ESTUDIO SOBRE CIBERSEGURIDAD EN LA ALTA DIRECCIÓN

Dr. Erick Iriarte Ahon

Diciembre, 2024

ESTUDIO SOBRE CIBERSEGURIDAD EN LA ALTA DIRECCIÓN

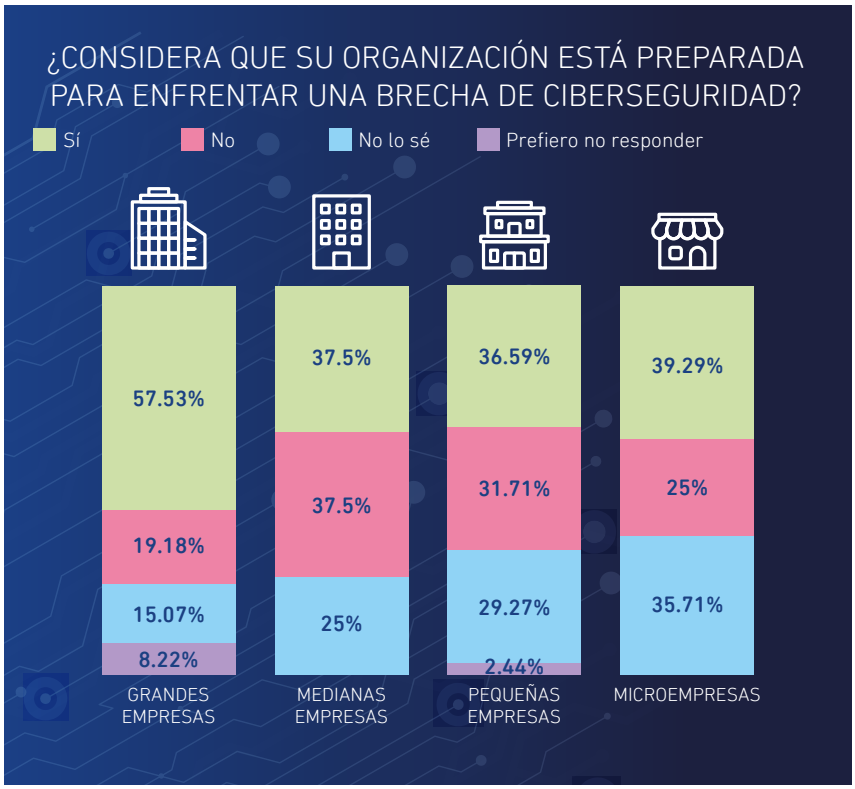
Por el Dr. Erick Iriarte Ahon

El presente estudio esta realizado por eBIZ con el apoyo de IALaw es el primero que se realiza en el Perú sobre la temática. El enfoque era poder conocer como la Alta Dirección de las empresas peruanas esta enfrentando la acción y la toma de decisión en materia de ciberseguridad pero también el conocimiento real que tienen del fenómeno digital.

El levantamiento de información

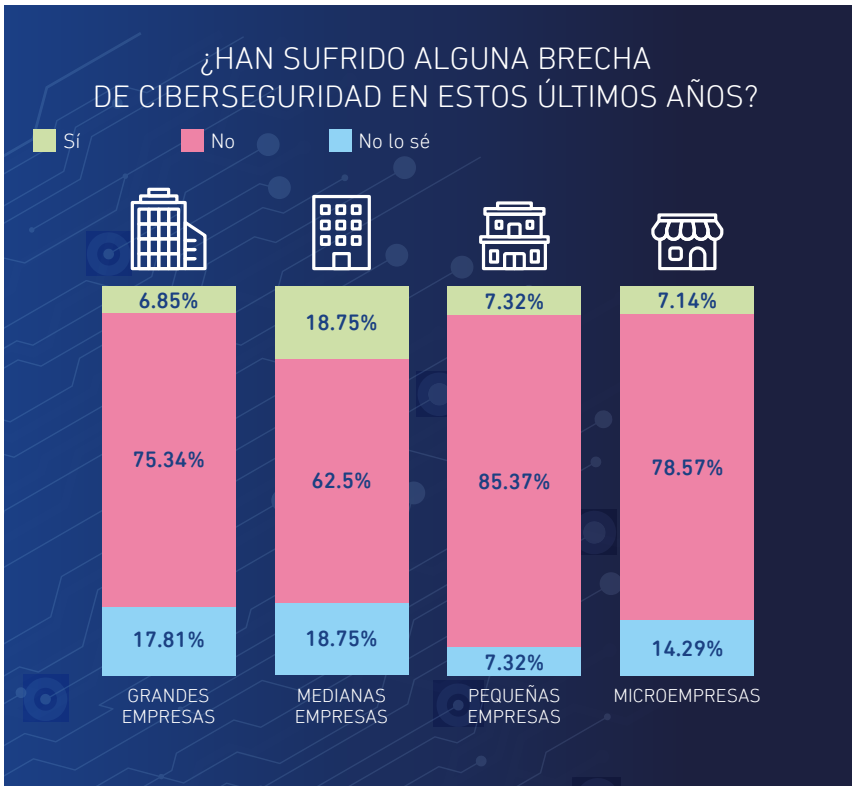
Recopilamos información de 158 empresas (73 grandes, 16 medianas, 41 pequeñas y 28 microempresas), sobre como están enfrentando los problemas de ciberseguridad. La diversidad de sectores que respondieron la encuesta anónima nos ha permitido tener un abanico de áreas de respuesta. Se utilizó para la recopilación un formulario en googleforms, anónimizado y se utilizaron las redes de eBIZ y del PAD para solicitar a altos funcionarios que respondan dicha encuesta.

