Digital Trust Insights 2021

La ciberseguridad madura por la aceleración digital.

pwc

Índice

Introducción

Desde hace un tiempo que la ciberseguridad dejó de ser un área exclusiva de los departamentos de tecnología. Hoy los líderes de seguridad están trabajando en estrecha colaboración con los equipos comerciales, para fortalecer y aumentar la resistencia de la organización en su conjunto.

Los resultados de nuestra encuesta anual Digital Trust Insights 2021, realizada a más de 3200 directivos de negocios y tecnología de todo el mundo, nos brindan una visión detallada de las claves para abordar con éxito los desafíos actuales y los que están por venir en el ámbito de la ciberseguridad.

La pandemia ha acelerado los planes de digitalización de las empresas, que se han visto obligadas a dar un salto en el uso de las tecnologías digitales para, en muchos casos, cambiar o reinventar sus modelos de negocio. Este contexto provoca un aumento de las brechas de seguridad de las empresas, que se encuentran más expuestas que nunca a los ciberataques. Es por esto que el rol de los CISO (Chief Information Security Officer) es clave. Sus decisiones de negocio y su visión estratégica, en el corto y mediano plazo, se vuelven más necesarias que nunca.

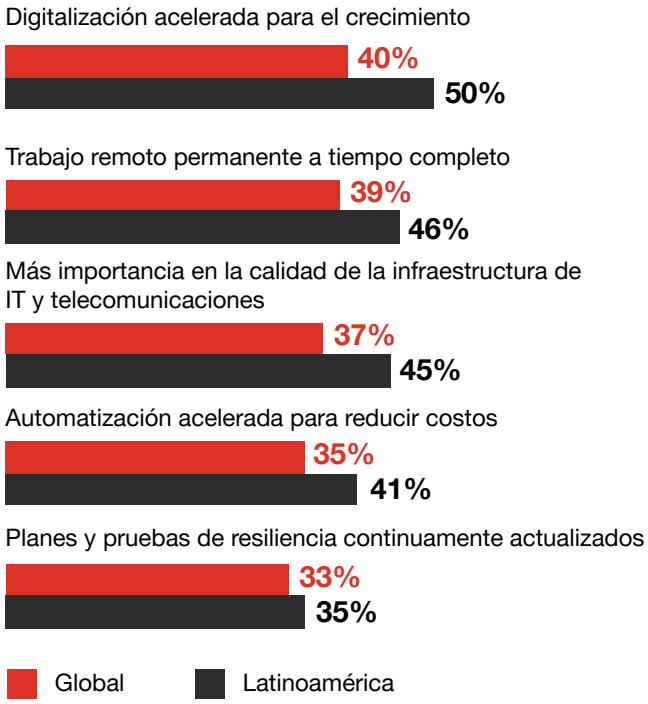
1 Restablecer la estrategia cibernética y desarrollar el liderazgo para los tiempos que se aproximan

Las transformaciones comerciales son más radicales y rápidas

Según los encuestados, en los primeros tres meses de la pandemia, sus organizaciones se digitalizaron a una velocidad sorprendente.

A nivel global el 40% de los ejecutivos afirmó que está acelerando la digitalización, quizás adoptando estrategias comerciales que no habían imaginado antes, mientras que lo que respecta a América Latina el 50% está optando por una digitalización acelerada para su crecimiento.

Los negocios están cambiando...



Los nuevos tiempos exigen un restablecimiento de la estrategia cibernética

El 96% de los encuestados a nivel global aseguró que ajustará su estrategia de ciberseguridad debido al COVID-19. La mitad de este porcentaje tiene más probabilidades de considerar la ciberseguridad en todas las decisiones comerciales, lo que representa un aumento del 25% a comparación de la edición anterior.

Por su parte, casi el 100% de los encuestados de América Latina decidirá ajustar sus estrategias de ciberseguridad.

