Identity & Access Management – Adelántate al robo de identidades en tu empresa

Sobre esta guía:

Esta guía está pensada para responsables de TI, CIOs y ejecutivos que necesitan una solución para la gestión de identidades y accesos.

Identity & Access Management

El acceso y la identidad de los usuarios en las empresas se han convertido en uno de los activos digitales más importantes. La gestión de identidades y el proceso de adquisición de roles de acceso es uno de los temas más resaltantes entre los CIOs de las grandes empresas.

La presidenta de HP Inc., Helena Herrero (2017), destaca cómo muchos responsables de TI se centran exclusivamente en la seguridad de los ordenadores, servidores y dispositivos móviles, una fórmula que ya se está quedando obsoleta. Esto se debe a que la nueva puerta de entrada de los ciberataques está orientada hacia los dispositivos conectados, afectando principalmente los que están dentro del compendio del Internet de las Cosas (IoT).

En esta guía vamos a tratar los puntos más relevantes del **Identity & Access Management** (IAM): el contexto actual de la seguridad digital, los desafíos a los que se enfrentan los responsables de área de TI y el funcionamiento de las categorías de soluciones interrelacionadas.

Esta **guía** está pensada para responsables de TI, CIOs y ejecutivos que necesitan una solución para la gestión de identidades y accesos.

Tabla de contenidos

1. El Contexto 4

1.1 El mercado de la seguridad digital 4
1.2 Seguridad en la nube 5
1.3 Empresas pequeñas y medianas bajo amenaza 5
1.4 Tendencias en seguridad digital 6

2. El reto 7

2.1 Desafío para el CIO 7
2.2 Pérdida de productividad y calidad 7
2.3 Shadow IT 8
2.4 La brecha de identidad 8

3. La Solución 9

3.1 Identity Access Management (IAM) 10
3.2 Usabilidad IAM 11
3.3 WS02 Identity Server 12

4. Conclusiones 14

1. El Contexto

Hace más de una década la tecnología se transforma con una tasa de crecimiento muy acelerada. En la década de los 80´solo unos cuantos usuarios tenían el privilegio de acceder a las computadoras. Pero en los siguientes años el acceso fue expandiéndose y las empresas comenzaron a tener más ordenadores/computadoras y más sistemas informáticos.

La gestión de los datos en los sistemas y en los procesos de negocio llevó a replantearse el acceso a dichos sistemas. El cuidado de la información y la salvaguarda de los datos se convirtieron en un tema crítico dentro de las organizaciones.

Es en este momento cuando surgen regulaciones por parte de gobiernos y estándares de seguridad por parte de las empresas para la protección de datos.

1.1 El mercado de la seguridad digital

Muchas empresas al enfrentarse a una transformación digital inminente y al tener que migrar sus aplicaciones críticas de negocio a la nube, se llenan de dudas y se frenan ante la seguridad de estos modelos de gestión.

La garantía de la seguridad de los datos e identidades es una de las principales preocupaciones de las empresas, sobre todo por las claves de negocio que se puedan albergar. Además, una nueva Ley Europea de Protección de Datos hace que todas las empresas que operen con cualquier país de la UE se vean afectadas por la normativa.

Gartner, consultora especialista en tecnologías de la información, previó que los servicios de seguridad que se basan en la nube aumentarían un 21% en 2017, alcanzando el valor en conjunto de 9.000 millones de dólares en 2020. Mientras los atacantes mejoren sus estrategias y robos, las empresas deben estar al tanto y mejorar sus capacidades de seguridad. De allí el crecimiento del mercado de la seguridad digital.

> *“Gartner, consultora especialista en tecnologías de la información, previó que los servicios de seguridad que se basan en la nube aumentarían un 21% en 2017, alcanzando el valor en conjunto de 9.000 millones de dólares en 2020.”*

Es así, que los CIOs y responsables TI son los líderes de la seguridad de los sistemas de la empresa. Deben estar comprometidos con la evaluación constante de los niveles de seguridad del negocio y estar al tanto de la última tecnología.

