

ESTADO DE LA ADOPCIÓN DE

ZERO TRUST

EN LATINOAMÉRICA



```

if(money_bah
    printf("\n
    money_b
    )
    )
    if(money_b
        printf("\n
        )
        )
        if(money_s
            {
                printf("\n
                money_s
            )
            )
            if(money_s
                {
                    printf("\n
                    money_s
                )
                )
                if(money_s
                    {
                        printf("\n
                    )
                    )
                    return 0;
                }
            }
        }
    }
}

```

Qué Nos Depara
El Futuro _____ 32

1
0
1
0
1
0

INTRODUCCIÓN



En la era de la transformación digital, las nuevas tecnologías surgen constantemente y redefinen las industrias, creando nuevos modelos de negocio. El proceso de adopción determina la capacidad de la empresa para aplicar estas nuevas tecnologías con el fin de obtener una ventaja competitiva o simplemente mejorar su rendimiento.

Los beneficios de rendimiento de la adopción de nuevas tecnologías se han demostrado en términos de aumento de la productividad, reducción de costes o por la mejora de otras dimensiones no financieras, como la calidad del producto o la adaptabilidad a las nuevas necesidades de los clientes y la sociedad cómo un todo.

El Cloud Computing está impactando en la mayoría de los sectores, independientemente del tamaño de las empresas y es la base para la adopción de tecnologías de propósito general y tecnologías emergentes como el IoT masivo o la inteligencia artificial.

Además, nuestro lugar de trabajo ha cambiado, volviéndose casi remoto por completo de la noche a la mañana. Este cambio ha obligado a las organizaciones a adoptar rápidamente mecanismos que permitan a sus colaboradores realizar sus labores de forma efectiva, colaborando a través de servicios en la nube y compartir datos fuera del perímetro de la red corporativa.



Conforme las organizaciones se vienen adaptando a este nuevo escenario de transformación, los ciberdelincuentes también han evolucionado sus ataques, haciéndolos cada vez más sofisticados y dirigidos, aplicando tácticas más específicas, con más recursos para alcanzar sus objetivos.

En línea con la evolución y adopción del cloud han aparecido metodologías para hacerlo más seguro, como el modelo Zero Trust que permite establecer estrategias guía de securización, para diferentes industrias y organizaciones en todo el mundo.

En este estudio, desde NTT DATA y Microsoft abordamos la adopción del modelo Zero Trust en organizaciones de Latinoamérica, obteniendo una visión del modelo desde el interior de estas empresas y la percepción del beneficio del mismo para su seguridad, así como, los principales obstáculos que identifican en su adopción.

El resultado de este viaje por LATAM nos permitirá conocer la madurez de la adopción del modelo de Zero Trust en las principales organizaciones de la región.

METODOLÓGIA



La metodología aplicada por NTT DATA y Microsoft para la realización del estudio que da origen a este informe ha sido exploratoria y descriptiva y se ha ejecutado en dos fases:

1

Revisión documental:

En esta fase se revisaron diversos estudios realizados a nivel de la adopción del Cloud Computing.

2

Realización de entrevistas a responsables de la toma de decisiones a nivel de seguridad de 35 grandes empresas de Latinoamérica de alcance regional o país. Estas conversaciones han permitido entender el enfoque de adopción y madurez del modelo de Zero Trust en grandes organizaciones de países como Brasil, México, Colombia, Chile, Perú y Argentina.

Este estudio se realizó entre el mes de diciembre del 2021 y el mes de mayo del 2022.

En las entrevistas aplicadas se recolectó información de los participantes sobre temas como: el estado de adopción de la nube en sus organizaciones, el conocimiento y aplicación

del modelo de Zero Trust, las prácticas aplicadas dentro de los entornos empresariales, los beneficios percibidos del modelo para la seguridad, principales barreras de adopción detectadas y la visualización del futuro de sus organizaciones, desde los nuevos enfoques de seguridad en la nube.



RESUMEN EJECUTIVO



Adoptar Zero Trust, empieza a verse como una prioridad para mejorar la seguridad, pero la ausencia de talento y presupuesto son retos aún por superar.

El Cloud Computing es hoy un driver de crecimiento en las organizaciones. Más del 75% de las organizaciones participantes tienen ya servicios disponibles o migrados al cloud y afirman que seguirán evolucionando sobre ello.

Este crecimiento les ha obligado a replantearse la seguridad. Un 69% de estas organizaciones tiene una estrategia definida y socializada enfocada en la formación del talento del área de ciberseguridad para proteger a la organización de los riesgos inherentes al cloud.

Como consecuencia, hoy en día el modelo Zero Trust es bien conocido en la región. El 88% de los participantes conocen el modelo de Zero Trust y un 50% lo utiliza para el despliegue y uso de sus entornos de cloud, de hecho, **adoptar Zero Trust, empieza a verse como una prioridad para mejorar la seguridad.**

El 54% de las organizaciones participantes consideran además que se ha vuelto muy crítica la inversión en la adopción adecuada del modelo de Zero Trust en sus organizaciones. Adicionalmente, un 38% se encuentra en este camino, siendo la adopción de Zero Trust parte de su estrategia actual de seguridad.

Zero trust es un modelo enfocado a la seguridad en 6 capas: identidad, endpoints, aplicaciones, datos, infraestructura y red.



Tras las conversaciones con las empresas de la región se percibe que las capas de mayor adopción del modelo son **red e infraestructura**; ambas capas han heredado en el cloud, las buenas prácticas implementadas en los entornos on-premise, lo que se traduce en una mayor madurez de adopción de los controles respectivos; En el caso de las capas de aplicaciones y endpoint queda aún más camino por recorrer y resulta interesante constatar en el caso de las aplicaciones, cómo las organizaciones coinciden en destacar que su protección es cada vez más importante, sin embargo, los controles definidos como básicos para su protección, no están implementados en más de la mitad de las organizaciones.

En el caso de los endpoints, la problemática viene dada por la velocidad de su crecimiento en números, lo que ha compensado el aumento de la protección en cuanto a cantidad de dispositivos. Precisamente por este aumento en número de endpoints es que no consiguen avanzar de forma significativa.

El hecho de que el modelo Zero Trust sea un referente en la industria, está impulsando su adopción en las organizaciones. Más del 52% de las organizaciones considera que se



encuentra por delante de otras en su proceso de adopción, lo que demuestra que las organizaciones se encaminan a una mayor seguridad y aumento de la eficiencia de sus esfuerzos.

Los mayores beneficios que se perciben del modelo son por una parte, **tener un mejor control sobre el entorno del cloud y por otra, una protección más adecuada de los datos de sus clientes.**

Finalmente, el modelo Zero Trust da mayor control a las áreas de ciberseguridad sobre la nueva infraestructura, cada vez más utilizada en las organizaciones, y de las operaciones de mayor riesgo e impacto.

A pesar del conocimiento del modelo por las organizaciones, el reconocimiento de sus beneficios y de existir una clara intención por implantarlo, este proceso no ha finalizado aún.

Las barreras que actualmente existen para su completa adopción están relacionadas con el talento humano, el desarrollo del caso de negocio y el soporte de los partners; y de alguna manera, las tres están relacionadas con la primera: La barrera del talento.

Las organizaciones no cuentan con talento propio o tercerizado para ejecutar las iniciativas relacionadas con la adopción de Zero Trust. El no disponer de estos equipos hace que ni siquiera se llegue a realizar el caso de negocio para la implantación de seguridad en nube y por



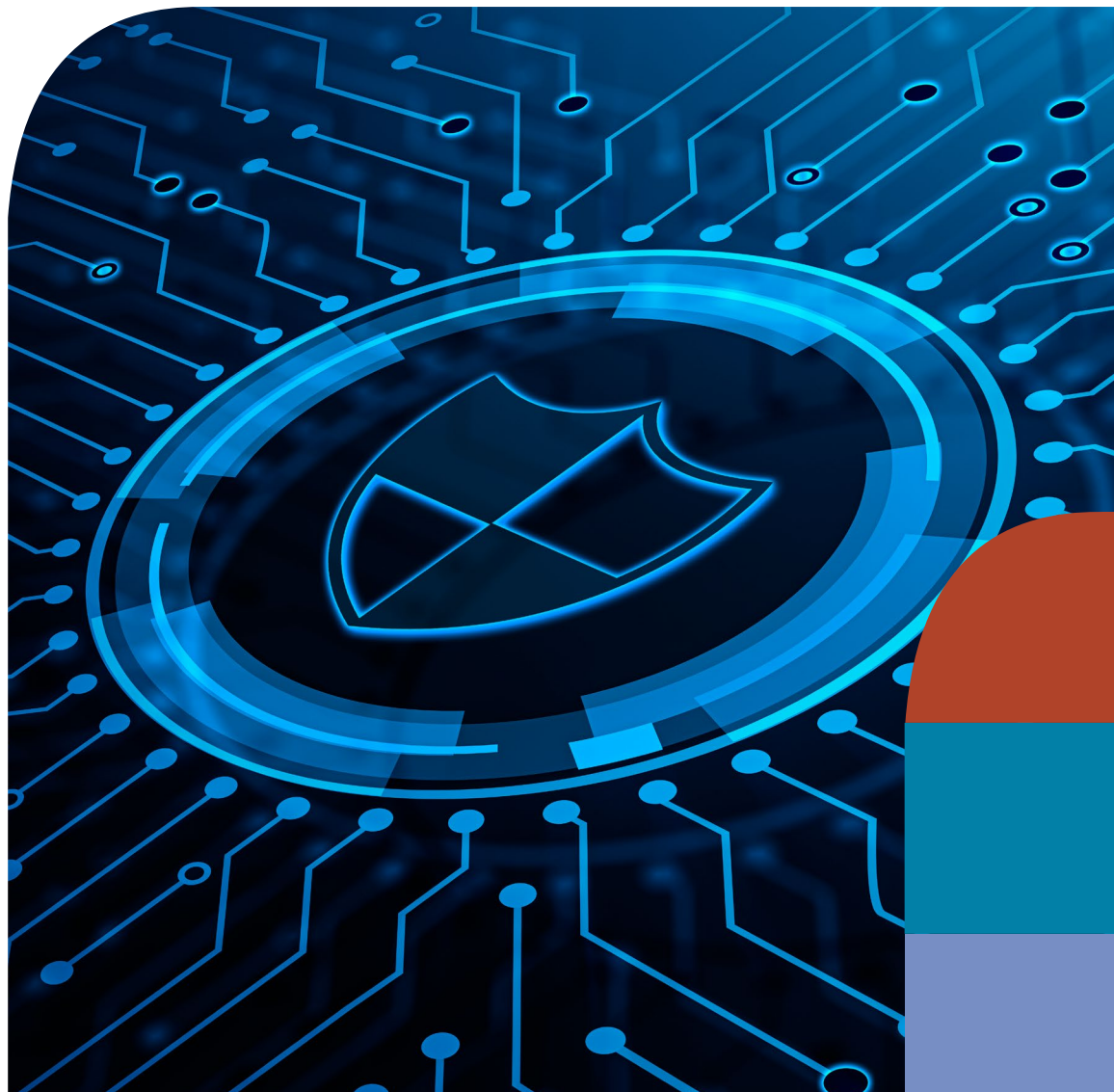
tanto, no se logra la esponsorización del C-level.

A la hora de implantar productos, la propia falta de talento especializado hace necesario un mayor soporte de los fabricantes, lo que algunas veces no se dispone en la medida necesaria.

Otras barreras percibidas son la compatibilidad con los sistemas legados y la falta de presupuesto, **y es que, aunque cada vez más Zero Trust es una prioridad, su implementación requiere de presupuestos adicionales.**

El 73% de los encuestados considera que puede lograr finalizar la adopción de Zero Trust dentro de sus organizaciones y están considerando un horizonte a mediano plazo para ello, por lo que la planificación asociada a la estrategia del negocio se convierte en el principal sustento, para aumentar el presupuesto requerido

Conforme se van implementando cada una de las capas y se demuestren los beneficios, los tiempos de adopción pueden reducirse y aumentar la inversión.