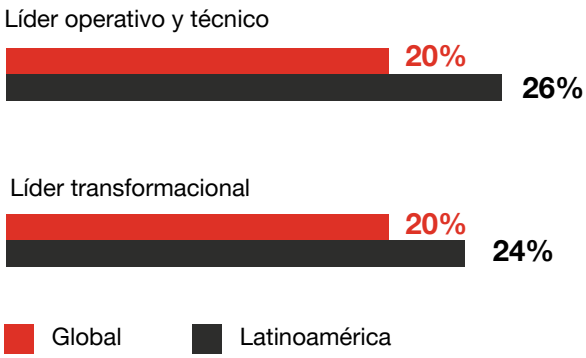
...y también sus ciberestrategias

Los CISO están evolucionando según las necesidades de las empresas

Los nuevos tiempos también exigen nuevos liderazgos. A nivel global el 20% manifestó que necesita un CISO como líder transformacional y otro 20% como líder operativo y técnico.

Algunos CISO ya ocupan estos roles y muestran las cuatro cualidades más buscadas por los ejecutivos: pensamiento estratégico (38%), capacidad para asumir riesgos (38%), habilidades de liderazgo (36%) y capacidad para reconocer y fomentar la innovación (34%).

...y también sus ciberestrategias



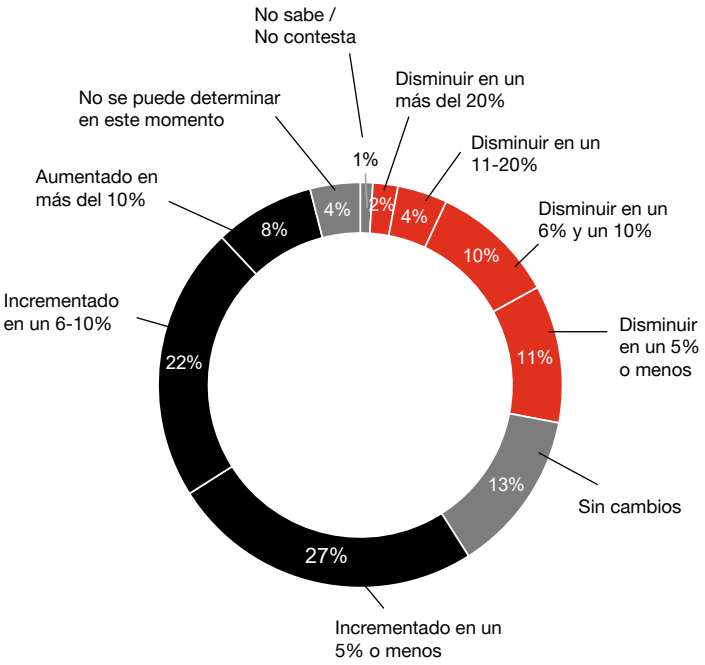
2 Reorganizar el presupuesto en ciberseguridad para optimizarlo

Para más de la mitad de los encuestados los presupuestos en ciberseguridad aumentarán

El 55% de los encuestados a nivel global indicó que aumentará su presupuesto en ciberseguridad, teniendo en cuenta, entre otras, las siguientes acciones, el 51% agregará personal cibernético a tiempo completo en 2021, incluso cuando la mayoría (64%) de los ejecutivos esperan que los ingresos comerciales disminuyan. Sin dudas la ciberseguridad está cobrando más relevancia, pero aún así, el 27% incrementará en un 5% o menos su presupuesto y el 13% no incorporará cambios.

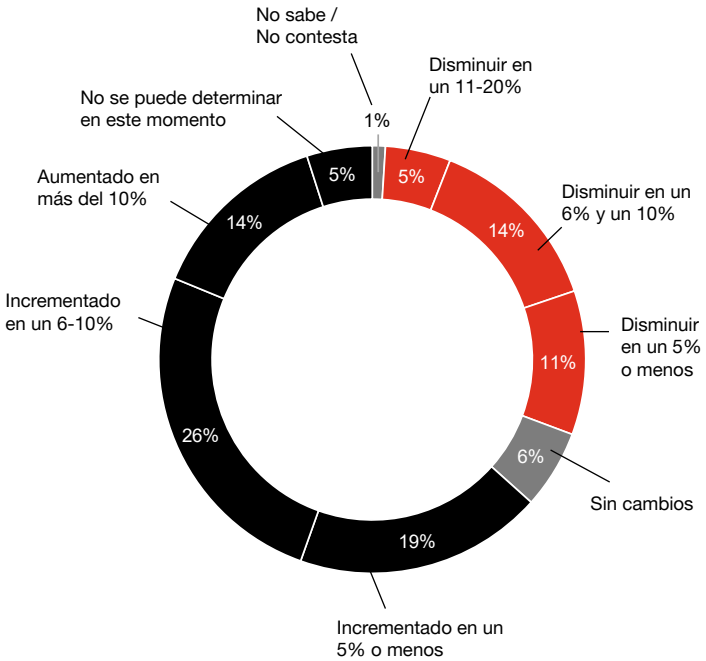
En lo que respecta a América Latina el 59% de los ejecutivos encuestados aumentará sus presupuestos de ciberseguridad, mientras que el 30% disminuirá la inversión y un 6% mantendrá sin cambios el presupuesto para el área.

