SIMPLIFICA LA IDENTIDAD

Mejora la imagen y los costos de TI

KAAB

ENIGM4 | Creando capacidades tecnológicas

kaab.en1gm4.com

Administración de Identidades

Una clave para la confianza en TÍ

El problema

Una gestión de usuarios inadecuada puede dañar de manera drástica la confianza en las áreas de TI

Uno de los grandes problemas que enfrenta un CIO es la confianza en los servicios que proporciona, estos deben de ser de bajo costo y dejar satisfecho al cliente (interno y externo). Es común la sensación en el personal de TI, de que, si todo funciona, las áreas de sistemas no son tomadas en cuenta, pero si algo no funciona están en el centro del huracán.

Generalmente se tiende a pensar en problemas graves como la suspensión del servicio de tecnología, pero además de éstos, hay otros que día a día **dañan la confianza de la compañía en los servicios de TI**, tal es el caso de la gestión de datos de los usuarios, que se convierte en el dolor de cabeza más común para el personal encargado de TI en particular la administración de contraseñas y los privilegios de los usuarios.

De acuerdo a un análisis realizado sobre la experiencia de los usuarios, los problemas relacionados con sus cuentas de acceso a los sistemas, son los que más les generan molestias, porque les inhibe el acceso a las herramientas.

Por el otro lado la atención de estos incidentes termina siendo un costo directo para las áreas de TI y por supuesto para la productividad de la compañía. Es importante no perder de vista que además se generan costos indirectos que son mucho más delicados ya que hay una afectación en la imagen del servicio de TI y en la confianza de la compañía.

Los usuarios quieren la atención y la quieren inmediatamente

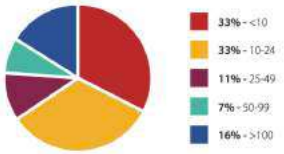
Alcance general

Las organizaciones generalmente ven estos problemas como parte de la operación, sin embargo, considero que un acercamiento más frontal al problema puede traer beneficios directos a las áreas de TI y a la organización.

Este documento da una visión general de los problemas de una gestión inadecuada de las identidades, explica los elementos críticos de la tecnología que pueden resolver este problema, también expondremos la propuesta de un producto que implementa estos puntos críticos para una organización.

Antecedentes

¿Pero cómo hemos llegado a este punto?



Aplicaciones a implemenatr en el 2017 Fuente OutSystems

Desde hace una década la tecnología ha venido creciendo de una manera inimaginable y con una tasa muy acelerada. En los años 80´s el acceso a las computadoras estaba restringido a unos cuantos usuarios privilegiados, pero con el pasar de los años las computadoras fueron más accesibles a los usuarios y por lo tanto las empresas empezaron a tener muchas más computadoras y por lo mismo más sistemas.

Esta situación derivo en muchos más datos en los sistemas, además de muchos sistemas en los procesos de negocio. Fue entonces que el acceso a los sistemas se convirtió en un tema en el que valía la pena interesarse para cuidar los datos de los

usuarios tanto en las empresas como de manera personal. Es por ello que la seguridad en los sistemas se sumó como un punto crítico, por lo mismo surgieron regulaciones . tanto de los gobiernos como de las empresas que emitían y emiten estándares de seguridad y de protección de datos.

De acuerdo a Edward Deming la variabilidad en los procesos impacta directamente la productividad y la calidad

Situación Actual

¿Cuál fue el resultado?

Empresas con múltiples sistemas que tienen a su vez múltiples usuarios, con múltiples contraseñas, con múltiples privilegios y que tienen procesos de. altas, bajas y cambios, que tienen que estar gestionados 7 x 24, con usuarios que cada vez son más exigentes en el servicio, sumado a la complejidad de los diferentes sistemas, se tiene que considerar la misma complejidad a los diferentes flujos internos de información para la gestión de los datos de los usuarios, ya que cada organización es única en la manera como maneja el flujo de la información de los datos de los usuarios.