Para ataques avanzados, prepárate con la tecnología adecuada

2.2 Seguridad en la nube

En 2016 se registraron más de 160 grandes brechas de seguridad en compañías relevantes en España. Esto supuso un gasto de 9,5 millones de dólares (Dealerworld, 2017). Hoy más que nunca se hace necesaria la protección de los dispositivos conectados y las identidades con las que las personas acceden a las diferentes aplicaciones. Además, uno de los principales problemas a los que se enfrentan los directivos es que el vector de ataque se transforma y cambia rápidamente.

> *"En 2016 se registraron más de 160 grandes brechas de seguridad en compañías relevantes en España."*

La migración hacia la nube ya es un hecho por lo que crece la demanda por aumentar los niveles de seguridad en dicho espacio. Por este motivo, se establece como uno de los mercados con mayores oportunidades.

Tres características que hacen que las empresas consideren su seguridad:

- Crecimiento vertiginoso de ciberataques a empresas
- Robo de datos
- Aumento de las vulnerabilidades

2.3 Empresas pequeñas y medianas bajo amenaza

Uno de los mitos que sostiene el mundo de la seguridad digital es que los ciberataques solo ocurren a las grandes organizaciones. Pero esto no es del todo cierto, porque el mercado de la seguridad ha visto un impulso gracias a las empresas pequeñas y medianas.

En 2017 los servicios de seguridad basados en la nube pretenden alcanzar un crecimiento mundial de 5.900 millones de dólares según Gartner. Según la revista especializada Dealerworld, este dato es muy relevante ya que situaría el mercado de la seguridad en la nube por encima del mercado total de seguridad de la información.

Otro punto importante por resaltar, es que las empresas de nueva creación como las pymes o las startups, demandan soluciones ágiles con características simplificadas. Buscan soluciones con modelos de entrega atractivos y que ofrezcan la seguridad adecuada para sus modelos de negocios.

Podemos enumerar tres factores clave por la que aumenta la preocupación de las empresas por la seguridad en la nube:

- Aumentan las amenazas a la seguridad empresarial
- El personal de las empresas demanda mejoras en los servicios de gestión
- Mayores beneficios operacionales y de costes.

2.3 Tendencias en seguridad digital

Los analistas vislumbran que los principales nichos de servicios de seguridad basados en Cloud con mayor éxito y escalabilidad son el Security Information and Event Management (SIEM) y el **Identity Access Management** (IAM) como **tecnologías emergentes.**

SIEM es una tecnología que combina dos productos de seguridad dispares: SIM (Security Information Management) y SEM (Security Event Manager). Es una solución que analiza y prioriza eventos de seguridad dentro de la red. Proporciona de esta manera un análisis a tiempo real de alertas de seguridad generadas por el hardware y el software de red.

El IAM, tema central de esta guía, es una tecnología usada para automatizar la gestión de identidades de los usuarios y los permisos de acceso.

Los expertos apuntan que los servicios emergentes como SIEM e IAM son los que ofrecen un crecimiento potencial muy significativo para las empresas. Sin embargo, es interesante apuntar que según las previsiones de Gartner, los productos comprendidos dentro del segmento de los **Identity Access Management** son los de mayor crecimiento para los próximos 3 años.

IAM es un producto tecnológico englobado dentro de las Identity & Access Management as a service (IDaaS).

2. El reto

Es común encontrarse con el caso de que, si todo funciona, las áreas de TI no son tomadas en cuenta pero si algo va mal, son estas áreas el ojo del huracán.

2.1 Desafío para el CIO

Los problemas graves que pueden acaecer como la suspensión de un servicio tecnológico, suelen tomarse en primera instancia. Estos problemas traen consigo la pérdida de confianza de la empresa en los servicios TI. Convirtiéndose así en un problema principal para los CIO: la confianza en los servicios que proporciona.

Además, a esto hay que sumarle que el inconveniente más común que tiene el personal de TI es particularmente la administración de identidades según contraseñas y los privilegios de acceso de los usuarios.