Global



- Neto: disminución 26%
- Neto: aumento 55%

Latinoamérica



- Neto: disminución 30%
- Neto: aumento 59%

La mayoría de los ejecutivos no confía en el proceso presupuestario

El 44% piensa cambiar su proceso presupuestario y el 37% está totalmente de acuerdo en que la cuantificación de los riesgos cibernéticos puede mejorar significativamente la forma en que gestiona el gasto frente a los riesgos. Sin embargo, más de un tercio coincide plenamente en que las organizaciones pueden fortalecer su posición cibernética, al tiempo que se contienen los costos, gracias a la automatización y racionalización de la tecnología.

La confianza en los procesos y presupuestos cibernéticos es baja en la actualidad.

3 Equilibrar la situación con respecto a los ciberatacantes

Las nuevas tecnologías ayudan a reducir los ciberdelitos

La innovación está cambiando el juego de la ciberseguridad, brindando nuevas ventajas a los defensores y nivelando el campo de juego con los atacantes. Entre un 15 y 19% de los ejecutivos encuestados ha manifestado que se está beneficiando de las nuevas tecnologías. Ellos son los que denominamos los *early adopters*, es decir que no solo afirman acceder a soluciones mucho más avanzadas para proteger su negocio frente a ataques sofisticados sino que también invierten en la clásica trifecta de transformación digital (personas, procesos y tecnologías) para reducir la brecha que los ciberatacantes han mantenido durante mucho tiempo.

Más transformación, implica más progreso

En su mayoría, los ejecutivos aseguran haber logrado un “progreso significativo” en los últimos tres años en la gestión de los riesgos, en conseguir mayor resiliencia, mayor confianza y, en definitiva, en una transformación digital más rápida.

Los principales resultados, informados por el 43% de los ejecutivos, son mejores experiencias de los clientes, respuestas más rápidas a incidentes e interrupciones y una mejor prevención de ataques exitosos.

Estos resultados sugieren que invertir en todas las ventajas en tecnologías, procesos y capacidades de su personal es fundamental para lograr avances significativos contra los ciberatacantes.

Progreso de los objetivos de ciberseguridad en los últimos tres años.

Global 74%

América Latina 77%

Mejor gestión de riesgos

- Experiencia de empleado menos costosa
- Menores costos de cumplimiento
- Menores costos de gestión de riesgos

Global 77%

América Latina 80%

Mayor resiliencia

- Tiempos de respuesta más rápidos
- Menor tiempo de inactividad y costos asociados
- Mayor prevención de ataques exitosos

Global 76%

América Latina 81%

Mayor confianza

- Mayor fidelidad de los clientes
- Mayor cumplimiento de la normativa
- Mayor confianza de los líderes

Global 76%

América Latina 81%

Impulso al negocio

- Entrada acelerada a nuevos mercados
- Lanzamiento acelerado de nuevos productos
- Experiencia de cliente mejorada
- Experiencia de empleado mejorada
- Transformaciones más exitosas

La seguridad en la nube es el próximo gran cambio

Las empresas están trasladando rápidamente sus operaciones (75%) y seguridad (76%) a la nube. Es por esto que eliminan los sistemas estáticos e inseguros en favor de sistemas integrados de nube más dinámicos y ágiles.