ADOPTIÓN DE ZERO TRUST EN LATINOAMÉRICA

VISIÓN GENERAL

El Modelo de Zero Trust está basado en la filosofía de que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso para conectarse a sistemas o servicios de TI hasta que se autentique, y la identidad debe ser comprobada de forma constante.

Los distintos componentes técnicos de la arquitectura Zero Trust están orientados a:

- Garantizar la confianza en la red y frenar los ataques maliciosos,
- Proporcionar acceso seguro a las aplicaciones para los usuarios y clientes,
- Reducir la complejidad y ahorrar en recursos de TI.

Por otra parte, el modelo Zero Trust consta de las siguientes capas:

IDENTIDAD

La identidad es esencial para implementar Zero Trust y nos permite verificar que solo las personas, los dispositivos y los procesos a los que se les ha otorgado acceso a los recursos pueden acceder a ellos convirtiéndose en el control clave, para administrar el acceso en las áreas de trabajo moderno.

Las soluciones de identidad usan Zero Trust mediante:

- Directivas de acceso y autenticación sólidas,
- Acceso con privilegios mínimos con permisos y acceso granulares,
- Controles y directivas que administran el acceso a recursos seguros y minimizan el radio de ataques.

APLICACIONES

Hoy en día, las aplicaciones y las APIs proporcionan la interfaz mediante la cual se

consumen los datos. En un área de trabajo moderna, la adopción de aplicaciones de Software como Servicio (SaaS) basadas en la nube genera nuevos desafíos para las áreas de tecnología.

Los objetivos de esta capa son:

- Descubrir las aplicaciones de TI en la sombra,
- Garantizar los permisos adecuados en la aplicación y el acceso respectivo, con un entorno de análisis en tiempo real que supervise y controle las acciones de los usuarios,
- Identificar y combatir las amenazas cibernéticas en las aplicaciones y servicios en la nube.



INFRAESTRUCTURA

La infraestructura tecnológica, tanto local como multi cloud, se define como todo el hardware (físico, virtual, contenerizado), software (código abierto, de origen y de terceros, PaaS, SaaS), microservicios (funciones, API), infraestructura de red, instalaciones, entre otros, que son necesarios para desarrollar, probar, entregar, supervisar, controlar o dar soporte a los servicios de TI.

La capa de infraestructura nos permite identificar y analizar comportamientos de riesgo, a través de tecnologías que permiten centralizar información del resto de capas para sacar conclusiones y definir acciones de mitigación.

ENDPOINTS (DISPOSITIVOS FINALES)

Hoy en día, los datos pueden fluir a través de una gran variedad de dispositivos, desde IoT a teléfonos inteligentes, BYOD a dispositivos administrados por personal externo o interno, y cargas de trabajo locales a entornos alojados en la nube. Esta situación requiere de un monitoreo constante que permita validar el estado y el cumplimiento del dispositivo, para un acceso seguro.

Esta capa nos permite la visibilidad de los dispositivos que acceden a la red, garantizar el cumplimiento de los niveles de seguridad requeridos según la organización, así como comprobar la seguridad de todo aquello que tiene acceso a los datos de trabajo, incluidas las aplicaciones que se ejecutan en los dispositivos RED.

Las redes empresariales tradicionales están diseñadas para proporcionar a los usuarios acceso a aplicaciones y datos alojados en centros de datos operados por la organización, con una fuerte seguridad perimetral.

Sin embargo, hoy en día se ha masificado el uso de servicios y datos fuera del entorno corporativo. Dado que las aplicaciones y los servicios se han movido a la nube, los usuarios necesitan acceder desde una variedad de dispositivos personales y de trabajo.

Por ello, las soluciones de red son una parte importante del modelo Zero Trust y su objetivo es:

- Comprobar que el ingreso y la salida en el borde de la red es permitido,
- Inspeccionar el tráfico en busca de contenido malintencionado,
- Admitir el acceso con privilegios mínimos y el principio de "asumir una falta", al permitir que las organizaciones segmenten redes y solo conecten usuarios al segmento de la red a la que necesitan acceso.

DATOS

Los equipos de seguridad están muy centrados en proteger la seguridad de los datos, incluso si salen de los dispositivos, las aplicaciones, la infraestructura y las redes que se encuentran bajo el control de la organización. Para ello, los datos deben clasificarse, etiquetarse y cifrarse de forma correcta, y el acceso debe restringirse en función de esos atributos.

Esta capa nos permite cubrir el alcance en torno a la seguridad de los datos y restringir su acceso en función de las políticas de la organización.



IDENTIDAD

Dentro de la capa de identidad, hemos indagado acerca de cómo las organizaciones enfocan sus esfuerzos en cuanto a:

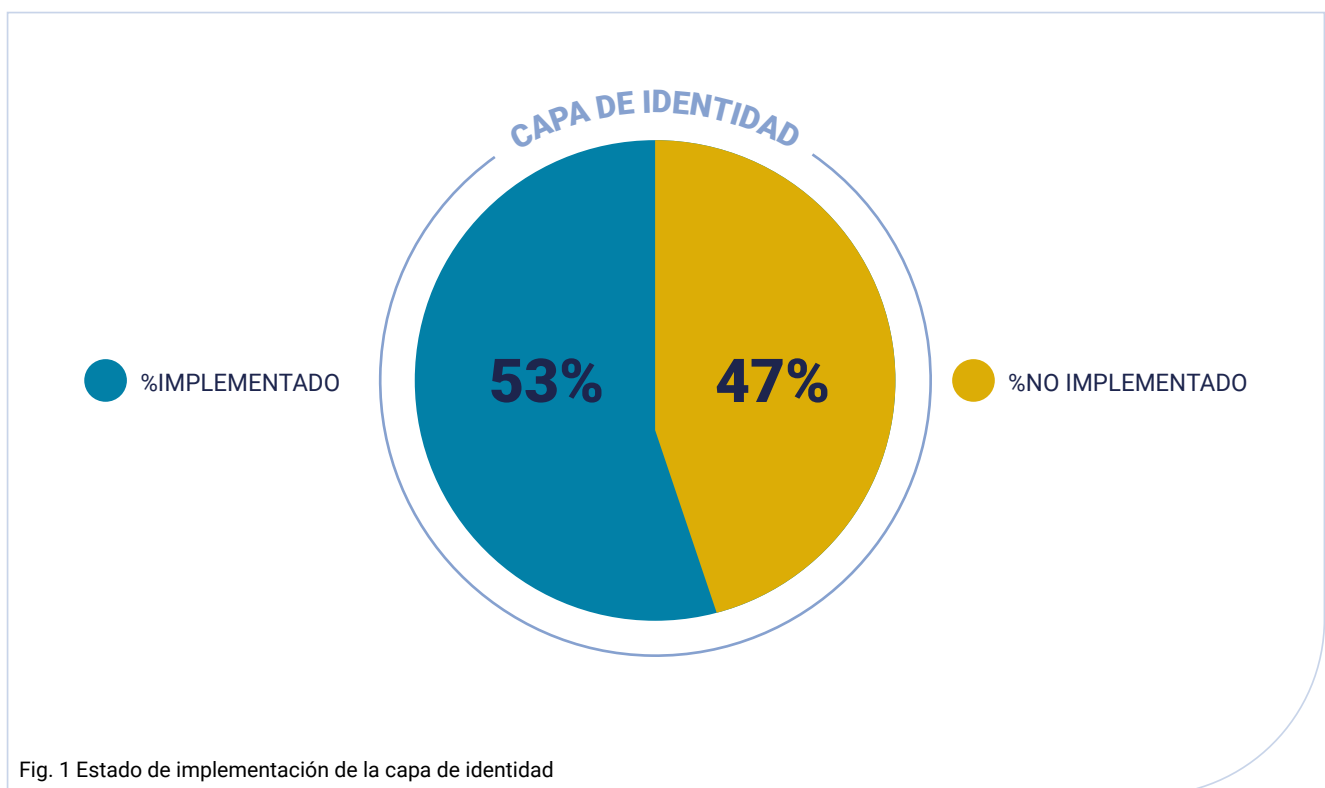
- Implementar y ajustar sus políticas de acceso a recursos, considerando mecanismos de autenticación cada más fuertes, basadas en la implementación y uso de técnicas de inicio de sesión única (SSO);
- Adoptar soluciones de gestión de identidad y acceso (IAM) que usen una mayor cantidad de datos;
- Usar herramientas para proteger, detectar y corregir riesgos de forma automatizada, y mejorar su postura de seguridad, a nivel de la identidad.

Las organizaciones coinciden en que la capa de identidad es prioritaria en la implantación del modelo Zero Trust.

Sin embargo, si analizamos la adopción de cada uno de los controles de la capa de identidad, se observa una dualidad: Por una parte, existen compañías que aún no han iniciado alguno de estos controles ó están comenzando su adopción, mientras otras compañías tienen una

adecuada adopción de gran parte de los mismos, por lo que están muy avanzadas.

Concretamente, el 47% de los encuestados aseguró tener un avance significativo en la implementación de los controles (Fig. 1).



En la adopción de los controles más básicos, las organizaciones priorizan principalmente los mecanismos de autenticación fuerte y su

asociación con las políticas definidas, para tener un mayor control sobre el acceso a sus recursos (Fig 2).

CONTROLES DE LA CAPA DE IDENTIDAD

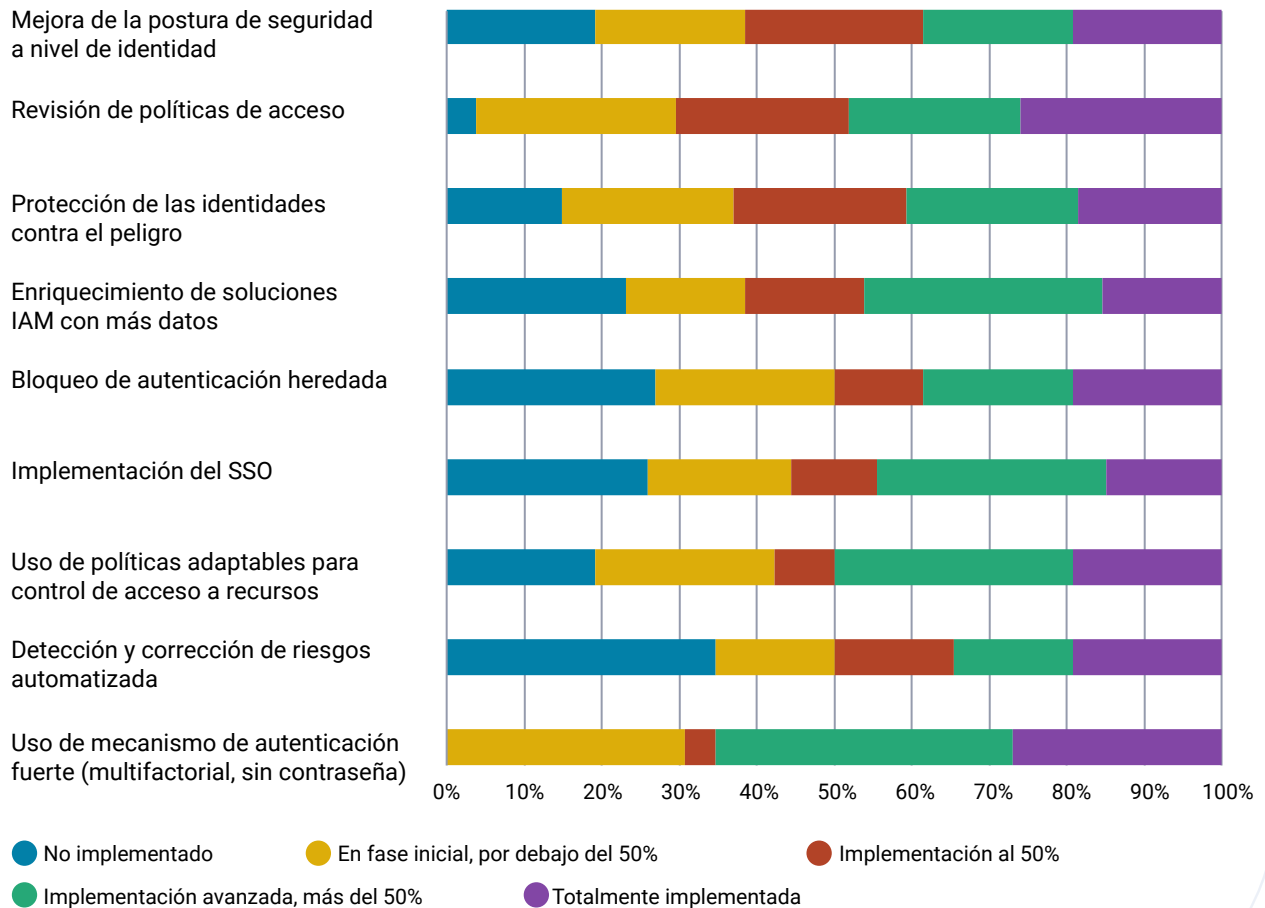


Fig. 2 Listado de controles base para la capa de identidad

Por otra parte, las organizaciones siguen usando el SSO, como un mecanismo de centralización para la autenticación y autorización, sin llegar a una implementación completa. En cualquier caso, la adopción de SSO es un paso necesario para poder explorar y adoptar nuevas tecnologías orientadas a cubrir las necesidades a nivel de esta capa en los entornos del cloud.

