SEGURIDAD QUE NO PROMETE: CUMPLE

El equipo de seguridad de IBM integra todas las soluciones necesarias para garantizar la seguridad de cualquier organización.

Roque Juárez de Jesús, Consultor de Seguridad de IBM

Hoy en día, uno de los mayores problemas a los que se enfrentan las empresas es la desorganización y la pérdida de tiempo debido a la desigualdad de operación y administración de la seguridad de información que requieren los servicios de negocio soportados por su infraestructura tecnológica.

La solución que ofrece el concepto de herramientas y servicios "Total Authentication Solution", permite a las organizaciones una plataforma tecnológica de alta seguridad a través de aplicaciones orientadas a la optimización del flujo de los procesos y servicios de los negocios.

"Nosotros aprovechamos la flexibilidad de nuestro portafolio de seguridad para construir una solución integral en términos de la gestión de la identidad digital y del control de acceso de los usuarios a los aplicativos y recursos de infraestructura de acuerdo a los requerimientos específicos de cada organización." dice Roque Juárez de Jesús, Consultor de Seguridad de IBM.

Los servicios profesionales y administradores de seguridad, integran todos los beneficios necesarios para que la empresa pueda tener un proceso de gestión de la operación de la seguridad asertivo y eficiente, sin la necesidad de utilizar aplicaciones particulares que no son compatibles entre sí.

HERRAMIENTAS INTEGRALES PARA LA GESTIÓN DE SERVICIOS DE SEGURIDAD

La plataforma multinivel permite que las organizaciones incrementen la complejidad de protección de sus soluciones. Con esto la empresa puede optimizar los módulos de seguridad y garantizar impermeabilidad ante los ataques generados por usuarios internos o terceras personas.

Una de las grandes ventajas del "Total Authentication Solution" es que incrementa el funcionamiento de las soluciones de control de acceso, desde el manejo de la identidad digital, la autenticación en el recurso de infraestructura hasta la autorización a partir de la integración con soluciones del segundo factor de la autenticación.

TECNOLOGÍA ANTIFRAUDE: IDENTIFICAR, REGISTRAR Y REPORTAR

El desarrollo tecnológico no sólo brinda beneficios, desafortunadamente los robos están a la orden del día y las corporaciones deben ser más cautelosas para proteger uno de sus activos más importantes: la información. Para ello requieren de cimientos sólidos que soporten su seguridad y que les permitan anticiparse para responder ante la ocurrencia de sucesos inesperados .

IBM tiene un conjunto de soluciones especializadas que permite a los clientes sentirse seguros durante la ejecución de sus procesos de negocio, desde una simple transacción hasta el nivel de actividades de gestión, dado que es muy eficiente para proteger diferentes categorías de recursos de información, desde las bases de datos hasta las plataformas.

Específicamente, uno de los sectores que experimenta más atentados es el financiero, por su naturaleza y valor de la información digital que maneja. Los bancos necesitan de tecnologías que puedan detectar anomalías y desviaciones en tiempo real del manejo de datos tanto de los clientes como de los usuarios.

Las soluciones modulares de nuestro ofrecimiento, otorgan el beneficio a las instituciones de poder utilizar el portafolio de seguridad de diferentes maneras.

El portafolio de servicios antifraude de IBM se divide en 3 categorías:

- **Sección preventiva:** Las herramientas de esta área permiten limitar las actividades de los usuarios, así mismo, el intento de cualquier desviación se impide de forma automática por el sistema, se registra y se reporta de acuerdo al proceso de cada cliente.
- **Sección detectiva:** Revisa detalladamente la ejecución de las transacciones y actividades de todos los usuarios y operadores, detectando las inválidas con base al marco normativo de operación y seguridad de las organizaciones.
- **Sección correctiva:** Registra, preserva y apoya el análisis de toda la información que se generó en los diferentes recursos de infraestructura, para apoyar procesos de auditoría, análisis causa raíz y cumplimiento.

La infraestructura de los sistemas de seguridad creados por IBM cuentan con los módulos y funcionalidades indispensables para realizar revisiones y garantizar una excelente operación con base a las prácticas y exigencias que el cliente tiene que cumplir de acuerdo a su entorno profesional y legal.

SOLUCIONES QUE PROTEGEN, ACONSEJAN Y ORIENTAN

La plataforma de soluciones de seguridad está preparada para ofrecer una alternativa viable en el cumplimiento de los doce requerimientos determinados por el Consejo de Seguridad PCI (Payment Card Industry Data Security Standard) y el acuerdo de Basilea II, el cual consiste en recomendaciones sobre la legislación y regulación bancaria.

Gracias a esto, las organizaciones tienen la oportunidad de configurar plantillas de revisión y de monitoreo alineadas con las requerimientos específicos que emite la CNBV (Comisión Nacional Bancaria y de Valores).

Previo a la determinación del cumplimiento de los estándares legales, los especialistas en seguridad de IBM, ayudan al cliente a elegir la mejor forma de apegarse a la normatividad exigida a través de la gestión del riesgo, la cual consiste en apoyar a la corporación a determinar el nivel de riesgo con el cual pueden operar.

El servicio y la plataforma de soluciones integrales de IBM, están listos para enfrentarse ante los ajustes administrativos y de manejo de información personal de los clientes que dicta la Ley Federal de Protección de Datos Personales en Posesión de Particulares.