Más de un tercio (35%) de los ejecutivos están totalmente de acuerdo en que el cambio a la nube, es fundamental para la próxima generación de soluciones comerciales para su organización.

4 Desarrollar resiliencia para cualquier escenario

Las perspectivas de ciberamenazas para el próximo año 2021

El 40% del total de los encuestados, aumentará las pruebas de resiliencia para garantizar que, si ocurre un evento cibernético disruptivo, sus operaciones comerciales críticas se mantendrán en funcionamiento.

En 2020 han aumentado notablemente los ciberataques: intrusiones, ransomware, violaciones de datos, e intentos de phishing.

Ante este escenario, más de las tres cuartas partes de los ejecutivos aseguran que las evaluaciones y las pruebas, bien hechas, pueden ayudarlos a orientar sus inversiones en ciberseguridad.

El **40%** de los ejecutivos manifestó que aumentará las pruebas de resiliencia en 2021

5 Preparar el equipo de seguridad para el futuro

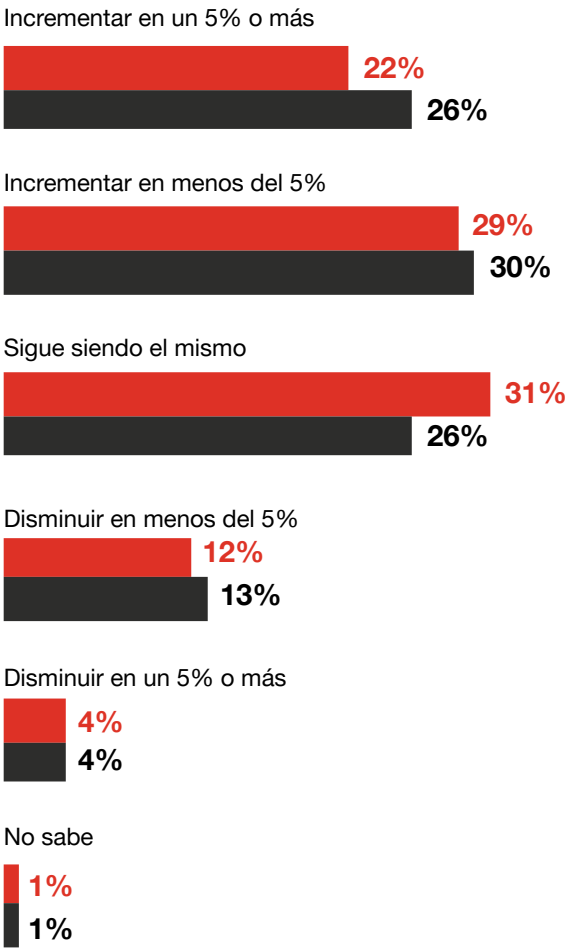
Se busca: 3,5 millones de personas para trabajos de ciberseguridad en 2021

A nivel global, más de la mitad (51%) de los ejecutivos incorporará personal de ciberseguridad a tiempo completo durante el próximo año. Por su parte el 22% aumentará su personal en un 5% o más.

Esto parece no ser suficiente, para 2021 se espera una alta demanda a nivel mundial de puestos de ciberseguridad, pero la falta de trabajadores calificados hace difícil satisfacer la necesidad de la industria.

Los puestos más buscados son: soluciones en la nube (43%), ciberinteligencia (40%) y análisis de datos (37%).

En América Latina, el 56% de los ejecutivos planea incorporar puestos de ciberseguridad a tiempo completo durante el próximo año. Por su parte el 26% aumentará su personal en un 5% o más.



Ciberseguridad: las nuevas habilidades que se buscan en el siglo XXI

Al momento de contratar nuevos talentos en ciberseguridad, no solo se buscan habilidades digitales sino también sociales y de negocios.

En América Latina, el 56% de los ejecutivos busca en sus nuevos empleados habilidades analíticas, el 57% habilidades comunicativas y el 58% en creatividad.