Las empresas se encuentran actualmente utilizando múltiples sistemas, estos sistemas tienen una gran multitud de usuarios e identidades, que se traducen en múltiples contraseñas y distintos privilegios. Seguidamente, están gestionados por distintos procesos de altas, bajas y cambios y además, tienen que estar en funcionamiento los siete días a la semana y las veinticuatro horas del día.

Según la consultora Halock, cada persona tiene un promedio de 25 cuentas en diferentes sistemas y sigue creciendo con cada nuevo servicio o app que aparece en el mercado. Este fenómeno los expertos lo denominan como *identity sprawl* (expansión de la identidad) y sumado a las múltiples identidades internas en una empresa, el panorama no es muy esclarecedor. Además, este *identity sprawl* se simplifica en el hecho de que las personas tienen muchas identidades pero solo pocas contraseñas para gestionarlas. Parece ser una gran oportunidad para los hackers en atacar a las organizaciones por este lado.

Atender estos incidentes ocupa tiempo, recursos y son un coste directo para las áreas de TI, viéndose afectada la productividad de la compañía.

2.2 Pérdida de productividad y calidad

Si la gestión no está orientada para atender la complejidad de los diferentes sistemas y de los diferentes flujos internos de información para la gestión de los datos de los usuarios, se introduce variabilidad dentro de los procesos de la compañía.

Esta variabilidad hace que los procesos pierdan sentido y que la calidad y productividad disminuyan. Esto se suma a que los usuarios quieren la atención de manera inmediata y más cuando se trata de incidentes de alta, baja o modificación de usuarios. Según Gartner, el reseteo de contraseñas ocupa un 30% de las llamadas de *Help Desk*.

Estos incidentes llevan a una percepción de ineficiencia por parte del área TI, culpando de manera injusta a los CIOs por la entrada de variabilidad en los procesos de gestión de identidades.

"Los usuarios pierden la confianza en el área de Sistemas y en el CIO."

2.3 Shadow IT

Este término se refiere a los **dispositivos, softwares y servicios que no están controlados por el departamento TI** por lo que no cuentan con una aprobación manifiesta de la organización. Básicamente, nos referimos a cuando una persona de la organización decide usar un servicio en la nube sin el consentimiento de la empresa. Es muy común para aplicaciones de gestión de tareas, proyectos o agendas.

El problema radica en que se puede exponer a la empresa a riesgos indeseados; como el uso de datos en dichas aplicaciones sin la protección adecuada. Esta práctica tiene doble vertiente, por un lado es una amenaza a la seguridad y por otro, es una oportunidad para que las personas trabajen con las aplicaciones que mejor le funcionan.

Sin embargo, para nuestro caso de estudio, Shadow IT representa una amenaza al no estar conectado en el núcleo del directorio. Esto genera más identidades sin administración central, procesos caóticos y brechas de seguridad.

Otro riesgo que puede desencadenar la práctica de Shadow IT es la **dependencia de un proveedor.**

Las grandes compañías de servicios como Microsoft, Google o Amazon diseñan sus infraestructuras como grandes embudos de conversión que tienen como objetivo crear una dependencia como proveedores. Una vez tengan la identidad de la persona y así los de la compañía, puede bloquear servicios para que, eventualmente, tengas que pagar por los mismos. Es una práctica muy extendida como método de captación de clientes. Una vez captan tu identidad y utilizas sus servicios, poco a poco excluirás otras alternativas y la empresa se comprometerá a pagar por los servicios.

2.4 La brecha de identidad

Actualmente, nuestros bienes y activos están más conectados que nunca. Las empresas y organizaciones que operan en los mercados globalizados exigen agilidad y eficacia en el trabajo.

Esta conectividad hace que los sistemas estén vulnerables ante amenazas de seguridad y una de las más comunes es la brecha de identidad en la seguridad de las organizaciones. Según el Breach Level Index (BLI), **el robo o secuestro de identidades e información personal responde al 53% de todas las brechas de seguridad** para el año 2015.

