



Consultoría de identidad híbrida Entra ID y AD DS



DATOS QUE APOYAN LA SEGURIDAD DEL CLOUD

La protección de la identidad sigue siendo el mayor motivo de preocupación en las empresas y sus equipos, pero también es la mayor oportunidad para mejorar su seguridad.

- La cantidad de ataques de contraseña aumentó en un número estimado de 921 ataques por segundo en 2022, un aumento del 74 % desde 2021.
- Los actores de amenazas se están volviendo más creativos para eludir la autenticación multifactor (MFA).
- Los atacantes obtienen, frecuentemente, acceso a cuentas de terceros u otras cuentas altamente privilegiadas conectadas a una organización. Luego, usan esas credenciales para infiltrarse en la nube y robar datos.

CONSECUENCIAS DE UNA MALA GESTIÓN DE IDENTIDAD

01

Tiempo de inactividad del usuario

02

Tiempo de corrección

03

Daño a la reputación

04

Pérdida de propiedad intelectual

05

Pérdidas monetarias directas

06

Multas de cumplimiento

07

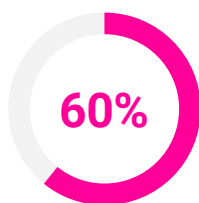
Costos de respuesta y remediación

08

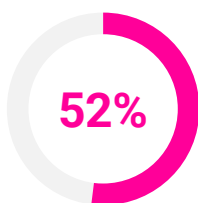
Pérdida de ingresos y clientes

09

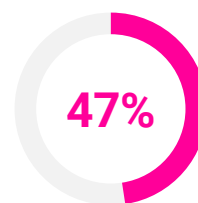
Honorarios legales



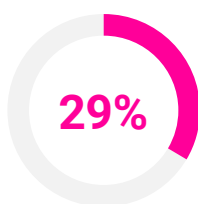
Datos perdidos



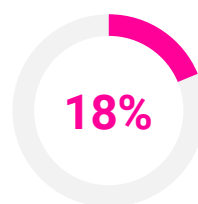
Cuentas o credenciales comprometidas



Infecciones de ransomware



Infecciones de malware



Pérdida financiera

VENTAJAS DE SABER GESTIONAR LA IDENTIDAD



Seguridad

Es destacable el aumento considerable del nivel de seguridad que se produce en el entorno.



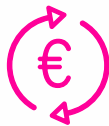
Facilitar procesos

Gracias a la gobernanza y organización de la identidad los procesos realizados con esta se simplifican en gran medida.



Cumplimiento

Hoy en día la importancia de la identidad llega a ser exigida en las certificaciones como ENS o ISO27001.



Ahorro de costes

Es cierto que la seguridad supone un esfuerzo mayor por parte del departamento IT, tanto en conocimientos como en procedimiento, pero está demostrado que a la larga el ahorro de costes es mayor.



Gobernanza y organización

Conocer y saber trabajar la identidad permite controlar y gobernar el parque de equipos y usuarios.



Tranquilidad

No hay nada como saber que tienes un equipo formado con las herramientas necesarias para ayudarte a estar protegido.

LA IDENTIDAD ES EL NUEVO CAMPO DE BATALLA

Existe un desajuste peligroso entre los protocolos de seguridad de la mayoría de las organizaciones y las amenazas a las que se enfrentan. Tradicionalmente los atacantes intentaban forzar su entrada en las redes rompiendo la seguridad perimetral, su táctica preferida ahora es más simple: **atacar la identidad del usuario.**

Los métodos son conocidos y variados, ingeniería social, fuerza bruta, phishing... amenazas con las que estamos familiarizados, pero todavía en muchas empresas no se aplica el esfuerzo necesario para **mitigar estos agujeros de seguridad.**

Desde Nunsys Group tenemos claro cómo **ayudar a nuestros clientes a proteger sus identidades** desde la posición más básica de la seguridad en los entornos tradicionales.

- En cuanto al **usuario**: acceso condicional, MFA o normativa de contraseñas y de bloqueo de cuenta.
- En la **seguridad en el dispositivo** de trabajo: Microsoft Intune, LAPS y plataformado seguro de equipos y navegadores.
- La protección del **acceso administrativo**: PIM, Modelo de tiers de Microsoft y Administración de cuentas de servicio (GMSA).

Implementando correctamente estas medidas de seguridad damos un giro 360 a la seguridad del usuario, todas ellas aplicadas con herramientas y **buenas prácticas de Microsoft** y bajo el marco de trabajo del **Esquema Nacional de seguridad.**

IDENTIDADES HÍBRIDAS Y CLOUD

Para las **identidades híbridas o en la nube**, el sabor es otro. Debido al cambio y evolución constante de las herramientas **Cloud de Microsoft**, resulta esencial formar a nuestros clientes y explicarles las nuevas funcionalidades.

Momento Clave

Empezar con una formación específica para empezar a trabajar con las identidades de **Microsoft Entra ID** y cómo utilizar las **herramientas de IAM** que ya ofrece Microsoft. Donde además de aprender a funcionar, enseñamos las claves para mantener nuestra infraestructura de identidad híbrida o solo en nube segura.

PONEMOS A TU DISPOSICIÓN NUESTRO SERVICIO DE CONSULTORÍA

Nuestro servicio de consultoría de identidad híbrida Entra ID y AD DS pone al servicio del cliente nuestro expertis en este campo, ofreciendo nuestro conocimiento técnico y de valor sobre la seguridad de la identidad, ¿En que consiste?

Entrevista y estudio de la infraestructura

Una toma de contacto para aterrizar y conocernos.

Inspección manual y con herramientas de Entra ID y AD DS

Evaluamos el estado del entorno y las herramientas.

Capacitación de Entra ID para el equipo TIC

Formación específica para trabajar con la herramienta cloud de Microsoft Entra ID.

Entrega de informe de resultados

Elaboramos y entregamos un informe con puntos de mejora para empezar a trabajar.

Definición de acciones a realizar

Escuchamos la trayectoria y proyección del cliente para diseñar un plan de acción.

Alianza como partner de identidad

A partir de este momento el cliente es capaz de depositar la confianza de la gestión de la identidad en nosotros para estar a la vanguardia y conocer y aplicar las últimas novedades de la tecnología.



CONFÍA EN NUNSYS GROUP, PARTNER CON LA MÁS ALTA CERTIFICACIÓN DE MICROSOFT CLOUD IDENTIDAD

Nunsys Group es el aliado en la seguridad de la identidad. Podemos poner en marcha proyectos tanto sencillos como complejos, que acerquen a nuestros clientes a dominar la gobernanza de la identidad, enfocándonos tanto en medidas más sencillas como LAPS, en otras más complejas como securización de cuentas de servicio o PasswordLess o proyectos avanzados de IAM, PAM o IGA.



Si quieres conocer como te podemos ayudar para llegar a la meta del gobierno de la identidad mediante los servicios de **Consultoría híbrida de Entra ID y AD DS** ponte en contacto con nosotros.



Esteban Rueda Pérez
Comercial
Gerente de Negocio Modern Workplace

esteban.rueda@nunsys.com



nunsys
GROUP[®]

960 500 631

www.nunsys.com

info@nunsys.com