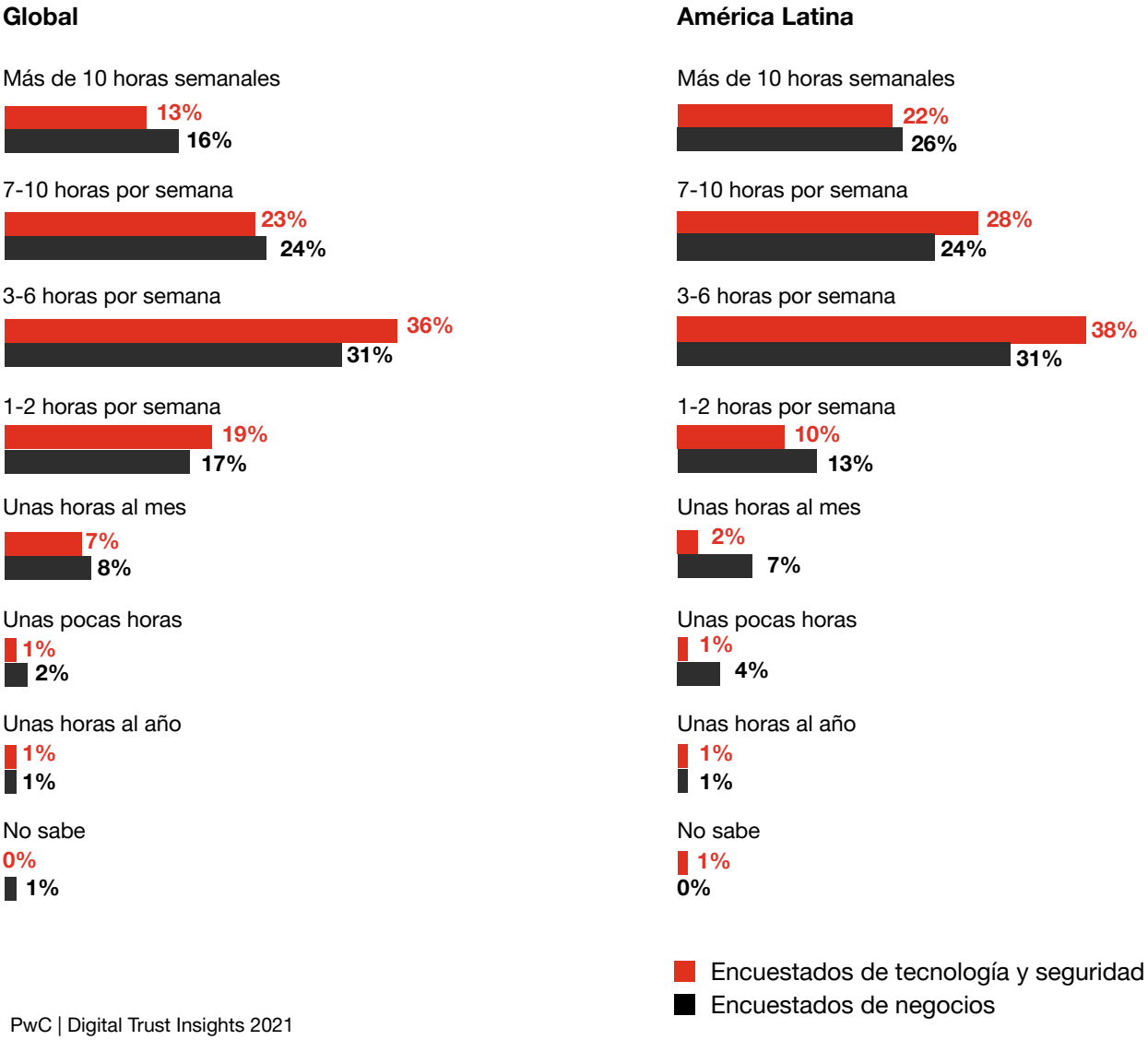
Las nuevas demandas en el mercado laboral, se corresponden al rol ampliado del CISO, es decir un lider no solo tecnológico sino también versátil, capaz de trabajar en equipo y agregar valor a la compañía en general.

No obstante, estos nuevos perfiles en tecnología y seguridad son muy difíciles de cubrir y ante la falta de trabajo calificado muchas compañías apuestan a sus empleados.