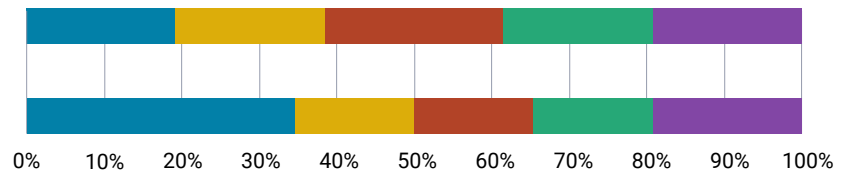
En relación con los controles de la capa de identidad, destacan dos que implican una mayor madurez de la organización para proceder a su adopción: La mejora de la postura de seguridad a nivel de identidad y la detección y corrección de riesgos automatizada, pudiéndose apreciar que las organizaciones buscan mejorar su postura de seguridad (solo un 19% no ha iniciado aún), mientras que la gestión de riesgos automatizada representa un mayor desafío (un 35% no ha iniciado aún). (Fig. 3)



CONTROLES DE LA CAPA DE IDENTIDAD

Mejora de la postura de seguridad a nivel de identidad

Detección y corrección de riesgos automatizada



● No implementado
 ● En fase inicial, por debajo del 50%
 ● Implementación al 50%
 ● Implementación avanzada, más del 50%
 ● Totalmente implementada

Fig. 3 Controles orientados a mejorar la capa de identidad

En conclusión, se podría decir que la capa de identidad, aunque se considera prioritaria y clave en la protección del cloud, representa un área de oportunidad aún para las organizaciones en la región, especialmente para ciertos controles que tienen una adopción menor, pero que implican una mayor seguridad.



APLICACIONES

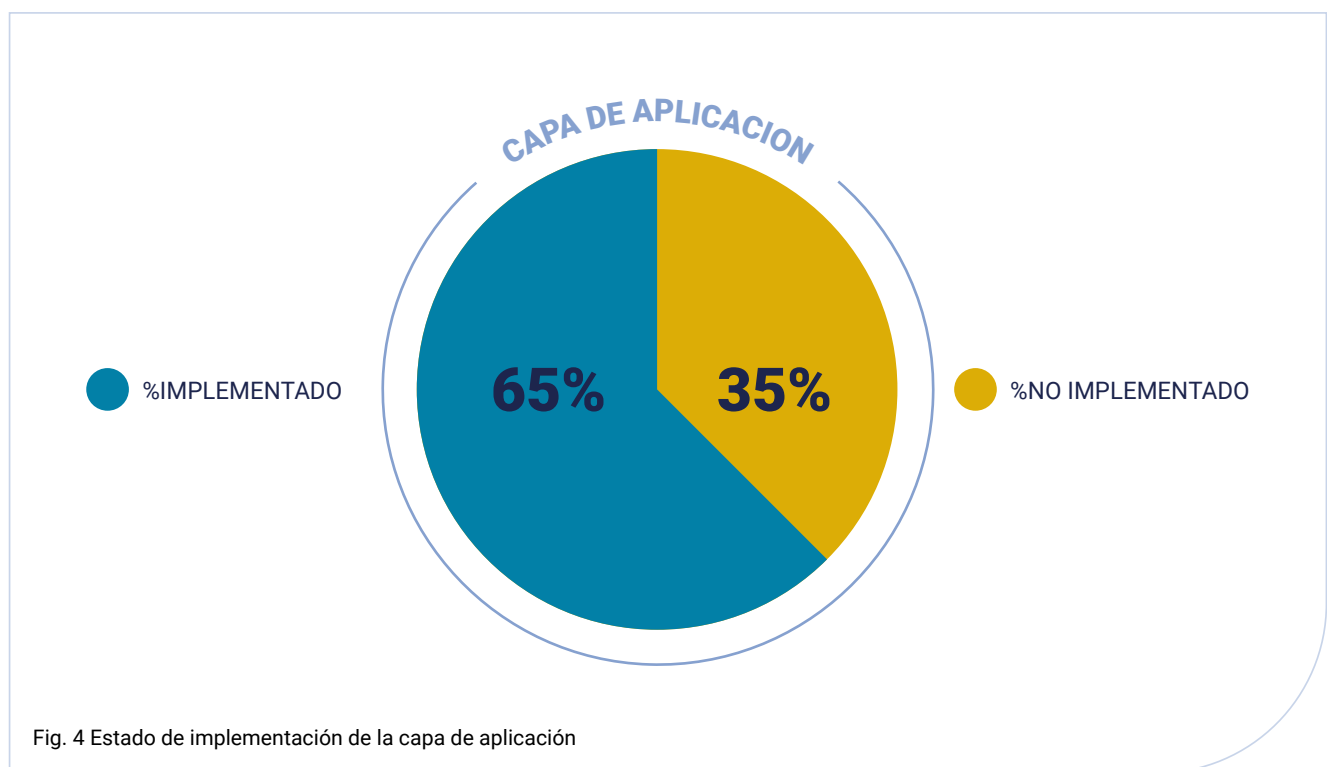
Dentro de la capa de aplicación nos hemos interesado en el nivel que las organizaciones han alcanzado respecto a:

- Evaluar los riesgos en torno a los nuevos elementos en TI,
- El uso y mejora constante de políticas de control de acceso para diversas aplicaciones dentro y fuera de su entorno,
- La forma en que enfrenta la presencia de herramientas que no encuentran bajo la responsabilidad del área de IT (shadow IT),
- La implementación de tecnologías que les permita una mejor visibilidad, integrando

mecanismos de seguridad y un análisis de investigación y respuesta centralizada.

Los ataques asociados a las aplicaciones son comunes hoy en día y las organizaciones dicen ser conscientes de que es necesario mejorar sus niveles de seguridad en este aspecto. Esto contrasta con el nivel de adopción percibido en el presente estudio.

Al consultar sobre el nivel de avance en adopción de los controles Zero Trust de esta capa, observamos que solo un 35% de ellos se encuentran implementados, siendo una de las capas donde se observa una menor adopción. (Fig. 4)



De los 7 controles revisados, especialmente los 4 considerados básicos en esta capa (Fig. 5) se puede extraer algunas ideas:

- La mayoría de las organizaciones emplea los principios base de la seguridad de información para implementar estos controles en sus entornos cloud, pero su alcance sigue siendo muy limitado y en algunos casos, emplean

demasiado tiempo en analizarlos o explorarlos, sin tener una ruta de implantación definida.

- Este hecho provoca una menor visibilidad sobre lo que ocurre entre las aplicaciones y los usuarios, es decir, no se pueden visualizar las acciones que se están realizando, ni si son realmente los usuarios los que realizan estas acciones.

CONTROLES DE LA CAPA DE APLICACION

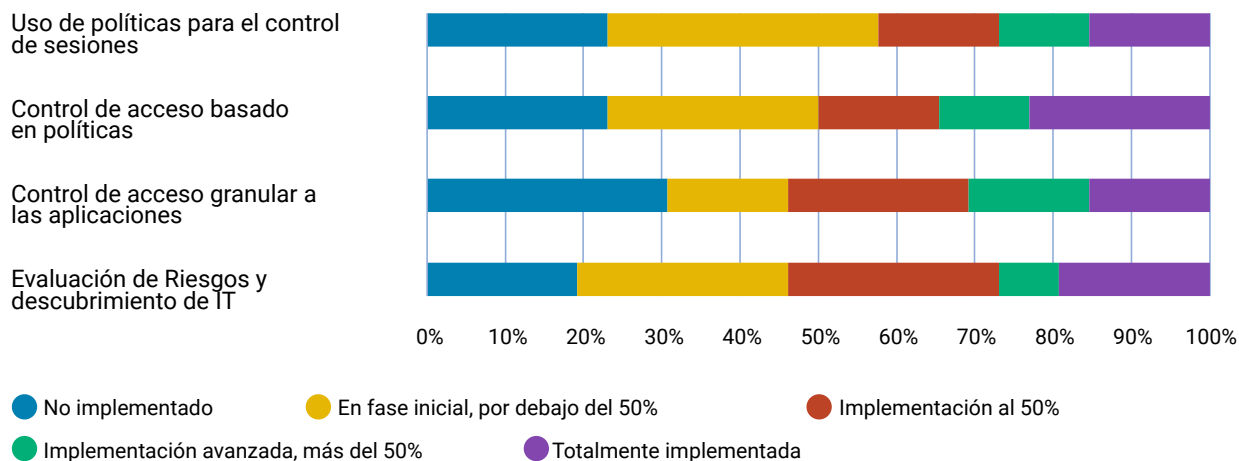


Fig. 5 Listado de controles base para la capa de aplicación

Por otra parte, hay 3 controles que se consideran los más avanzados, y sobre los que se observa una menor adopción, entre los que

destaca el bajo uso que aún se hace de herramientas de seguridad para conectarse a la nube (Fig. 6)

CONTROLES DE LA CAPA DE APLICACION

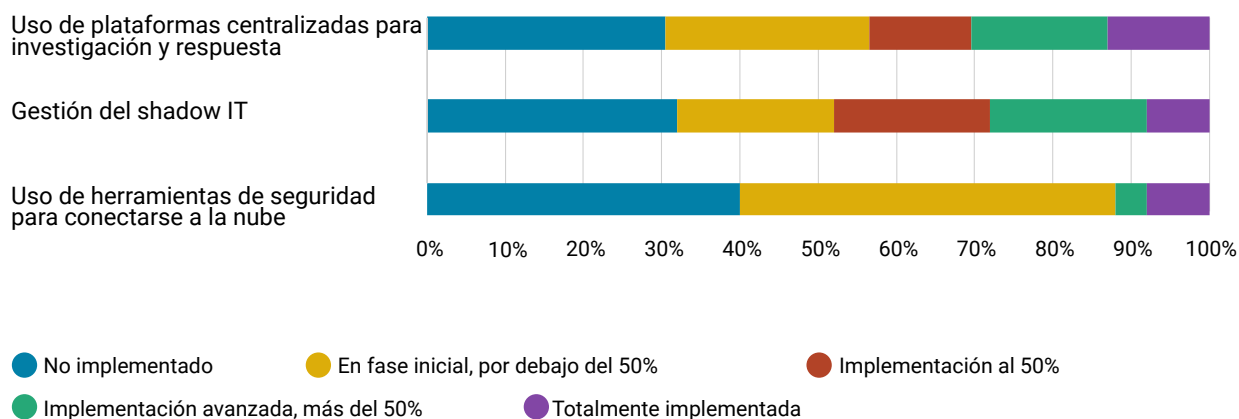


Fig. 6 Controles orientados a mejorar la capa de aplicación

INFRAESTRUCTURA

Dentro de la capa de infraestructura se considera el nivel de implantación que las organizaciones tienen respecto a:

- Contar con una visión granular de los controles en el acceso para la protección de recursos privilegiados relacionados con la

ejecución de labores de carga de información, en entornos de nube híbrida;

- La forma en que los equipos de operaciones pueden usar esta información para analizar el comportamiento de los usuarios, identificar amenazas e integrarlas a tecnologías de análisis y respuestas automatizadas.