Un problema de variabilidad

Una gestión no diseñada para atender estas necesidades en la gestión de los usuarios introduce variabilidad a los procesos de la compañía. **"El enemigo de todo proceso es la variación"**, debemos entender que no hay dos empresas idénticas y por lo tanto las necesidades de los usuarios son variables. El Dr. Edward Deming, afirma que la productividad y la calidad aumentan mientras la variabilidad disminuye lo contrario también es cierto.

¿Pero qué se pierde con una pérdida de productividad y calidad?

Es fácil ver que hay una pérdida de horas hombre que es tangible y que es fácil de calcular. Para dimensionar esto demos ejemplo de un estudio realizado en YPF (empresa líder en la industria de energía en Argentina) que cuenta con 15 000 usuarios y que tiene un promedio de 3 días de atención por los incidentes de alta baja modificación de usuarios.

Los usuarios quieren la atención y la quieren inmediatamente

Analia Benitez, Gerente de Seguridad de YFP decía "En 15 mil usuarios, tener 40% de incidentes relacionados con bloqueo de usuarios es una cantidad importante. YFP necesita reducir esos números". Según una estadística de Gartner el **30% de las llamadas del Help Desk son incidentes de reseteo de contraseñas.** Pero los costos ocultos de esto están directamente relacionados con la percepción de la organización sobre los procesos de TI, lo cual genera una sensación en los usuarios de estar no atendidos y de ineficiencia del área de Sistemas. En general las expectativas son muy altas **el usuario quiere la atención y la quiere inmediatamente;** hay una frase de uso común: "percepción es realidad" y muchas veces el área de TI es culpada injustamente por fallas en los procesos de gestión de identidades.

Lo anterior se puede resumir en pérdida de confianza en el área de TI y principalmente la sensación de que el **CIO no está haciendo nada al respecto.**

Solución

¿Pero cómo resolver los problemas en los procesos de gestión de identidades?

Un sistema de calidad ideal debe resolver el problema de variabilidad

De lo anterior es fácil deducir que la meta es resolver la variabilidad en la gestión de los datos de identidad, incluyendo la contraseña y los privilegios en los sistemas. Un sistema ideal de control de calidad consiste en controlar cada una de las variables que afecta un proceso que sistema pueda ajustar las variables y que pueda predecir los efectos de esas variables en la calidad y en la percepción del servicio. Resumiendo lo anterior debemos tener un sistema que tenga las variables bajo control.

Siguiendo las ideas anteriores es necesaria una integración de todos los datos de los usuarios, esta tesis de integración resolvería el problema de la complejidad de muchos orígenes de información de diversa naturaleza y diferentes grados de complejidad en una sola fuente integral de datos.

Siguiendo en la línea de evitar la variabilidad de los sistemas, es necesario en la medida de lo posible evitar la intervención humana en el proceso, a efecto de evitar variables que no controlemos en el proceso y por lo tanto como efecto contar con un mayor control del sistema.

Pero es necesario que este sistema creado para la reducción de variabilidad sea extremadamente flexible para garantizar que los cambios en los procesos internos de la organización puedan ser incorporados en el sistema de administración de identidades.

¿Single Sign-on?

Una de las aproximaciones que se tienen para resolver este dilema es generar un solo acceso a los sistemas (single sign-on). Desde mi punto de vista esta solución incrementa la complejidad de lo que por su naturaleza ya es un problema complejo, al convertirse en un punto único de falla, además de que al implementarlo introduce nuevas variables a los ya de por si complejos sistemas de una organización.

KAAB, Nuestra propuesta

Ante el panorama señalado, se diseñó KAAB, un sistema de administración de identidades que permite a las empresas una homologación de la información de las personas en tiempo real, para garantizar su homologación en los diferentes sistemas, incluyendo de manera particular y de forma diferenciada, la información de la contraseña, con el fin de garantizar que todos los sistemas tengan la misma información de los usuarios y reducir inconsistencias entre los datos, evitando así la variabilidad asociada a estos procesos.

Para evitar la variación asociada a la particularidad de cada empresa se **le agregó flexibilidad a todo el proceso,** a través de un mecanismo de generación flujos de trabajo para adecuarse a los flujos de operación reales en los procesos internos de la compañía.,

También cuenta con una **integración bidireccional de datos** que es un proceso de sincronización de la información en todos los sistemas o en los repositorios de información (conocido técnicamente como aprovisionamiento de información).