En este sentido, casi tres cuartas partes de los ejecutivos de tecnología y seguridad a nivel global afirmó dedicar tres o más horas semanales al aprendizaje y formación relacionado con su trabajo, y más de un tercio (36%) dedica más de siete horas semanales.

En cuanto a América Latina el 72% de los ejecutivos de tecnología y seguridad, aseguró invertir tres o más horas a la semana en cursos y capacitaciones, mientras que el el 48% dedica más de siete horas a la semana.

Las últimas tecnologías requieren invertir en la capacitación y aprendizaje del personal



Acceder al talento a través de modelos de servicios gestionados

Las plataformas de servicios administrados (redes, nube, datos, herramientas analíticas, visualización, aprendizaje automático) están en constante evolución.

Al pasar a un modelo de servicios administrados, una organización puede evitar no solo los costos de inversión en tecnología, sino también los riesgos que plantea la tecnología heredada, incluida la necesidad de actualizaciones constantes. Casi el 90% de los encuestados usa (o planifica hacerlo) servicios administrados.

Acerca de nuestros servicios de seguridad de la información

En PwC Argentina contamos con una práctica que tiene más de 24 años en el mercado. La misma está compuesta por profesionales con vasta experiencia y diversidad de conocimientos en materia de seguridad de la información, especializados por industria, plataforma y aplicación. Contamos además con un laboratorio especialmente diseñado para estudios de seguridad y análisis, así también con un Security Operation Center que permite monitorear eventos de seguridad en forma activa (7x24), y que incorpora inteligencia ante amenazas, detección de vulnerabilidades, y cuando sea requerido, respuesta a incidentes.

Organización: ciberseguridad y seguridad de la información

- Evaluación y diagnóstico del nivel de madurez y estructura organizativa de las áreas.
- Asistencia en la definición y desarrollo del mapa de ruta estratégico de ciberseguridad/seguridad de la información en la organización.
- Evaluación del nivel de cumplimiento en las distintas prácticas y procesos en relación a las mejores prácticas y/o estándares del mercado (NIST, ISO 27000, PCI-DSS, Ley de Protección de los Datos Personales, SWIFT CSP, Normativas del Banco Central, etc.) y asistencia en la alineación a dichas normativas.
- Clasificación de los activos de información.
- Asistencia en la definición y desarrollo de procesos e indicadores de seguridad de la información.

Implementaciones de soluciones de ciberseguridad

- Gestión de identidades y accesos (CIAM y IAM).
- Identidad digital con uso de biómetricas.
- Protección de activos en la nube (Cloud Access Security Broker y seguridad nativa de la nube).
- Implementación de soluciones de Identidad Digital con uso de biométrica.
- Gestión de usuarios privilegiados.
- Implementación de herramientas para la prevención y detección del fraude financiero.
- Detección de vulnerabilidades en redes de Tecnologías de la Operación (OT)
- Gestión de riesgos.
- Implementación de esquemas de seguridad para distintas plataformas y sistemas.
- Diagnóstico de configuración de los sistemas y recomendaciones de mejora.
- Seguridad en redes OT/ICS.
- Análisis de arquitectura de red global.
- Revisión del ciclo de vida del desarrollo de software (SDLC) y desarrollo con metodologías ágiles y DevOps.

Pruebas de intrusión

- Red externa (modalidad caja negra).
- Red interna (modalidad caja gris).
- Red inalámbrica.
- Detección de redes inalámbricas (WiFi) con el fin de identificar el inventario de la compañía. A su vez, analizar el nivel de cifrado de seguridad y protección de las redes en uso por parte de la organización.
- Ingeniería social
- Ejercicios Red Team - OSINT

Ingeniería social

- Phishing SCAM.
- Acceso físico.
- Naiting.
- Ingeniería social reversa.
- Pharming.
- Vishing.

Ciberinteligencia

- Monitoreo 7x24 sobre los activos críticos del negocio, para la detección de:
  - Fugas de información.
  - Robo de credenciales.
  - Hacktivismo, activismo en la red y ataques DDoS.
  - Exposición/vulneración.
  - Uso no autorizado de marca, logo o imagen.
  - Seguimiento de dominios.
  - Seguimiento de identidad digital.
  - Protocolos de actuación.
  - Amenazas sectoriales.
  - Amenazas socio-culturales.