El principal objetivo de esta capa es tener una visión granular del tránsito de los datos, entre sus infraestructuras on premise y el Cloud Computing.

Todas las organizaciones consideran que la capa de infraestructura debe tener una serie de controles acordes al entorno y al tipo de negocio. Por ello, el nivel de adopción de estos controles es superior al de otras capas, aunque no por ello se considera que es ideal. (Fig. 7)

Las organizaciones entrevistadas coinciden en haber llevado las buenas prácticas de seguridad on premise al cloud y como consecuencia se aprecia un mayor nivel de adopción de esta capa.

Sin embargo, dado que el cloud tiene su seguridad específica, y en algunos casos se está adoptando muy rápido, no logran una adopción completa del modelo Zero trust.

La Fig. 8, muestra el nivel de adopción de los 7 controles de seguridad de infraestructura que consideramos más básicos, o que una compañía debería cubrir primero. Como puede apreciarse, al menos el 61% de las organizaciones se encuentran en una fase de implementación o despliegue de diversas soluciones y el 49% restante tienen ya una gran parte de sus soluciones desplegadas.

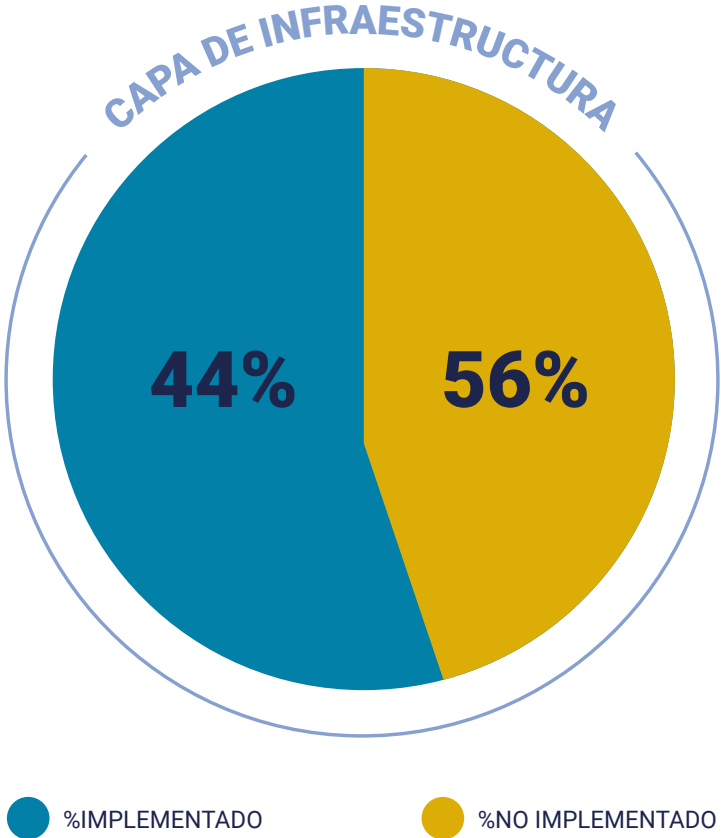


Fig. 7 Estado de implementación de la capa de infraestructura

CONTROLES DE LA CAPA DE INFRAESTRUCTURA

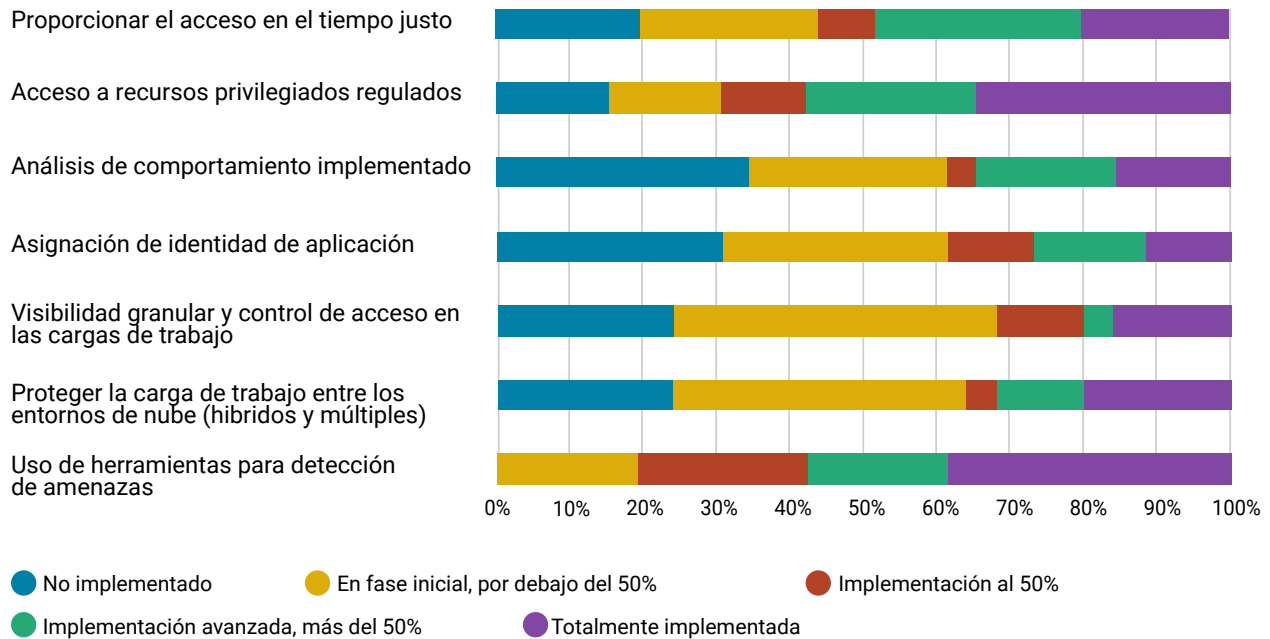


Fig. 8 Listado de controles base para la capa de infraestructura

En este camino de adopción, todas las organizaciones han empleado diversas rutas, bajo el enfoque de consolidar y analizar sus logs, optando por contratar servicios de terceros (SOC, SIEM), para ayudarles con la interpretación y el establecimiento de

estrategias basadas en esta información, con el fin de prepararse para el siguiente salto en la ruta de adopción de nuevas arquitecturas o necesidades del negocio, bajo los entornos cloud y su convivencia con el mundo on premise.

CONTROLES DE LA CAPA DE INFRAESTRUCTURA

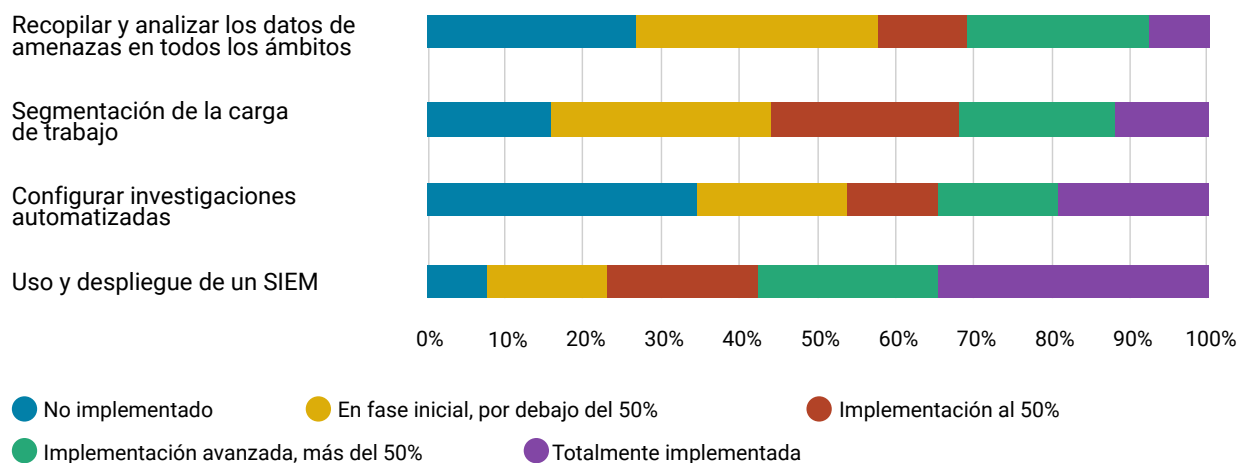


Fig. 9 Controles orientados a mejorar la capa de infraestructura

El deseo de adoptar el modelo Zero Trust aumenta la preocupación de las organizaciones por implementar mecanismos de

automatización que les permitan estar un paso por delante de cualquier evento que pueda ocurrir dentro de sus entornos.

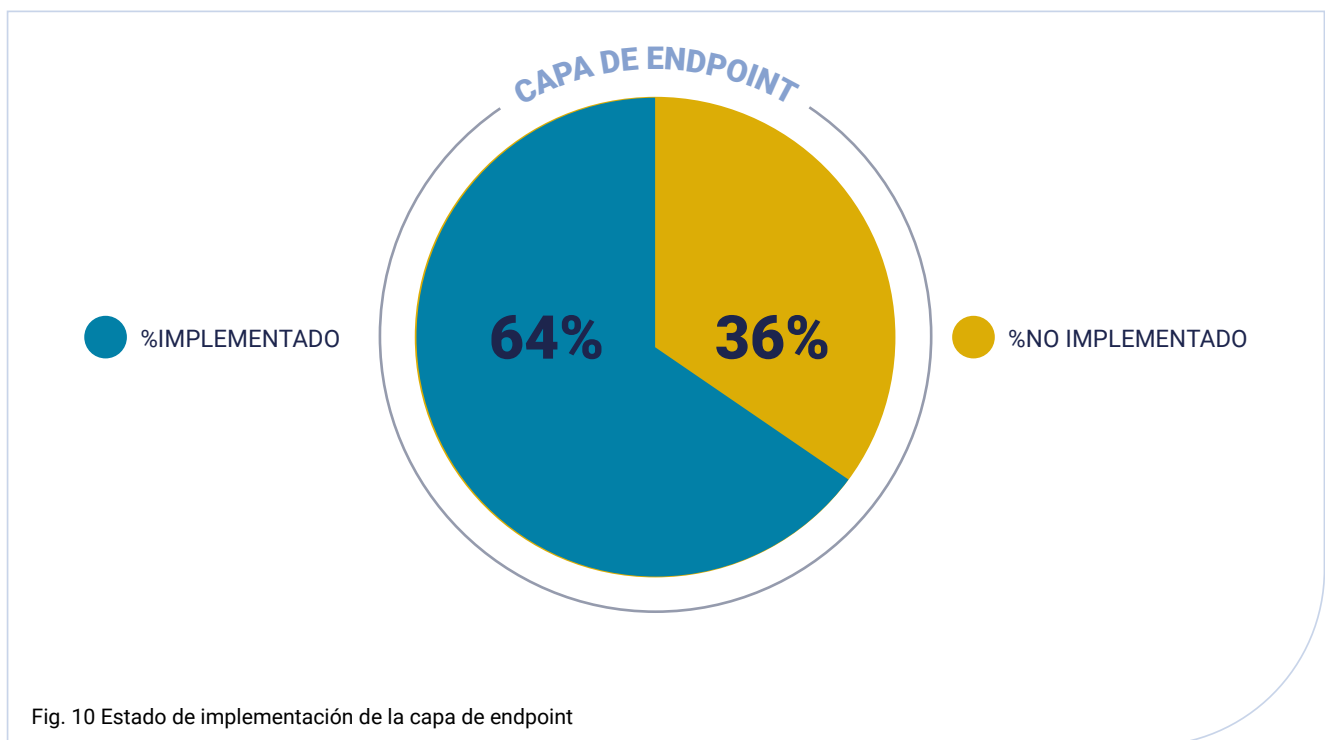
ENDPOINTS

Dentro de la capa de endpoint se considera el nivel de implantación que las organizaciones tienen respecto a:

- Uso de políticas y controles para prevenir la pérdida de datos en todo tipo de dispositivos tanto de usuarios internos como externos,
- El nivel alcanzado en la detección de amenazas y evaluación de riesgos en tiempo real,
- La estrategia que se sigue para gestionar los activos y sus vulnerabilidades en todos los entornos, incluyendo la nube y equipos remotos,

- La forma en que se garantiza el cumplimiento y mejora de postura, antes de conceder el acceso a los recursos de la organización.