La flexibilidad es la clave en el manejo de la variabilidad

Incluye un **mecanismo flexible y de fácil implementación** que permite la conexión a diferentes sistemas y dispositivos mediante **conectores a sistemas.** La integración a **nuevos sistemas es muy sencilla y de corto tiempo y extremadamente flexible.** Existen conectores ya desarrollados en el producto para los sistemas más comerciales del mercado como SAP. Se han hecho integraciones en muy corto tiempo para sistemas tan complejos como aplicaciones en el sistema operativo AS400.

El producto está diseñado para estar **alineado a las más estrictas normas de seguridad.**

Por otro lado KAAB cuenta con **un módulo de autoservicio** para ayudar a las empresas a delegar el desbloqueo de contraseñas a los mismos usuarios con mecanismos de seguridad que garanticen el acceso a las personas correctas, con esto se optimizan los tiempos de atención y se evita la intervención de un operador.

KAAB puede **agregar de manera inmediata todos los procesos de altas, bajas y cambios de usuarios y contraseñas a los sistemas ya existentes** o a los nuevos, dejando a las áreas de sistemas este tiempo libre para el desarrollo de otras funciones críticas para la empresa.

Es de suma relevancia realizar la implementación y el mantenimiento de un sistema de esta naturaleza con personal especializado con una pasión por el servicio, que tenga presente la importancia de realizar un cambio a profundidad en los procesos relacionados con la identidad de los usuarios.

Es esencial hacer la implementación con personal que este consiente de la importancia de los procesos de negocio del cliente

Leonardo Tamayo CEO de Cryptos Systems[1] comenta "En Cryptos Systems, creemos firmemente en un proceso de venta consultiva de proyectos de TI. Nuestro objetivo principal es hacer que la tecnología tenga un alto valor para nuestros clientes, entendemos que no todos nuestros clientes son iguales y para nosotros KAAB es una herramienta alineada a nuestra meta de hacer un cambio radical en las organizaciones a través de nuestro concepto único de una plataforma de acceso inteligente".

Conclusión

Los procesos relacionados a la gestión de identidades, que incluyen todos los datos de los usuarios, son procesos críticos de alta variabilidad y de alta visibilidad, que de no estar bien gestionados pueden ocasionar una afectación importante, en la percepción que tiene la organización de la efectividad de las áreas de Tecnología, de una empresa y en la imagen particular del CIO. Las empresas deben tener en consideración la importancia de una adecuada gestión de identidades y considerar la implementación de herramientas como KAAB que estén diseñadas con el único propósito de hacer de la gestión de identidades una clave para la confianza el CIO.

1 Cryptos Systems es una empresa mexicana dedicada a la venta consultiva de proyectos de Seguridad de TI, Cryptos System ha desarrollado un concepto de plataforma que genera una administración ágil y eficiente que mejora los costos operativos y la percepción que se tiene de las áreas directivas de TI de las empresas

Acerca del Autor

Daniel Peñaloza es CEO de En1gm4 (kaab.en1gm4.com), entre su experiencia profesional está el haber sido entre otros puestos directivos CISO de Walmart de México y Centro América, Director de Sistemas de Santander México, cuenta con diversas certificaciones entre ellas CISSP (Certified Information Systems Security Professional) de ISC^2

Es Maestro de Tecnologías de Información por el Instituto Tecnológico Autónomo de México (ITAM), Maestro en Telecomunicaciones por la universidad francesa ENSTB (École Nationale supérieure des Télécommunications de Bretagne), cuenta con estudios a nivel Doctorado en Psicoanálisis por CEPSIMAC, es participante del programa MEDEX (Máster en Dirección de Empresas para Ejecutivos con Experiencia) del IPADE (Instituto Panamericano de Alta Dirección de Empresas)

Para Saber más

http://www.cryptos.com.mx/mx/manejo-de-identidades

Kaab@cryptos.com.mx