El primer aspecto que preguntamos era si la organización estaba preparada para enfrentar una brecha de seguridad. Las respuestas se pueden ver en el siguiente cuadro:

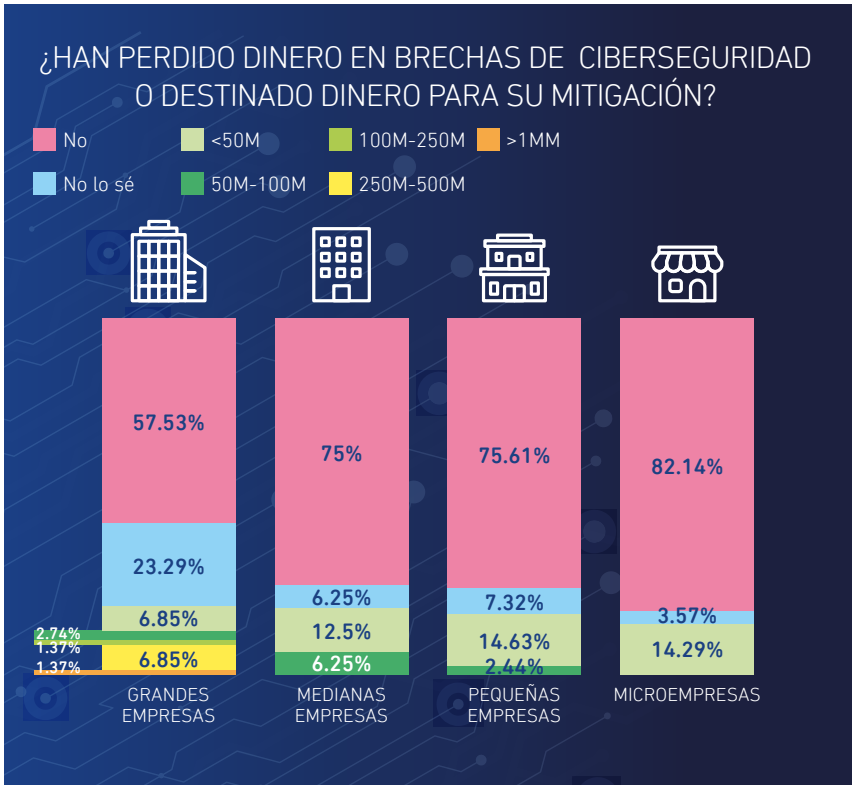


Mientras que la gran empresa presenta un 57.53% de respuesta a que su organización esta preparada para enfrentar una brecha de ciberseguridad, este numero se reduce a 36.59% en la pequeña empresa. La empresa micro y la mediana presentan valores de 39.29% y 37.50% respectivamente. Un dato a incorporar para este levantamiento de información es que un 19.18% de la gran empresa dice que su organización no esta preparada para enfrentar una brecha de ciberseguridad llegando a 37.50% para la mediana empresa y 31.71% para la pequeña empresa. Sin embargo si añadimos la respuesta "no lo se" es decir que no sabe si su organización esta preparada, combinadas suman un 48.73% del total de encuestados, frente a un 46.84% del total que diría que si están preparados.