Las organizaciones se encuentran en un escenario de constante implementación de estos controles para proteger y monitorear los dispositivos que se encuentran bajo su control, lo que representa un gran esfuerzo, considerando que hoy en día deben sumar, además, aquellos dispositivos que aún no son inventariados, así como los que son considerados externos a ellos. (Fig.10)



La necesidad de brindar mayor facilidad de acceso a los dispositivos y a los múltiples servicios que se ofrecen en la actualidad obliga a las organizaciones a explorar, de forma constante, nuevas alternativas encontrándose con etapas de implementación y despliegue demasiado largos.

De esta forma, los 5 controles de seguridad para la capa de endpoints que consideramos como

más básicos, como media, se encuentran a mitad de implementación.

Por otra parte, se aprecia una mayor prioridad por controlar los dispositivos de personal interno, siendo el control con mayor nivel de adopción. (Fig. 11)

CONTROLES DE LA CAPA DE ENDPOINT

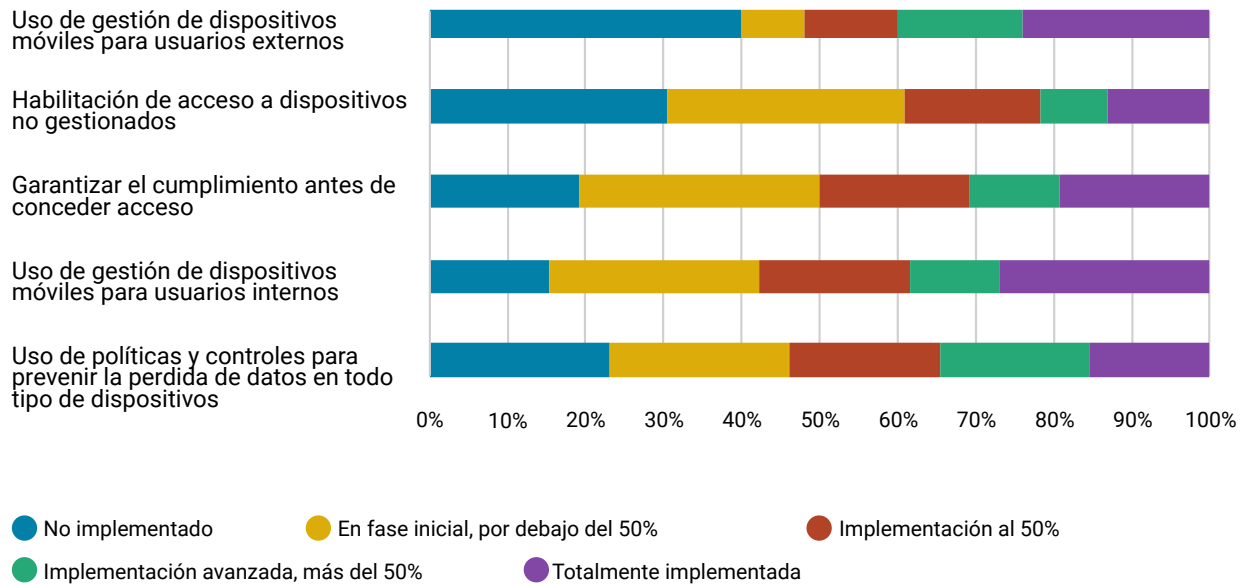


Fig. 11 Listado de controles base para la capa de endpoint

Muchas organizaciones en su afán por escuchar las necesidades de sus clientes y concentrar todos los esfuerzos en su satisfacción, en ocasiones se ven obligadas a dejar de lado las políticas de seguridad y la forma de gestionar los activos del negocio.

Como consecuencia, sus acciones responden en menor medida a la previsión de los posibles escenarios, lo que impacta directamente a los entornos de nube poniendo en alto riesgo la información que se almacena y se procesa en sus diversos ambientes.

Por todo ello, las acciones deben ser inmediatas y deben buscarse estrategias que equilibren la relación entre los requerimientos del negocio y la seguridad.



CONTROLES DE LA CAPA DE ENDPOINT

Gestión de activos y vulnerabilidades en todos los entornos, incluyendo la nube y equipos remotos
Detección de amenazas y evaluación de riesgo en tiempo real

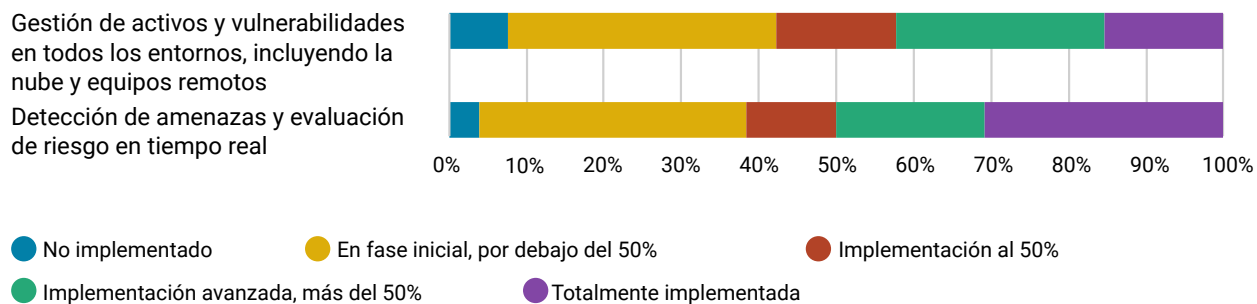


Fig. 12 Controles orientados a mejorar la capa de endpoint

Hay que mencionar también que las organizaciones donde los controles implementados a nivel del endpoint les permiten un nivel de seguridad superior, consideran que la intervención de sus socios estratégicos es muy importante para consolidar su eficacia. De ahí que el análisis del comportamiento de sus usuarios, vaya de la mano con su estrategia de protección, a nivel de esta capa de Zero Trust.



REDES (NETWORK)

Dentro de la capa de redes se considera el nivel de implantación que las organizaciones tienen respecto a:

- Usar controles de acceso como medidas de protección y filtrado en las redes,
- Usar mecanismos de encriptación a nivel de tráfico de red y administración,
- Emplear un análisis integrado, usando sensores y alertas automatizadas,

- Emplear infraestructura como código, en base a modelos de automatización (CI/CD).

La infraestructura de red permite el acceso a todos los datos. Por ello, los controles que se implementan proporcionan una mejor visibilidad y ayudan a frenar la posibilidad de que uno o varios atacantes puedan moverse lateralmente por la red.

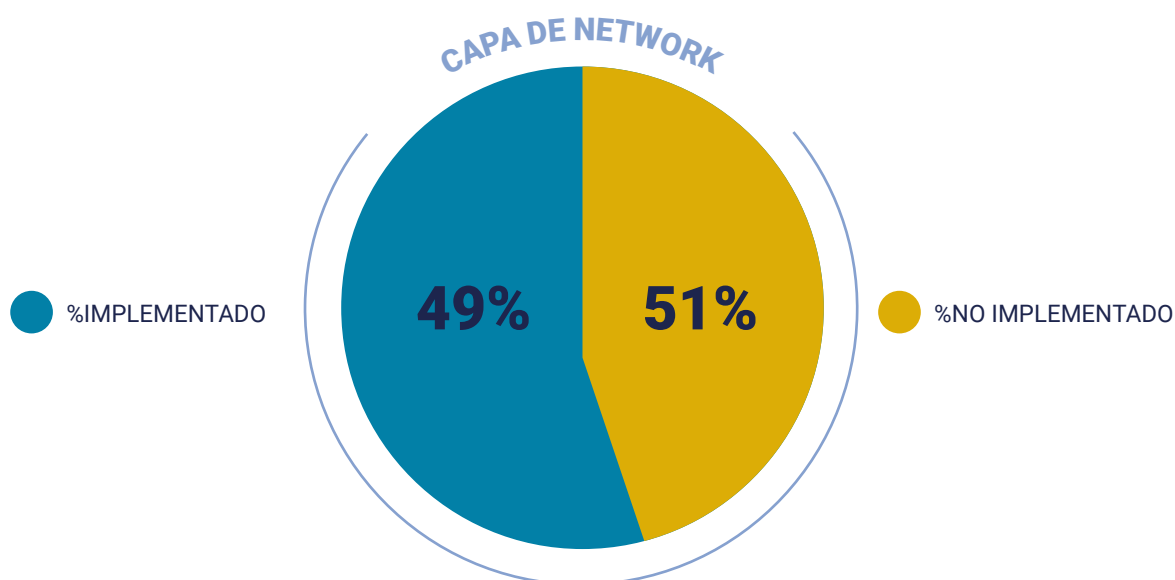
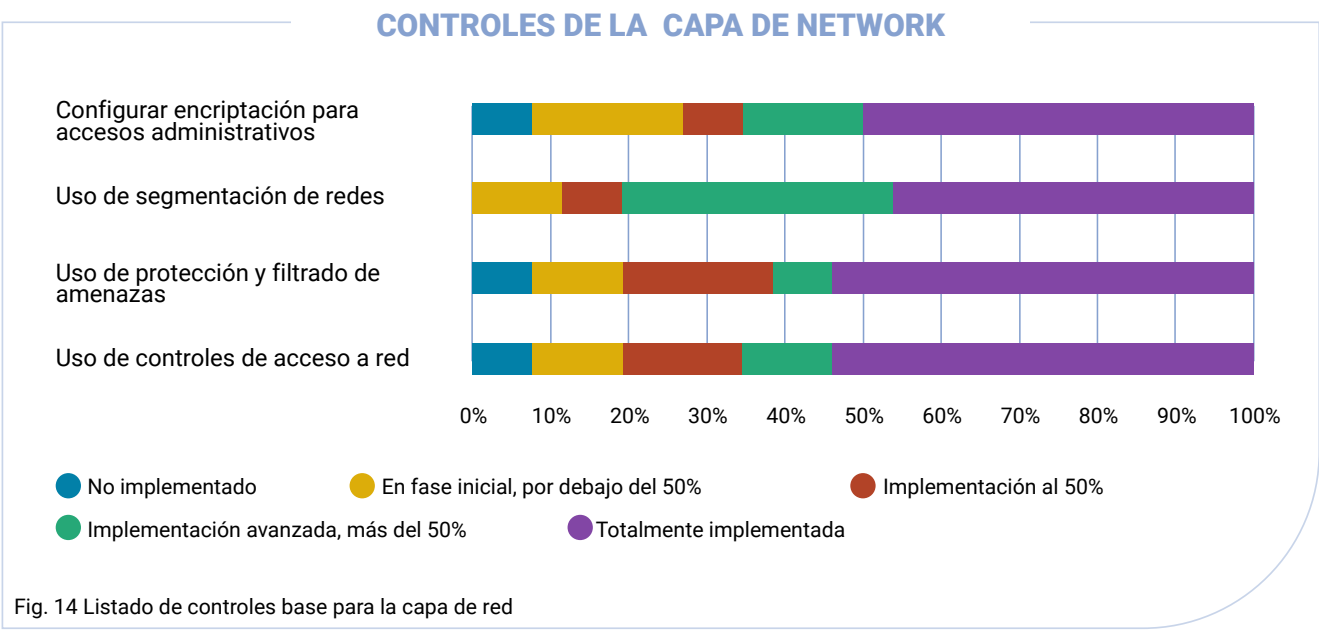


Fig. 13 Estado de implementación de la capa de red

En esta capa se observa un equilibrio entre los controles totalmente implementados y los que se encuentran en proceso de implementación (Fig. 14). Más del 57% de las organizaciones han considerado los esquemas base del mundo on premise y los han llevado al cloud, como parte de su estrategia de adopción, lo que propicia una mejora constante del uso de estos controles como, por ejemplo, aplicar una microsegmentación más profunda dentro de las redes, encriptación de extremo a extremo e incorporar alertas en base a los resultados de monitoreo y análisis.