Security Operations Center (SOC)

- Servicio de monitoreo de eventos de seguridad que funciona las 24 horas y permite alertar amenazas cibernéticas.
- Dentro de las actividades se incluyen:
  - Inventario de activos.
  - Evaluación de vulnerabilidades.
  - Monitoreo de comportamiento.
  - Detección de intrusos.
  - Security Information Event Management (SIEM).
  - Inteligencia ante amenazas.

Investigación forense

- Adquisición de evidencia (equipos físicos, tráfico de red, documentos, email, dispositivos móviles, mensajería instantánea, otros).
- Investigación de comunicaciones.
- Definición de palabras clave asociada con la investigación.

Respuesta a incidentes:

- Definir las acciones precisas para el monitoreo y control;
- Atención y recepción de eventos o potenciales incidentes;
- Proceso de notificación y escalamiento;
- Resolución y acciones pos-incidente.
- Asistencia en la gestión de la ciber-crisis: cuantificación de impacto del ataque, afectación de contratos con terceros y SLAs, incumplimiento de normativas, cómunicaciones a terceras partes y/o prensa, etc.

Desarrollo de procedimientos de gestión de cibercrisis

- Desarrollo de procesos integrales para la gestión de cibercrisis que permitan establecer las acciones frente a un incidente de seguridad con alto impacto para la organización, alineados a los procedimientos existentes del BCP/DRP.

Plan de continuidad de negocios

- Elaboración de análisis de impacto al negocio y análisis de riesgo.
- Definición de estrategias de continuidad
- Elaboración de procedimientos de recuperación de desastres (DRP).

Entrenamiento y concientización a usuarios

- Preparación y ejecución de capacitaciones, entremientos y actividades de concientización, que tiene como objetivo abordar los riesgos y amenazas que afectan la confidencialidad, integridad y disponibilidad de la información, así como las medidas de protección relacionadas.

Gobernabilidad, riesgo y cumplimiento (GRC)

- Implementación de seguridad SAP.
- Assessment y reingeniería de seguridad SAP.
- Implementación de matriz de segregación de funciones.
- Outsourcing de seguridad SAP.
- Implementación de sistemas GRC.

Acerca de la encuesta

La encuesta Global Digital Trust Insights 2021 (antes Encuesta Global de Seguridad de la Información (GISS) fue realizada por PwC en julio y agosto de 2020.

Los resultados analizados en este informe se encuentran basados en las respuestas de 3.249 ejecutivos de negocios, tecnología y seguridad (CEO, CFO, CISO y CIO).

El 55% de los encuestados son ejecutivos de empresas grandes (USD 1.000 millones o más en ingresos). El 15% pertenece a empresas con ingresos de USD 10.000 millones o más. Las mujeres ejecutivas constituyen el 28% de la muestra.

Los participantes pertenecen a diferentes industrias: tecnología, medios, telecomunicaciones (22%), mercados minoristas y de consumo (20%), servicios financieros (19%), manufactura industrial (19%), salud (8%) y energía y servicios públicos (8%).

Un 34% proviene de Europa Occidental, un 29% de América del Norte, un 18% de Asia Pacífico, un 8% de América Latina, un 4% de Europa del Este y un 3% de Medio Oriente.

Contactos

Enzo Taibi | Socio
(54 11) 4850-4635
enzo.i.taibi@pwc.com

Diego Taich | Managing Director
(54 11) 4850-6795
diego.taich@pwc.com

Diego Soreira | Gerente
(54 11) 4850-6030
diego.soreira@pwc.com

pwc

@PwC_Argentina /PwCArgentina /PwCArgentina /PwCArgentina /pwcargentina

© 2021 En Argentina, las firmas miembro de la red global de PricewaterhouseCoopers International Limited son las sociedades Price Waterhouse & Co. S.R.L, Price Waterhouse & Co. Asesores de Empresas S.R.L. y PwC Legal S.R.L, que en forma separada o conjunta son identificadas como PwC Argentina.