Sin embargo cuando se les preguntó sobre si habían sufrido alguna brecha de ciberseguridad un 77.22% dijo un categórico no, mientras tan solo un 8.23% del total indicó que si lo habría sufrido, y tan solo un 14.29% respondió, con mayor cautela, que no lo sabían. Cuando desgranamos los resultados la gran empresa respondió que no habían sufrido alguna brecha en un 75.34% superado con la microempresa con un 78.57% y la pequeña empresa con un 85.37%. En las respuestas que si habían tenido un incidente de ciberseguridad la gran empresa indico a penas un 6.85%, mientras que la pequeña empresa 7.32% y la microempresa 7.14%, la mediana empresa reporto sin embargo 18.75%. Un detalle, no menor, es que la pequeña empresa respondió solamente con un 7.32% a no saber si había habido una brecha de ciberseguridad en su organización.

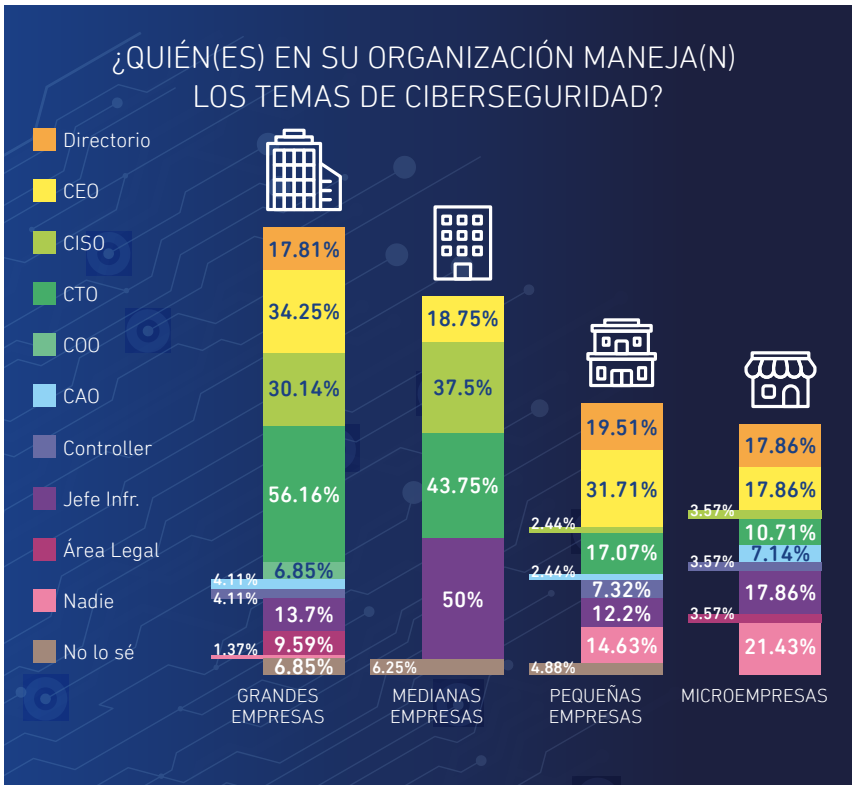


Aun no sabiendo si habían tenido una brecha la pregunta enfocada en cuanto han perdido por brechas de ciberseguridad o destinado a su mitigación (en el mejor de los casos ejercicios de recuperación de información, en el peor de los casos pago de rescate por información afectada), las respuestas nos reflejan que casi un quinto (17.72%) tuvo afectaciones económicas que conocen. El dinero oscila entre menos de 50mil soles (13500 USD aprox) hasta 1MM de soles (270000 mil USD aprox). El porcentaje de empresas que no sabían si habían destinado recursos financieros o sus perdidas por brechas de cberseguridad es 13.92% sobre el total de encuestados, llegando a un 23.29% para la gran empresa y disminuyendo al 3.57% para la microempresa.



También es claro, de las respuestas brindadas, que la percepción de no haber perdido dinero crece en la medida que disminuye el tamaño de la organización (57.53% para la gran empresa, 75.00% para la mediana, 75.615 para la pequeña y 82.14% para la microempresa). Solamente la gran empresa expreso perdidas o dinero destinado por mas de 100mil soles (27000 mil USD aprox).

A la pregunta de quienes se encargan de los temas de ciberseguridad, una pregunta de respuesta múltiple, la respuesta esta fundamentalmente enfocada en el ambiente técnico. La gran empresa respondió que en el 56.16% de los casos que sería el CTO, 30.14% el CISO y 13.70% el Jefe de Infraestructura. Agregan también responsabilidad sobre el CEO (34.25%) y sobre el Directorio (17.81%).