En otros casos, deben considerarse previamente los atributos de cada dispositivo, como el nivel de parches y la existencia de mecanismos de seguridad incorporados en cada uno de ellos, con el fin de supervisar y establecer las condiciones necesarias, antes de conceder el acceso a los datos existentes en la red.

La implementación de estas mejoras debe incluirse en el roadmap establecido por las organizaciones, como han expresado las participantes en este estudio.



CONTROLES DE LA CAPA DE NETWORK

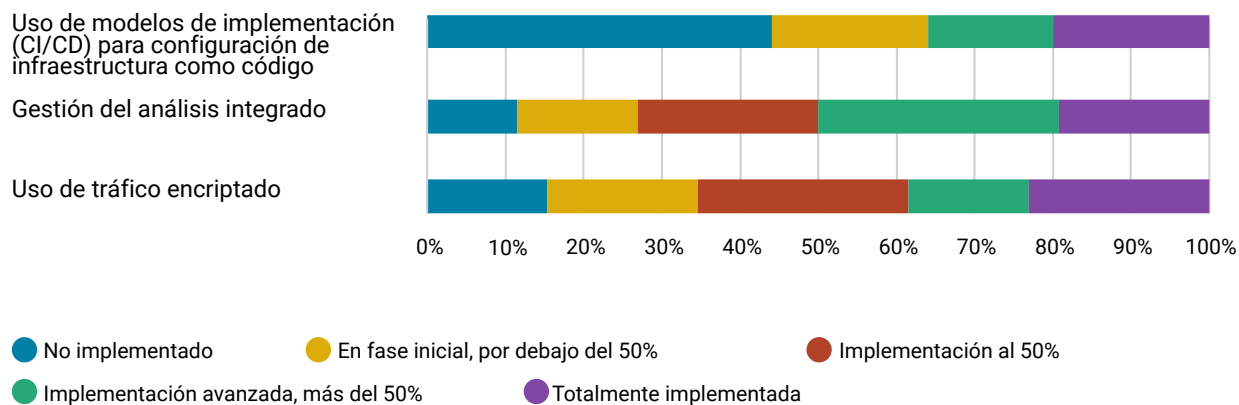


Fig. 15 Controles orientados a mejorar la capa de red

DATOS

Dentro de la capa de aplicación nos hemos interesado por el nivel que las organizaciones han alcanzado respecto a:

- El uso de taxonomías para la clasificación y etiquetado de datos.
- El uso de políticas de seguridad que permitan ejercer una toma de decisiones al momento de conceder o no el acceso a los datos.
- Hacer cumplir los derechos de acceso y uso de datos compartidos fuera de la empresa.
- Uso de cifrado de datos sensibles y su integración con mecanismos de orquestación y automatización para tareas de investigación y respuesta.

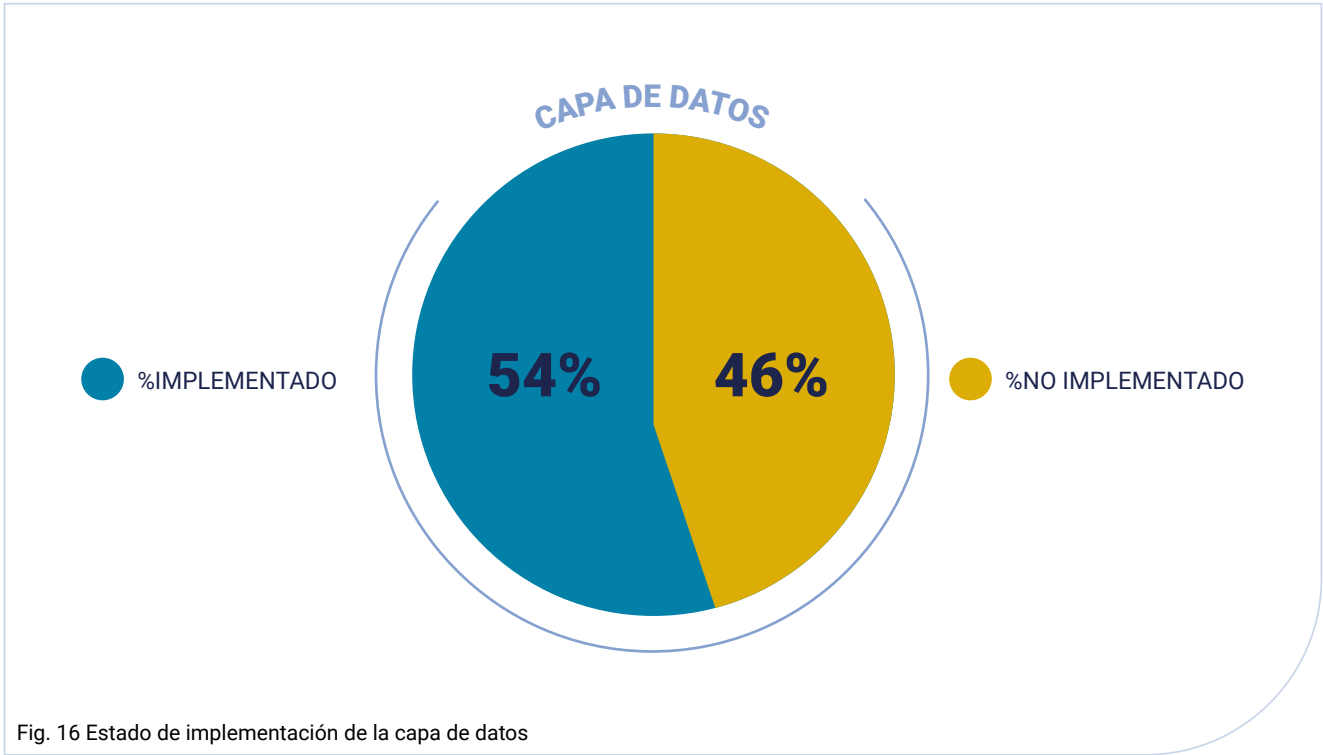


Siendo los datos el principal activo a proteger, las organizaciones incluyen controles para sus ambientes internos, pero no deben olvidar que estos deben permanecer seguros, incluso si se comparten fuera de los dispositivos, las aplicaciones, la infraestructura y las redes. Por ello, es recomendable clasificarlos, etiquetarlos y cifrarlos, con el fin de poder restringir su acceso.

La protección de los datos sigue un proceso de

adaptación propio de la adopción a los entornos del cloud, donde los controles que se aplican pretenden alcanzar un nivel de cobertura adecuado a los numerosos servicios que puede ofrecer la computación de la nube (SaaS, IaaS y PaaS).

Las organizaciones participantes en el estudio indicaron estar aún en una etapa de implementación que esperan finalizar para el año 2024 o 2025 (Fig.16).



La evaluación constante de los riesgos, para contextualizar los datos que se deben proteger, sin olvidar la concienciación de los usuarios en temas de sensibilidad y aplicación de políticas asociadas es de gran importancia para las organizaciones, así como establecer un gobierno de datos que incluya a las tecnologías, los procesos de la organización y las personas, de forma que se pueda garantizar la seguridad y privacidad de los datos.

CONTROLES DE LA CAPA DE DATOS

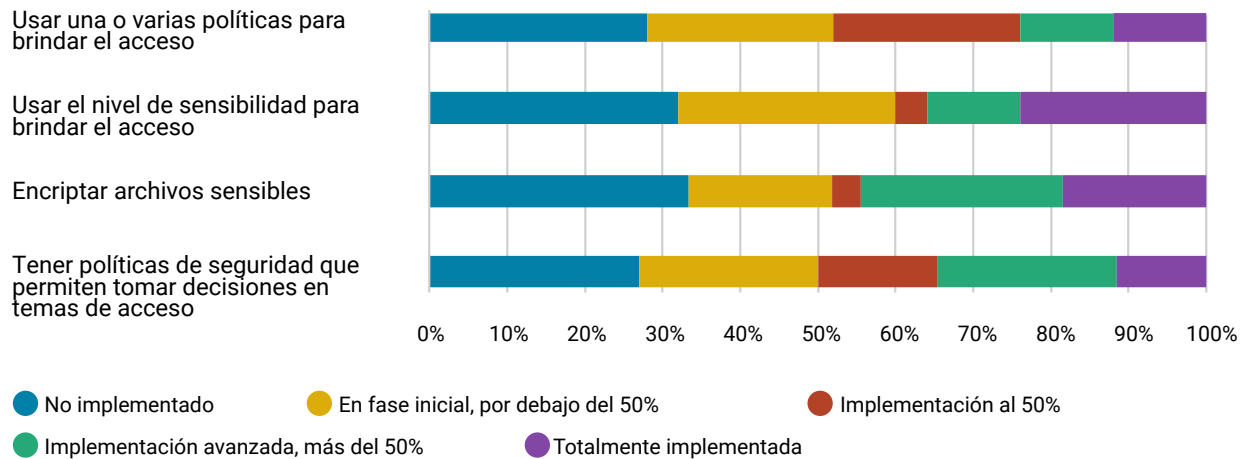


Fig. 17 Listado de controles base para la capa de datos

El uso de plataformas de análisis que permitan un aprendizaje automático para tener una mejor visibilidad de uso de la nube, contribuye a que las organizaciones puedan adaptar de una forma más rápida y fácil sus controles y políticas.

Una parte de la estrategia a seguir en la capa de datos, podría considerar la optimización y ajuste de las necesidades en función de los cambios del negocio.

CAPA DE DATOS

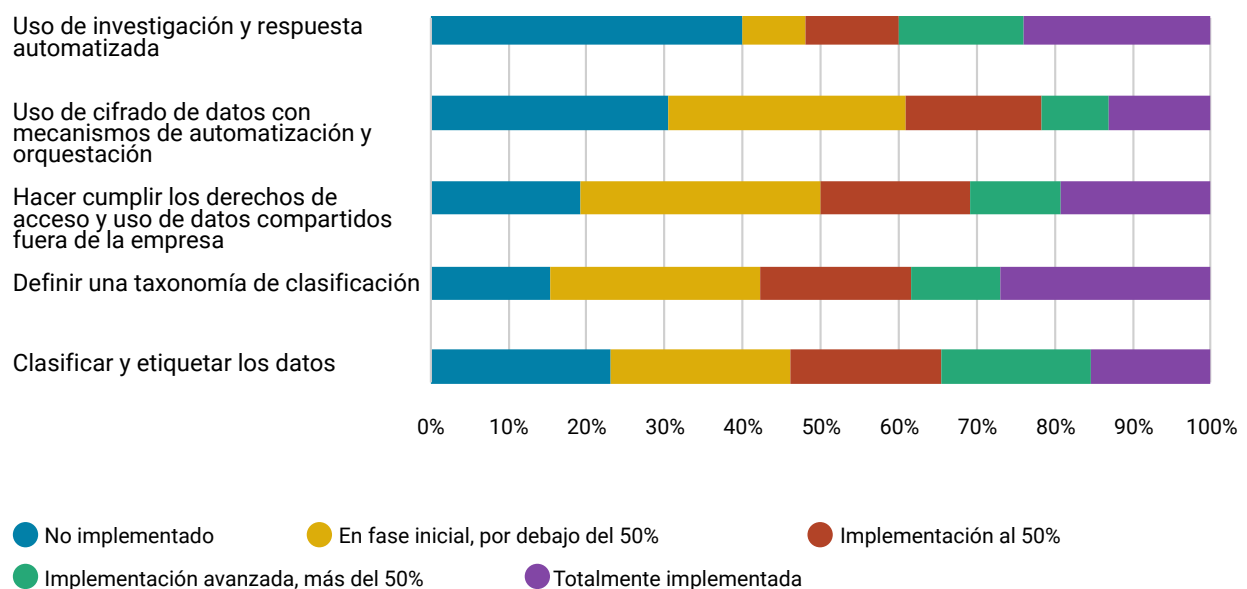


Fig. 18 Controles orientados a mejorar la capa de datos



BENEFICIOS Y BARRERAS

Además de realizar una revisión de la adopción de los controles de seguridad de cada una de las capas del modelo ZERO TRUST, se consultó a las

organizaciones participantes sobre los principales beneficios y barreras de la adopción del modelo. v

BENEFICIOS DEL ZERO TRUST

Sobre los posibles beneficios del modelo Zero Trust, los participantes seleccionaron los 5 beneficios percibidos como más relevantes para su organización.