Hubo un cambio en el *modus operandi* de los criminales digitales. Las estadísticas cambian: aumentan los ataques de robo de identidad e información personal con respecto a los robos de los números de tarjetas de crédito. Por ejemplo, empresas como JPMorgan Chase, MySpace, eBay o Yahoo han sufrido robos de identidades. La mayor de ellas registrada por BLI fue JPMorgan Chase con 83 millones de datos infringidos en 2014.

Pero el robo de identidades e información sigue creciendo de manera alarmante. El último caso de Equifax supera los 143 millones de datos de estadounidenses, alrededor de la mitad del país.

3. La Solución

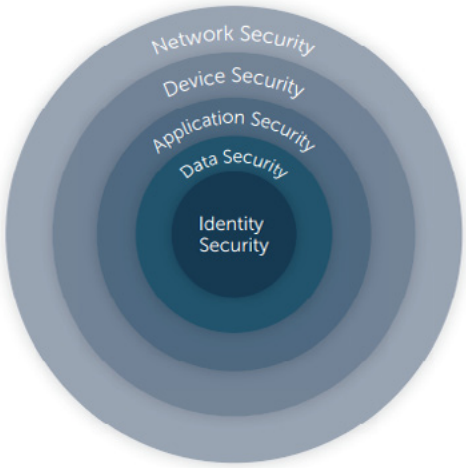
Desde el panorama del reto a los que se enfrenta un CIO, nos encontramos entonces con dos puntos importantes por solventar:

- **Eficacia:** La necesidad de agilizar los procesos y disminuir la variabilidad
- **Seguridad:** Mejorar la seguridad de las identidades y datos de la organización

La solución a estos problemas no responde simplemente a la instalación de un antivirus o un cortafuegos. Estas medidas de seguridad han quedado obsoletas y no responden a los riesgos actuales.

Para que una organización tenga un buen nivel de seguridad, se deben cumplir cinco capas de profundidad:

- **Network Security:** principalmente compuestos por firewalls, sistemas de detección y prevención de intrusos (IPS y IDS) y VPNs
- **Device Security:** dispositivos como servidores, ordenadores, portátiles, tabletas y móviles
- **Application Security:** tanto aplicaciones internas como de la web
- **Data Security:** Encriptación de los datos
- **Identity Security:** el núcleo de la seguridad empresarial.



Según lo que hemos avanzado como problemas y necesidades, resolver la variabilidad en la gestión de identidad, contraseña y accesos en los sistemas es la solución clave para mejorar la eficacia y la seguridad en la compañía. Es decir, necesitamos un sistema que tenga las variables de cada proceso bajo control.

Este sistema se recomienda que tenga tres características fundamentales: una **integración de todos los datos** de los usuarios, **evitar la variabilidad** de los sistemas (evitando la intervención humana) y **flexibilidad del sistema** para garantizar cambios en los procesos de la organización.

El área TI debe trabajar en conjunto con la política de la empresa, que será la encargada de establecer la concesión de los privilegios de acceso. Es así que todos los individuos y servicios estarán debidamente autenticados, autorizados y auditados.

La integración de algunas aplicaciones de uso común en una solución centralizada de gestión de la información sobre identidades es un reto complejo. Se necesita involucrar a diferentes áreas y procesos de una organización: desde socios o alta gerencia, hasta áreas como soporte o apoyo.

Con la colaboración de todos los actores de una compañía, con su disposición y compromiso, se consiguen buenos resultados y beneficios al aplicar un sistema Identity & Access Management (IAM).

Desde esta solución sabremos que la gestión de las identidades de empleados, proveedores, socios y clientes; desde servicios internos, compartidos y SaaS estarán aseguradas y mejorarán la eficacia de los procesos.

Ahora bien, sabemos el **qué debemos hacer** pero nos falta el c**ómo lo vamos a hacer.**

3.1 Identity Access Management (IAM)

IAM o gestión de identidades y accesos, funciona para administrar los datos relacionados con los perfiles de un usuario en una o varias aplicaciones. Es una solución interrelacionada que sirve para administrar la autenticación de usuarios, perfiles de cuentas, contraseñas, derechos y restricciones de acceso y otros atributos que la administración de la aplicación necesite.

