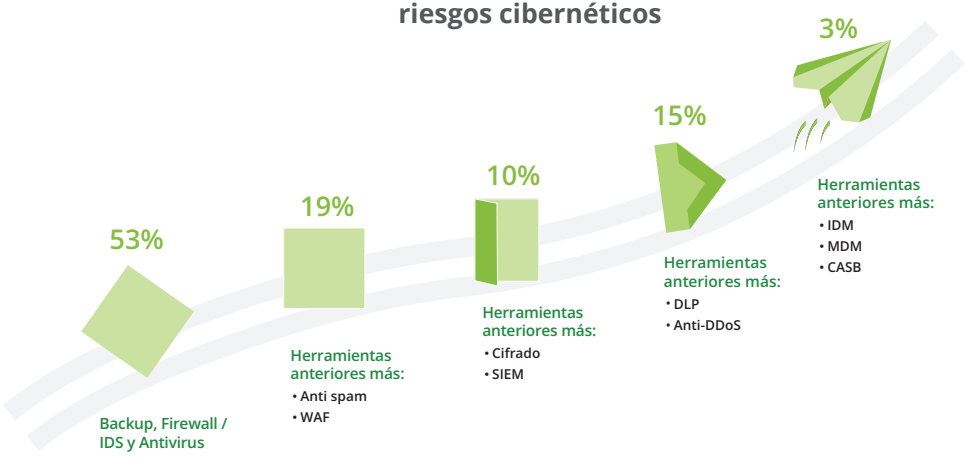


Nota: sólo se muestran los resultados más significativos, por lo cual en la estadística de Inversión por industria no se suma 100%.

PREVENCIÓN

El despliegue de herramientas es una de las principales defensas contra ciber-ataques, y como parte del sondeo consultamos a las organizaciones con qué tipo de herramientas cuentan actualmente:

Herramientas utilizadas para prevenir riesgos cibernéticos



Es interesante destacar que más del 50% de los participantes cuenta con herramientas básicas para reducir el riesgo de ciberseguridad / seguridad de información a través de despliegue de herramientas como firewalls, sistemas de detección de intrusos (ISD) y antivirus. Apenas un 3% de los participantes cuenta con soluciones que permiten reducir riesgos relacionados con servicios de almacenamiento en la nube como Cloud Access Security Broker (CASB por sus siglas en inglés), tecnología que está en auge hoy en día en muchas organizaciones.

VIGILANCIA

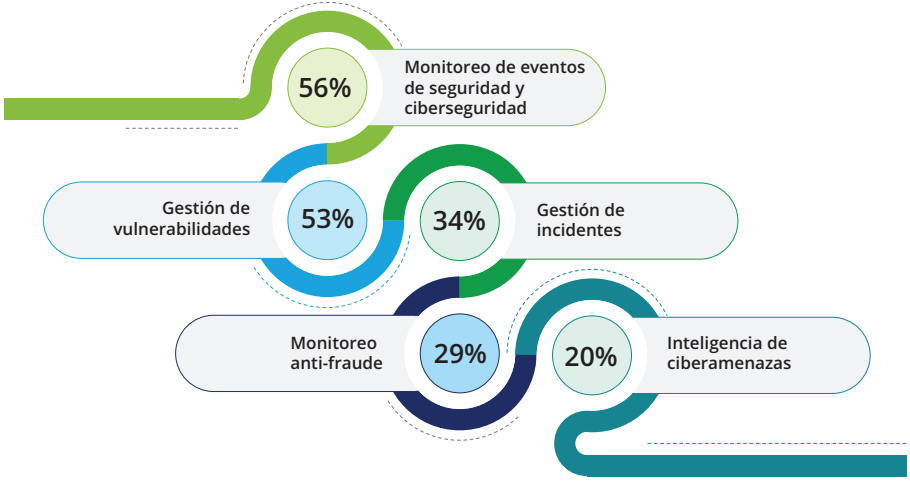
Como parte del sondeo y enfocado en la tendencia de proactivamente vigilar el ciber-espacio para conocer las ciber-amenazas a las cuales está expuesta la organización, consultamos sobre los servicios que actualmente gestiona un tercero en las organizaciones:

Apenas un 20% de participantes afirman realizar actividades proactivas de vigilancia como la "Inteligencia de ciber-amenazas" que permiten descubrir potenciales ataques contra la organización con cierta antelación para adoptar una estrategia de respuesta oportuna y pertinente.

La gran mayoría de participantes enfocan sus esfuerzos en actividades de naturaleza detectiva: Monitoreo de eventos de seguridad, 56% de los participantes, y Gestión de vulnerabilidades, 53% de participantes.