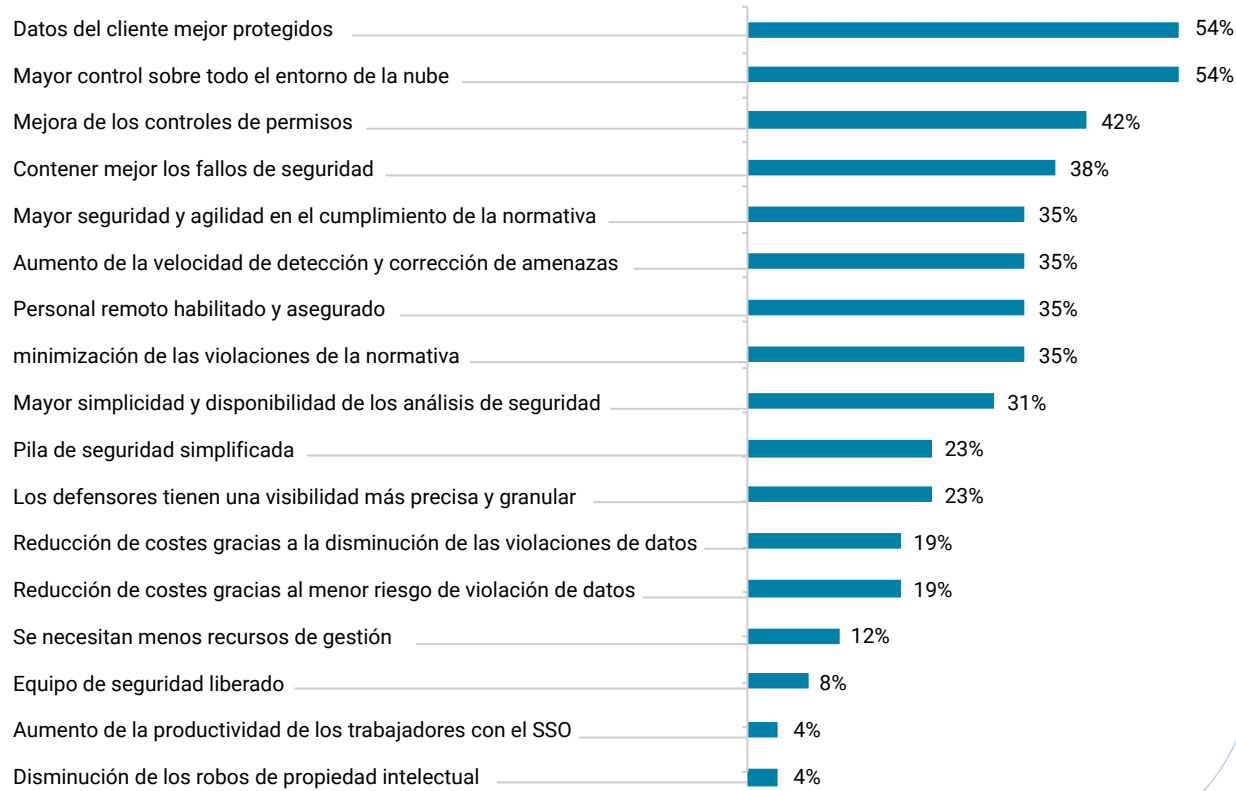
Más de la mitad de los participantes otorgaron uno de sus votos a tener un mejor control sobre el entorno del cloud, y a proteger de forma adecuada los datos del cliente.

La mejora de los controles de permisos y la contención de forma efectiva de los fallos de

seguridad que se puedan presentar en los entornos del cloud, resultaron el tercero y cuarto beneficio mejor percibidos.

El quinto lugar fue compartido por cuatro beneficios: la mayor seguridad y agilidad en el cumplimiento de la normativa, el aumento de la velocidad de detección de amenazas, la seguridad del personal remoto y la minimización de las violaciones de la normativa.

CONTROLES DE LA CAPA DE DATOS



BARRERAS PARA LA ADOPCIÓN DEL ZERO TRUST

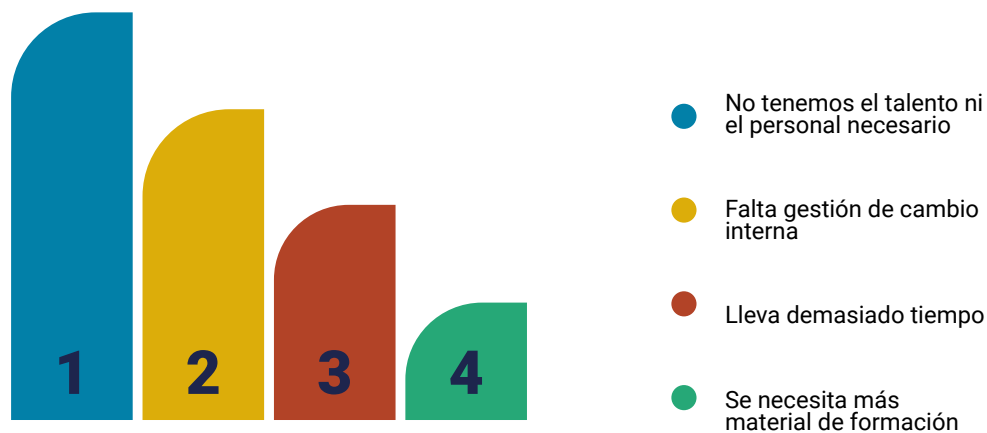
En la adopción del modelo Zero Trust, las organizaciones identificaron las principales barreras tomando en cuenta cinco aspectos:

Talento (o equipo), liderazgo, tecnología, partners y restricciones presupuestarias.

Por cada aspecto, los participantes del estudio ordenaron los factores de más impacto en la adopción.

TALENTO

BARRERAS DEL ZERO TRUST A NIVEL DE TALENTO

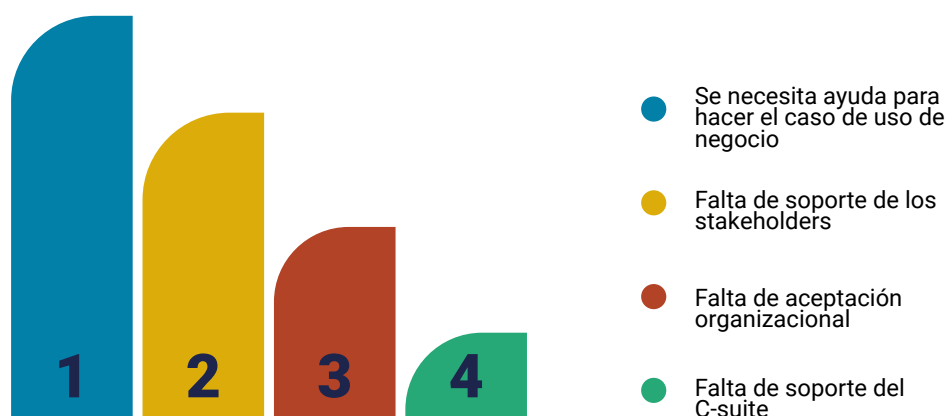


La principal barrera identificada es que no todas las organizaciones disponen de un equipo de ciberseguridad especializado en los entornos del cloud. Más del 60% de los participantes están

buscando este perfil en el mercado, o en proceso de formación del equipo dentro de la propia organización.

LIDERAZGO

BARRERAS DEL ZERO TRUST A NIVEL DE LIDERAZGO

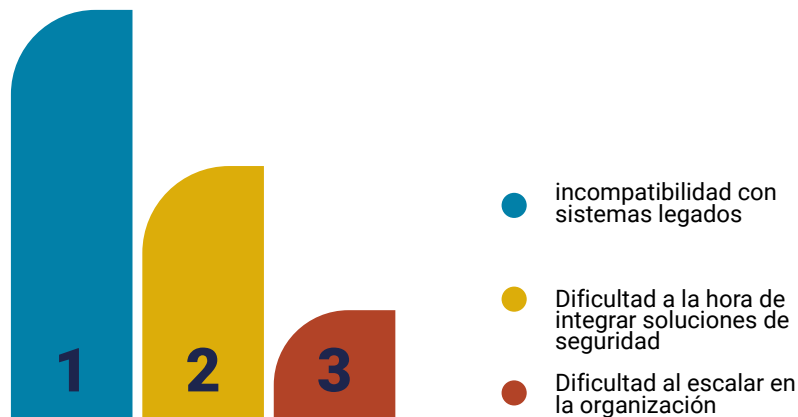


En cuanto al liderazgo, el 88% de los participantes conoce el modelo de Zero Trust, ya sea por interés propio o por el apoyo constante de sus socios estratégicos (partners) y la exploración de estas

nuevas tendencias, pero encuentran dificultad para establecer una estrategia de adopción rentable y medible en su organización.

TECNOLOGÍAS

PRINCIPALES BARRERAS A NIVEL DE TECNOLOGÍAS



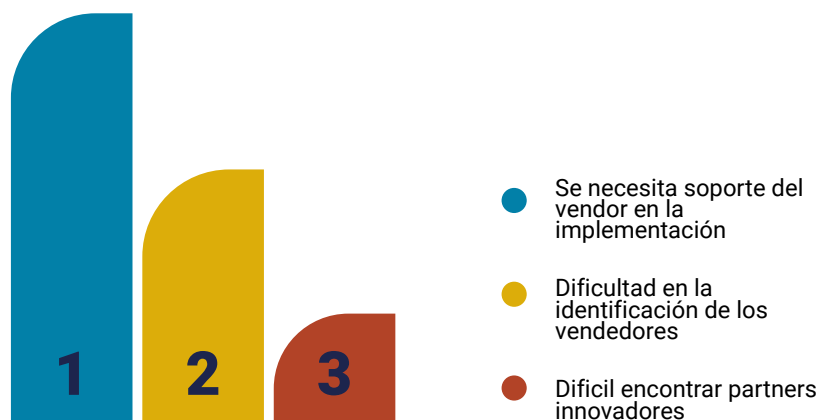
El 69% de las organizaciones afirman tener servicios disponibles en el cloud y consideran seguir evolucionándolos. En la mayoría de los casos se comienza con servicios de carácter colaborativo para posteriormente explorar otras alternativas, como almacenamiento o soluciones

de gestión de identificación y autenticación. Este avance dificulta la adopción de Zero Trust dentro de su organización.

La principal barrera percibida sin embargo es la incompatibilidad con los sistemas legados.

PARTNERS

BARRERAS DEL ZERO TRUST A NIVEL DE ALIADOS/PARTNER



Para implementar Zero Trust es necesario combinar los conocimientos en infraestructura y redes de una organización, así como su apetito de riesgo. Para esta implementación, las organizaciones se apoyan en sus socios estratégicos (partners), un aspecto que puede apreciarse como una barrera en la evolución.

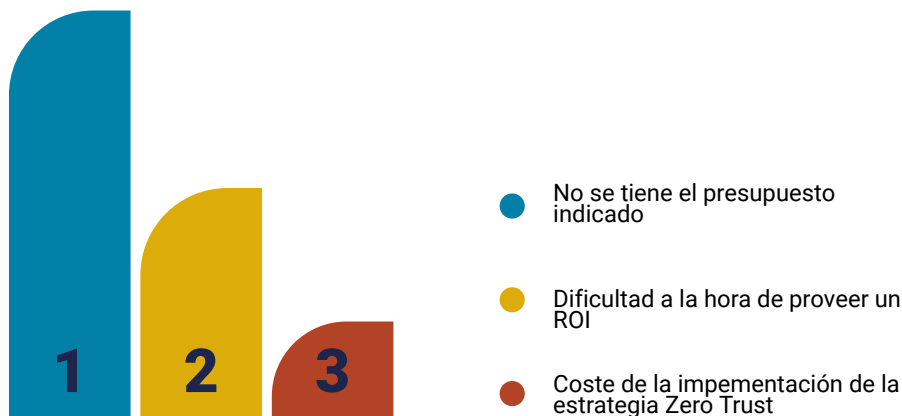
En la medida que las organizaciones hacen responsables a sus socios estratégicos con guiar

el camino de la adopción, reducen quizás de manera inconsciente, su responsabilidad con la toma de decisiones y el enfoque de cada uno de sus procesos y alineación con los objetivos del negocio.