Este sistema es un gestor de identidades y accesos que integra políticas y procesos organizacionales. Su objetivo es paliar nuestro problema principal, facilitando y controlando las identidades y los accesos en una empresa.

Estas **soluciones interrelacionadas** se basan principalmente en:

01 **Requisitos de contraseña:** Una computadora de alta gama crackea una contraseña en 5.5 horas. Los expertos recomiendan que uno de los requisitos de contraseña sea la de 12 caracteres. Para aumentar el nivel y complejidad de seguridad se deben tener en cuenta los siguientes factores:

- Longitud de contraseña
- Mayúsculas y minúsculas
- Números
- Caracteres especiales
- Tiempo de reutilización de contraseña

02 **Multi-Factor Authentication (MFA):** Los empleados son propensos a utilizar la misma contraseña en múltiples sitios, lo que hace que sean débiles y que aumente la posibilidad de mal almacenamiento. MFA es un complemento que mejora la seguridad en una contraseña estándar. Por ejemplo, las huellas dactilares o la impresión retiniana.

03 **Hashing & Salting de una vía:** tus identidades deben estar encriptadas en un solo sentido de transmisión de la información. Esto hace que sea extremadamente difícil su desencriptación.

04 **Entrenamiento:** las identidades están intrínsecamente vinculadas a nuestro comportamiento como usuarios. Por ello, es importante la concienciación de los empleados sobre los peligros latentes de un robo o plagio de identidades.

05 **Aprovechamiento de identidades SaaS:** directorios en la nube como Google Apps son extremadamente efectivos porque requieren poca inversión y mantenimiento IT. Sin embargo, estos no ofrecen un grado de control al nivel de un directorio porque este tipo de Apps no fueron creados como verdaderos directorios. Es decir, no podrá crear agrupaciones, automatizaciones ni capas de seguridad a los accesos e identidades. Esto genera mayores recursos para comprobar cada una de las aplicaciones y servicios de un negocio.

Para ello, se recomienda aplicar un SSO (single sign-on) por medio del sistema Indentity and access management, integrando las distintas aplicaciones de la nube y los recursos locales para dar respuesta a los negocios modernos.

3.2 Usabilidad de IAM

Como CIO debes identificar las necesidades de seguridad y control de tu organización. En este caso debes elegir los diferentes tipos de refuerzos de autenticación según la lógica de uso del usuario. Estos son algunos ejemplos comunes:

- Cuando un dispositivo es usado por primera vez
- Cuando un cliente realiza una transacción que no está acostumbrado a hacer
- Si un usuario está inactivo durante mucho tiempo
- Múltiples acciones en un periodo de tiempo corto.

Una vez identificadas, enfócate en las mejores soluciones que hagan que el trabajo de instalación y migración sea lo más ágil posible.

> *"No planees una personalización masiva de infraestructura de IAM. Enfócate mejor en soluciones que permitan una configuración rápida que aumente la velocidad de la migración..."*
>
> **— Gartner, 2015 —**

En el mercado existen diversas opciones pero nos centraremos en la propuesta de WSO2 por ofrecer una solución completa y proporcionar un servicio de seguridad uniforme.

3.3 WS02 Identity Server

WS02 Identity Server es el sistema de código abierto basada en los puntos fuertes de los estándares de seguridad más utilizados. Ofrece una plataforma de enfoque que permite a los CIOs aplicar una capa de seguridad uniforme sobre los activos existentes en el entorno digital. Una de sus ventajas es que es un proyecto en constante evolución, lo que permite mejoras continuas en cada nueva versión. Este punto es muy importante porque es un sistema que puede hacer frente a los nuevos retos de negocio, a las expectativas de los clientes y a las amenazas de los ciberataques.

Ilustración SEQ Ilustración * ARABIC 2: Imagen via WS02

¿Cómo funciona WS02 Identity Server?