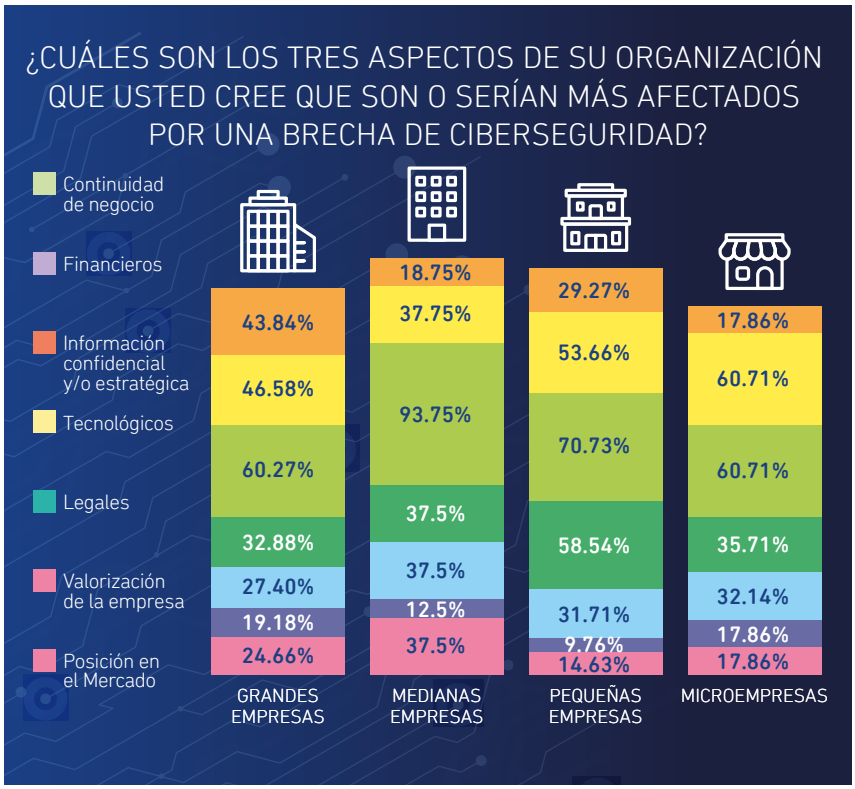


Cuando nos enfocamos en la mediana empresa si bien disminuye ligeramente la responsabilidad sobre el CTO (43.75%), aumenta sobre el CISO (37.50%) y sobre el jefe de infraestructura (50%). En el caso de la pequeña empresa la carga esta sobre el CEO (31.71%), siendo que son organizaciones mas pequeñas no aparece el CISO como respuesta (a penas 2.44%) y el jefe de infraestructura llega a un 12.20%.

Finalmente en el caso de la microempresa, aumenta sobre el jefe de infraestructura hasta un 17.86% la responsabilidad sobre el tema de ciberseguridad, y teniendo similar el porcentaje en relación al Directorio y CEO.

Es notable que en el caso de la pequeña y microempresa la respuesta "nadie" tendría la responsabilidad es de 14.63% y 21.43% respectivamente. En el caso de la gran empresa apenas un 1.37% indica que no habría un responsable. Si es importante señalar que salvo la microempresa, el resto de tipologías tienen respuestas de no saber quien es la persona responsable sobre el tema.

Finalmente le preguntamos sobre el impacto que sufren por las brechas de ciberseguridad las organizaciones. El impacto esta fundamentalmente enfocado en la información confidencial o estratégica que puede ser afectada, siendo además el mayor valor reflejado para la gran empresa (60.27%), para la mediana empresa (93.75%), la pequeña empresa (70.73%) y para la microempresa (60.71%). En contrapartida el concepto de valorización de la empresa es el que menor impacto se mostró en las respuestas siendo en todos los casos menores al 20%, pero en el caso de la pequeña empresa llega hasta 9.76%.



El segundo aspecto en general que se ve reflejado es el de el impacto financiero en todos los segmentos (el mayor es el de microempresa con un 60.71%), solamente superado por impactos tecnológicos a nivel de la pequeña empresa (58.54%). Cabe destacar que los valores para continuidad del negocio son mas altos en la gran empresa y en la pequeña empresa en comparación con la mediana y la microempresa.

Conclusiones.

El presente estudio ha buscado obtener información basada en información pública, siendo que la misma aún no se ha construido en la medida que las empresas no reportan las brechas aún a pesar de legislación en la materia (fundamentalmente para las empresas que están en bolsa o supervisados por la autoridad de valores). Esto es consistente con lo expresado por Amir et al (2018), Kamiya et al (2021) and Bansa et al (2023), sobre el ocultamiento de información, pero también por buscar que el impacto en su ecosistema sea menor.