En este escenario, el largo plazo y los escasos presupuestos hacen poco alentador el uso de Zero Trust.

PRESUPUESTOS

BARRERAS DE ZERO TRUST
A NIVEL DE PRESUPUESTO



La mayoría de las organizaciones participantes en el estudio, coinciden en señalar como una de las

barreras importantes en la adopción de Zero Trust el problema presupuestario.

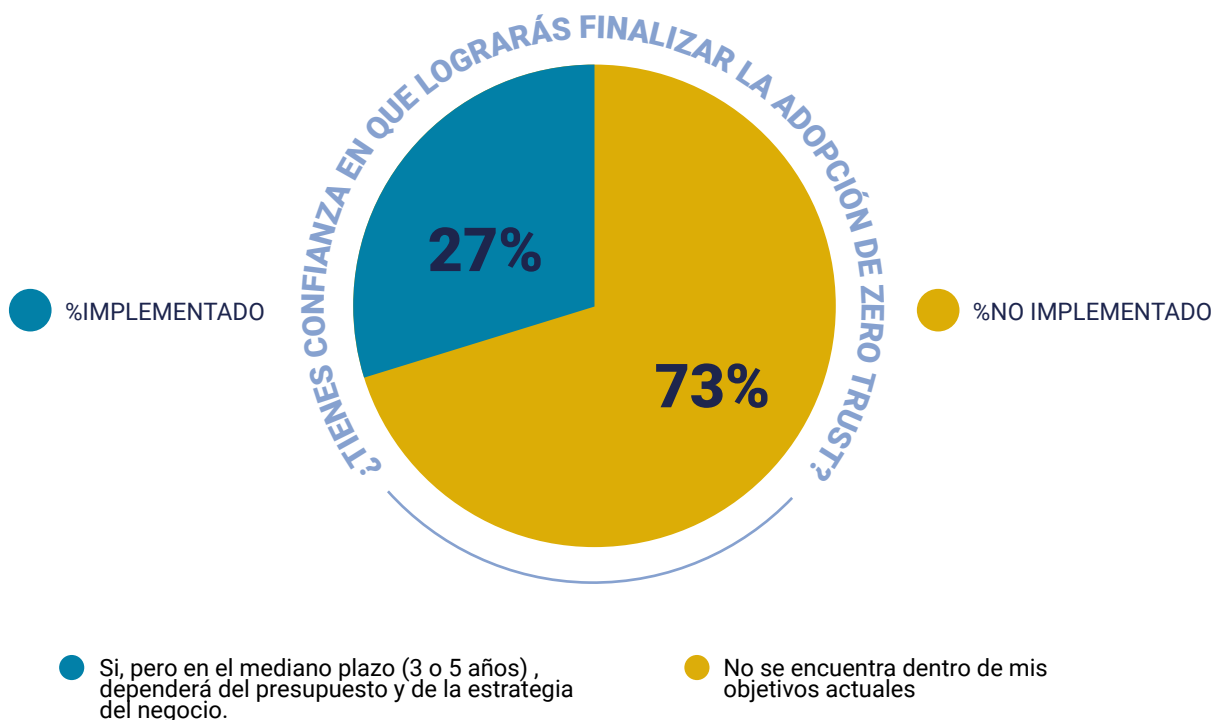
Y QUÉ NOS DEPARA EL FUTURO

Teniendo en cuenta que están llegando nuevas tecnologías que seguirán generando disrupción en el mercado, el camino de la adopción de Zero Trust se percibe como desafiante.

región están implantando el modelo, avanzando con él, y confían en finalizar su adopción en el medio plazo, lo que pone de manifiesto la aceptación de la seguridad como driver de la sostenibilidad de las organizaciones.

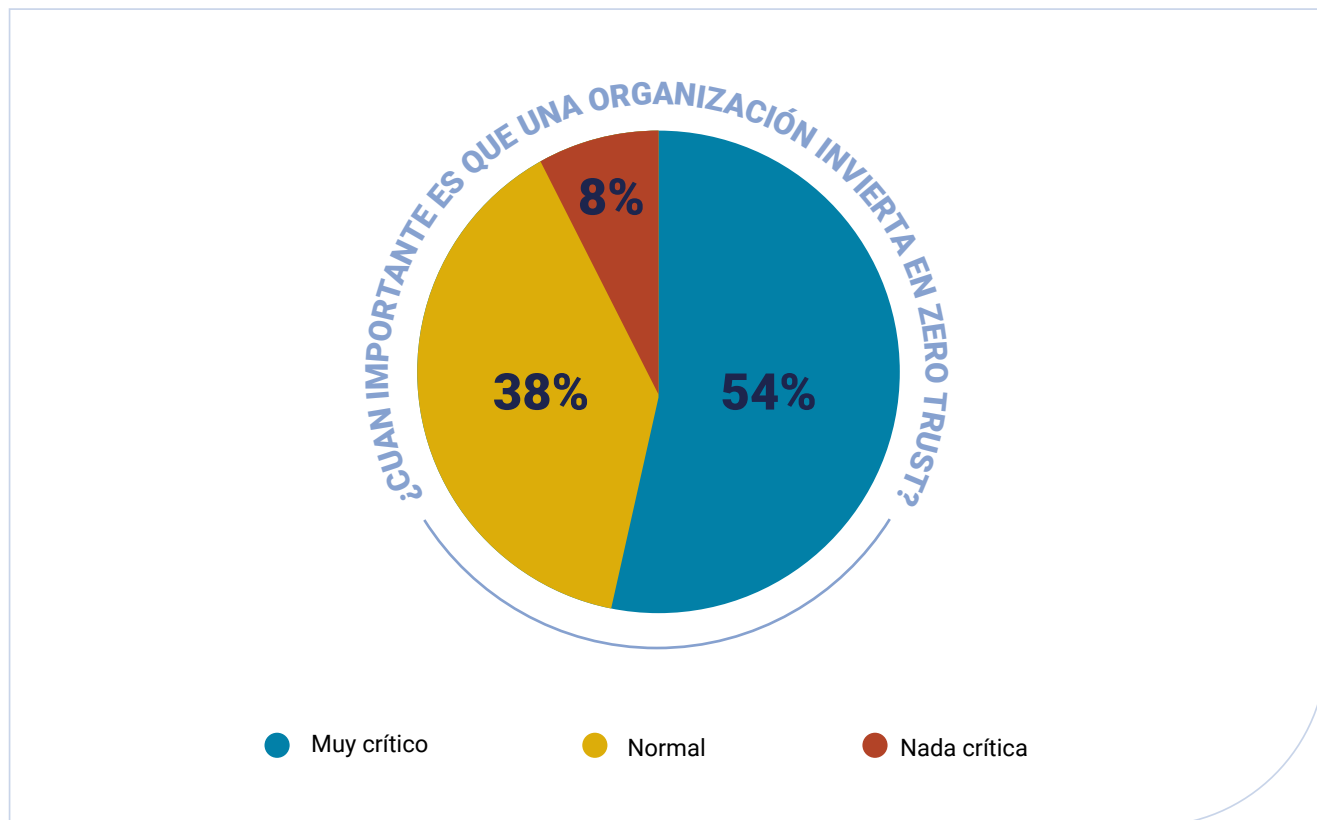
Sin embargo, las grandes organizaciones de la

No obstante, la escasez de talento y la falta de



inversión se perfilan como las principales barreras. Si bien el talento debe promoverse a través de la educación formal (cursos y universidades), las organizaciones pueden impulsar el desarrollo y formación interna de sus profesionales.

Por otra parte, la construcción de casos de negocio puede estimular un aumento del presupuesto, junto a la convicción de la criticidad de esta inversión para la seguridad, lo que en la actualidad solo es percibido por un 54% de las organizaciones participantes.



Finalmente, la obsolescencia debe tratarse con planes de transformación integrales, considerando que algunas organizaciones mantienen servicios altamente críticos en sistemas obsoletos. Solo una buena planificación puede eliminar la obsolescencia, abriendo la posibilidad de llevar esos servicios a la nube.



NUESTRA VISIÓN



Zero Trust no es un producto o una plataforma; tenemos que entenderlo como un marco de seguridad de "nunca confiar, siempre verificar", bajo el escenario de que "algo está pasando".

Las organizaciones participantes del estudio entienden que Zero Trust no puede ser comprado como producto, porque esto les llevaría a un posible fracaso y a no estar preparadas ante un ataque cibernético.



NTT DATA promueve que las organizaciones tengan entornos de trabajo adecuados para permitir una total flexibilidad ante los diferentes estilos de trabajo, sin restringir a los usuarios por su ubicación, como la oficina o el hogar, o por tipo de dispositivo. En el viaje hacia la implantación del modelo Zero Trust en la propia compañía en el 2018, casi dos años antes de la pandemia, los líderes de seguridad global de NTT DATA no solo aceptaron este desafío, sino que se impulsaron entre sí, para encontrar nuevas formas de enfrentarlo.

Según Markus Künzler, CISO de EMEA en NTT DATA EMEA Ltd,

Ahora es casi una competencia amistosa entre nosotros, todos tratando de encontrar ideas innovadoras y nuevas técnicas y formas de enfrentar los desafíos. Hay un espíritu real de la comunidad global cuando se trata del programa Zero Trust de NTT DATA.





Como NTT DATA hemos aprendido muchas lecciones en nuestro viaje Zero Trust que no son negociables y pueden aplicarse a cualquier organización que busque seguir nuestro camino, como por ejemplo:

- El liderazgo y patrocinio son esenciales para poder afrontar las barreras que surgirán dentro de la organización. Los líderes deben estar alineados desde el principio y asegurarse de que su equipo esté de acuerdo con ese destino es fundamental.
- Las tecnologías deben integrarse correctamente. Para aplicar Zero Trust se necesita una gran cantidad de soluciones tecnológicas de seguridad y de negocios que trabajen juntas para enviar y recibir las señales de seguridad necesarias a través de varios puntos de control.
- Mantener una comunicación clara con los usuarios. No importa qué tan bien diseñada podamos tener la ruta de Zero Trust; son los usuarios los que perciben los cambios y debemos asegurar que se sientan incluidos y educados en el cambio de comportamiento.
- Se debe trabajar la gestión del cambio. Los colaboradores deben sentirse incluidos en este camino y comprender las razones por las que se les pide un cambio de comportamiento. No es suficiente decirles el "qué", sino que también debe dárseles un "por qué" significativo.
- No es un camino que se recorre una vez; surgen nuevas amenazas y tecnologías, por lo que cada año hay que replantearse como evolucionar el enfoque de Zero Trust escogido para la organización.



No tomar en cuenta cualquiera de estas lecciones conduciría a una falla, o al menos, comprometería la arquitectura.

NTT DATA considera que los ataques cibernéticos de hoy en día son cada vez más sofisticados y complejos siendo un riesgo para la gestión de los entornos del cloud. Por ello, será necesario realizar siempre una revisión del gobierno de seguridad a todos los niveles, para disponer de una arquitectura de "confianza cero".

La experiencia, nos permite establecer la ruta que toda organización debe seguir, a través de un servicio integral que abarca la consultoría, la

implementación y la operación de la arquitectura.

Junto a empresas asociadas estratégicas, con una amplia trayectoria a nivel mundial en una amplia gama de campos técnicos, NTT DATA ha creado una estructura con más de 1000 especialistas capaces de apoyar a las organizaciones en este camino de Zero Trust.

@ maria.pilar.torres.bruna@nttdata.com

CONTACTO



ESTADO DE LA ADOPCIÓN DE

ZERO TRUST

EN LATINOAMÉRICA

NTT DATA

Microsoft