WS02 Identity Server proporciona una administración de seguridad tanto para aplicaciones web, servicios y API de la empresa. Este sistema permite reducir el tiempo de aprovisionamiento de identidad, garantizar las interacciones en líneas seguras y ofrecer un entorno de inicio de sesión reducido. Otras de las funciones son la creación, mantenimiento y finalización de cuentas de usuario a través de múltiples sistemas, incluyendo aplicaciones Cloud. Este sistema te permite tener una **identidad centralizada como Proveedor de Servicios**, un modelo que garantiza una mayor eficacia.

Los usuarios finales tendrán la interfaz 'Jaggery'. Además, las páginas de inicio de sesión y consentimiento de la interfaz pueden **personalizarse completamente** a las necesidades de cada organización. Lo más interesante es que se ejecuta como una aplicación web en un contexto independiente.

Características principales

Single sign-on

Es capaz de establecer puentes entre protocolos de un solo acceso a los sistemas como OpenID Connext, SAML 2.0 y WS-Federation que proporcionan una experiencia SSO unificada.

Autenticación fuerte y confiable

Posibilidad de aplicar autenticación multifactorial (MFA) con contraseña en SMS / correo electrónico (OTP), Fast IDentity Online (FIDO), MePin, Duo Security y más.

Administración y gobernanza de identidades

Permite gestionar usuarios o grupos de usuarios con flujos de trabajo automatizados. Puede implementarse como un elemento central para la gobernanza de identidades, facilitando la integración con otros proveedores de identidad tales como Google, Facebook, Twitter, Salesforce, entre otros.

Control y derechos de acceso

Autorización con control de acceso basado en roles y en atributos a través de políticas XACML. Proporciona un modelo de seguridad integral basado en OAuth 2.0 para asegurar el acceso a las API.

Seguimiento, auditoría e informes

Los CIOs pueden analizar las autenticaciones e informes integrados así como auditar las operaciones privilegiadas. Permite una mayor comprensión de los patrones de autenticación de aplicaciones de usuarios. Se proveen herramientas para obtener la información requerida para estos análisis en tiempo real y en modo batch.

Integración con sistemas para mejorar capacidades

El sistema permite construir soluciones a medida que respondan a los requisitos de administración y autentificación de múltiples factores utilizando una amplia oferta de conectores para WS02 Identity Server.

7. Conclusiones

La gestión de identidades y accesos incluidos en procesos de trabajo es un punto crítico para las compañías. Esta gestión interrelacionada incluye todos los datos de los usuarios, por lo que son procesos críticos de alta variabilidad. Al no estar bien gestionados y al incrementar la variabilidad en los procesos, pueden ocasionar una afectación importante a la compañía. Además, una mala gestión afecta a la percepción de los trabajadores y altos mandos de una empresa con respecto a la efectividad de las áreas de tecnología y a la imagen en particular del CIO.

Las empresas y en especial los CIOs deben tener especial consideración en la adecuación de sistemas IAM. Emplear servicios como WS02 Identity Server es garantía de dar respuesta a los dos principales problemas que incurre la administración de identidades y accesos: la eficacia y la seguridad.

> *“Para todo gran problema siempre hay personas y empresas que están buscando una solución a esta llamada “crisis de identidad”.”*

¡Muchas gracias!

Sobre Chakray:

Hacemos bien las cosas

En Chakray somos especialistas en servicios de arquitectura, consultoría y formación de Sistemas de Información Críticos. Nuestro equipo desarrolla proyectos de Open Source con el software más innovador de WSO2 con un único objetivo: Hacer que la tecnología de tu empresa sea la mejor.

¿Quieres mejorar tus sistemas?
¡Consulta a nuestros expertos!

Pregunta sin compromiso a nuestros consultores. **Te ayudaremos a encontrar la mejor solución para tu proyecto**.

CONTACTA CON NOSOTROS

CHAKRAY

DOING THE RIGHT THINGS.

WITH THE RIGHT TECHNOLOGY.
TO SUPPORT BUSINESS.

info@chakray.com | www.chakray.com