Es también relevante la respuesta que no han perdido dinero por brechas aún cuando indican que su organización si esta preparada para enfrentar las brechas de ciberseguridad, siendo que además indican que no han sufrido brechas de ciberseguridad en el año en curso. De la primera pesquiza encontramos que en efecto en la creencia que no han sufrido brechas, no habría dinero invertido o afectado, sin embargo el aumento de incidentes refleja una situación contraría. Refleja además que en cualquier caso la afectación ha estado mas en la gran empresa que si ha identificado gasto efecftivo en remediación antes que en los otros segmentos.

La preparación de funcionarios es fundamental, pero también es clara que la participación de los directorios es mínima frente a la problemática, siendo que se prefiere creer que la respuesta es desde la tecnología (se refieren como responsables al CTO, Jefe de Infraestructura o al CISO), antes que una solución integral desde la organización. Cabe destacar que para la gran empresa y para la pequeña son los CEOs parte fundamental que enfrentará las responsabilidad frente a una brecha. Queda también como caso el analizar las respuestas que nadie asuma la responsabilidad y que no lo sepan los tomadores de decisión, similar a la respuesta de no saber si ha habido perdidas por brechas de ciberseguridad.

Una conclusión colateral es la respuesta sobre el aspecto que es más afectado y se refleja en los temas de información confidencial y estratégica y el impacto financiero, y en menor medida la valorización de la organización o la posición en el mercado, conjuntamente con la continuidad del negocio; siendo que hay una disociación aparente entre unas y otras, manteniendo la visión de ser un problema de información y tecnológico, antes que estructural y financiero.

Los directorios están alejados del fenómeno de la ciberseguridad, sea porque se ha entendido como un tema técnico, sea porque considera que su organización no esta preparada (más del 50% de los que indicaron que eran directores de empresas indican que su organización no esta preparada para enfrentar una brecha de ciberseguridad o no lo saben); indicaron que sus organizaciones no habian sido atacadas en los pasados años o no lo sabían; respondieron que no sabían si habían tenido perdidas (solo 12.5% indicaron que habían tenido perdidas o gasto en mitigación, un solo caso reporto entre 250mil y 500 mil soles); Solo 25% considero que el Directorio era responsable de manejar el tema de ciberseguridad, siendo que se enfocaron fundamentalmente en el CTO y el CISO sus respuestas.

La pregunta que queda en el aire es ¿Por qué tras la pandemia siguen los directorios alejados de un problema que impacta en la continuidad de negocio, en la valorización de la empresa y en su posicionamiento en el mercado?

Sobre eBIZ

eBIZ es una empresa con más de 20 años de experiencia en soluciones eBusiness presente en diversos países de Latinoamérica. Nuestra misión es brindar, con eficiencia y eficacia, soluciones que faciliten la relación y las transacciones entre actores de las cadenas de suministro, innovando permanentemente mediante el uso de las TIC para la transformación digital de las empresas de la región. Nuestras soluciones de automatización y simplificación de procesos que van desde la gestión de requerimientos de usuarios internos, pasando por la publicación de órdenes de compra, hasta la gestión de facturas, desarrolladas y probadas en campo con más de un centenar de las más grandes empresas del sector minero e industrial del Perú y la región, facilitan esta interacción dentro de nuestro Ecosistema Digital de Negocios, en donde participan junto con decenas de miles de proveedores, para potenciar oportunidades y así crecer juntos. eBIZ cuenta con certificaciones ISO 9001, ISO 22301, ISO 27001 e ISO 37001, Huella de Carbono Perú – Medición 2019 del Ministerio del Ambiente, Es Empresa Acreedora de la Marca de Certificación "Empresa Segura, Libre de Violencia y Discriminación Contra la Mujer" del Ministerio de la Mujer y Poblaciones Vulnerables, y es licenciataria de las marcas país Marca Perú y Perú Xpert. eBIZ es orgulloso miembro de la red internacional de organizaciones lasallistas, y destina la totalidad de sus Utilidades

Más Información: https://ebiz.pe/

Sobre IALaw

Iriarte & Asociados, un colectivo legal y especializado en gestión pública, está arraigado en las Industrias Creativas y Culturales, con especial atención a las tecnologías de la información y comunicación.

Con una profunda experiencia en normativas de la Sociedad de la Información en América Latina, nuestra fortaleza radica en comprender y aprovechar las tecnologías, así como en utilizar la propiedad intelectual para proteger los intereses de nuestros clientes.

Aunque nuestro enfoque abraza lo tecnológico, también abogamos por el respeto al Patrimonio Cultural y Ambiental. A través de la intersección de la Propiedad Intelectual, Industrias Culturales y Derecho de Nuevas Tecnologías, forjamos una identidad que honra el pasado mientras abraza innovaciones, encarnando una síntesis entre la tradición y el futuro.

Más Información: https://iriartelaw.com/