Con proyección a futuro, muchas organizaciones planifican contratar asesoría especializada en tratamiento de datos personales, lo cual está empujado por la Ley de Protección de Datos Personales, que aún continúa como ante-proyecto en la Asamblea Nacional:

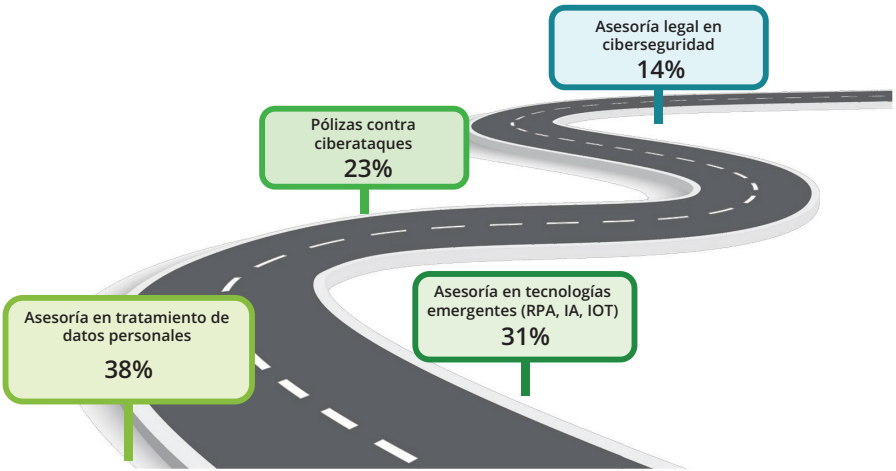
Principales servicios de ciberseguridad gestionados por terceros



A pesar de que tecnologías emergentes como el RPA está en auge en muchas empresas que persiguen optimizar costos operativos, la demanda de asesoría relacionada con este tipo de tecnología apenas alcanza el 31% de acuerdo a lo afirmado por los participantes.

Conforme estas tecnologías emergentes se despliegan más y más en las organizaciones y se modifiquen los procesos con un enfoque de saciar las necesidades del cliente ("client obsessed", puntal central de la Transformación Digital), nuestra percepción es que estos servicios generarán mayor demanda, esperemos que no sea para corregir errores, sino como parte de un enfoque proactivo de mitigación de riesgos.

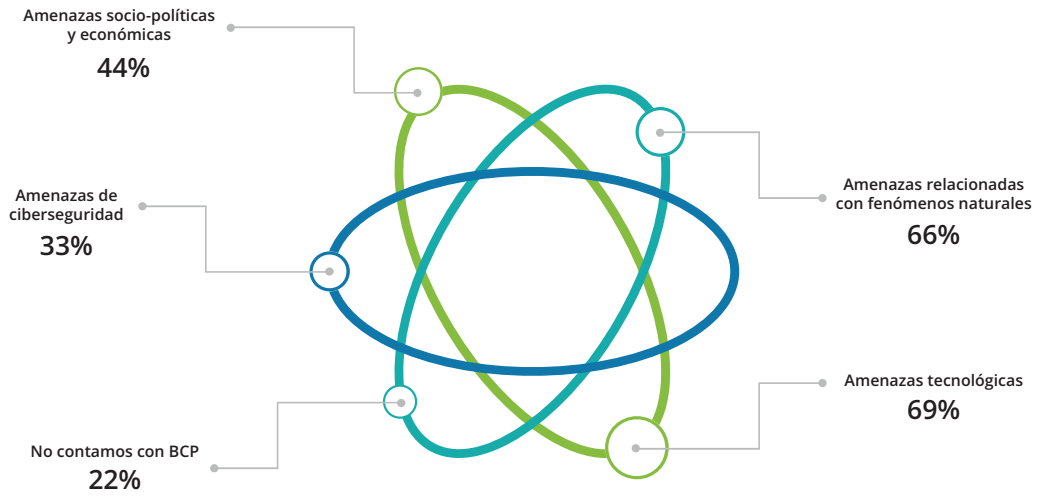
Principales servicios de ciberseguridad a necesitar o contratar en mediano y largo plazo



RESPUESTA

Las amenazas tecnológicas y relacionadas con fenómenos naturales son los aspectos más destacados en los planes de continuidad del negocio (69% y 66% respectivamente), con los que actualmente cuentan las organizaciones participantes.

Amenazas consideradas en el Plan de Continuidad de Negocio (BCP)



En épocas de incertidumbre, aún un 22% de los participantes afirman no contar con un plan de continuidad del negocio y lo cual seguramente puso en aprietos a estas y otras empresas que debieron modificar sus estrategias de continuidad para habilitar el teletrabajo ante la emergencia sanitaria por el Covid-19 (escenario poco probable en el pasado, pero materializado hoy en día).

CONCLUSIÓN

Existen aspectos alentadores que reflejan un leve, pero sostenido crecimiento en la importancia que la gestión de ciberseguridad tiene en las compañías, pero existen otras realidades como la demora en la aprobación de normatividad, la restricción de recursos y la falta de entendimiento de lo que requiere una gestión efectiva de ciber-riesgos para tener una práctica madura y que sea un referente a nivel regional.

ESTADO DE LA CIBERSEGURIDAD
ECUADOR 2020

ITahora Deloitte. AECI

Anunciantes Especial Seguridad: