Guía para gestionar la seguridad de tus sistemas SAP

NOVIS

La ciberseguridad es una de las principales prioridades de las empresas. Sus sistemas contienen una gran cantidad de información sensible y perderla puede llegar a costarles millones de dólares.

Los sistemas digitales pueden verse comprometidos tanto por errores humanos internos, como por ataques maliciosos del exterior. Para los sistemas SAP esto no es la excepción, por lo que las empresas han de implementar estrategias para mantener sus datos privados y protegidos.

El costo monetario promedio a nivel mundial de los delitos cibernéticos tuvo un incremento de 80.86% al pasar de 522,500 millones de dólares en 2018 a 945,000 millones de dólares en 2020, de acuerdo con el reporte The Hidden Costs of Cybercrime, elaborado por McAfee y Center for Strategic and International Studies (CSIS).

A esta última cantidad, se suman 145,000 millones de dólares en gastos por ciberseguridad, con lo que la economía global gasta más de 1 billón de dólares al año, por ciberdelitos.

Además de la pérdida financiera, existen otros aspectos en los que los delitos cibernéticos afectan a las empresas:

DAÑO Y DESTRUCCIÓN DE DATOS.

Esto puede incluir información confidencial de empleados y clientes, así como datos específicos de la empresa.

PÉRDIDA DE PRODUCTIVIDAD.

Durante y después del ataque, mientras se restauran los sistemas y se establece la estrategia de respuesta a él, ciertos departamentos pueden ver comprometida su actividad.

ROBO DE DATOS PERSONALES Y FINANCIEROS.

Tanto de la empresa, como de los clientes, la pérdida de datos personales y financieros también puede incidir en fraudes o malversación de fondos.

EL COSTO DE OPORTUNIDAD.

Es el monto que le cuesta a las empresas el que no se pueda brindar un servicio, concretar una venta o una transacción debido al incidente cibernético, es decir, lo que te cuesta no poder utilizar tus sistemas.

ROBO DE PROPIEDAD INTELECTUAL.

Esto puede abarcar desde procedimientos o secretos comerciales, hasta patentes.

DAÑO A LA REPUTACIÓN DE MARCA.

Hacia el público y sus clientes, la reputación de las marcas sufren daños y pérdidas de confianza. Incluso pueden llegar a perderse clientes o inversionistas si la información comprometida los afecta directamente.

Top 10 de riesgos en la seguridad de tus sistemas SAP

Un sistema de gestión de recursos empresariales como SAP abarca diferentes aristas y departamentos de las empresas, además de que maneja una gran cantidad de datos confidenciales.

SAP es una plataforma segura, pero hay diferentes soluciones y niveles de seguridad que son personalizables. Si no se hace un análisis real de los accesos y permisos otorgados a los trabajadores de la organización, puede crear serias vulnerabilidades.

Asimismo, SAP puede alinearse con regulaciones nacionales e internacionales para el manejo de información sensible o datos personales.

De acuerdo con la consultora RSM, los 10 principales riesgos de seguridad que pueden afecta a las soluciones SAP son:

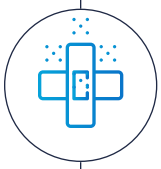
01. Vulnerabilidades en la infraestructura.

SAP funciona con diferentes hosts y cuenta con funciones remotas (RFC, por sus siglas en inglés). Si alguien puede entrar a través de esos RFC podría tomar control del sistema.

02. Configuración poco segura.

Existen muchas configuraciones que vienen predeterminadas y que no se personalizan durante la instalación de SAP.

Esto puede dejar algunas soluciones descubiertas o vulnerables a ataques externos o a fallas internas. La configuración de la seguridad de las soluciones debe ser independiente a la administración de parches.



03. Falla en la gestión de parches.

Los parches, como en cualquier sistema, sirven para reparar funcionalidades o vulnerabilidades detectadas en versiones anteriores y hacer los sistemas más estables y seguros.

Además, con la migración a la nube, la administración de parches se vuelve compleja, ya que debe estarse revisando constantemente cuáles son los parches necesarios para el sistema SAP de la empresa e implementarlos de forma oportuna.

04. Comunicaciones entre interfaces no encriptadas.

Un nivel básico en la comunicación entre soluciones es la encriptación de la información para que no esté expuesta a la mirada de cualquier persona.

Por otro lado, la información podría estar mucho más resguardada si es interceptada durante la transmisión.

05. Control en los accesos y segregación de funciones.

Los sistemas SAP están diseñados para establecer diferentes niveles de accesos y crear segregación de funciones (SoD, por sus siglas en inglés).

Realizar una mala ejecución en estos niveles puede incrementar el riesgo de fraudes, accesos de empleados a datos sensibles o información privada que no es necesaria para sus funciones.

06. Monitoreo de eventos de seguridad.

Se debe revisar de forma constante los accesos de las cuentas de usuarios privilegiados a las bases de datos y a las diferentes soluciones de SAP. Asimismo, debe monitorearse el uso del registro para identificar los eventos de seguridad que se hayan presentado.

07. Seguridad en la identificación del sistema.

Las identificaciones del sistema y las comunicaciones, con niveles de seguridad altos o con acceso libre a todas las soluciones, deben estarse revisando de forma constante, para evitar que alguien no autorizado pueda obtener estas credenciales y acceder a todo el sistema.

08. Brechas en código personalizado.

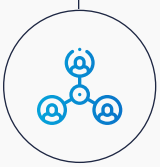
SAP es un sistema altamente personalizable, al que se le pueden agregar funcionalidades con código propio de las empresas. Este código puede dejar puertas traseras abiertas y que pasen inadvertidas para el desarrollador.

Cualquier cambio que se haga en torno a los objetos personalizados, debe quedar documentado, al mismo tiempo que se establecen medidas de seguridad específicas para ellos.

09. Accesos elevados para administradores y equipo de soporte.

Durante la implementación o el mantenimiento del sistema SAP suelen otorgarse accesos privilegiados para los administradores o el equipo de soporte.

Perder alguno de ellos representa un alto impacto en la seguridad, por lo que se recomienda mantener mecanismos de autenticación múltiples, así como controlar el acceso y la actividad de los usuarios para detectar alguna irregularidad.



10. Administración de usuarios.

Los diferentes usuarios pueden cambiar sus niveles de seguridad, cuentas o controles de acceso.

Debe gestionarse de forma efectiva cualquier modificación que se haga, ya que en ocasiones quien otorga los permisos puede no tener claro cuál es el acceso que se está otorgando a un usuario, ya que la solicitud viene de otros departamentos.

¿Cómo gestionar la seguridad de SAP?

Para gestionar de forma efectiva la seguridad de SAP deben considerarse tanto los elementos internos como los externos:

IDENTIFICA VULNERABILIDADES

El análisis debe ser lo suficientemente amplio para incluir la seguridad de las bases de datos, las cuentas de administrador del sistema, la infraestructura y la comunicación entre los diferentes hosts.

También debe analizarse el sistema operativo, así como los diferentes parches, antivirus y las interfaces del sistema.

Por último, deben considerarse las posibles vulnerabilidades en los diferentes entornos de red, ya sea interna o con las aplicaciones que se hayan migrado a la nube.

ALINEA LA CONFIGURACIÓN DE LAS SOLUCIONES SAP

Las configuraciones de las soluciones SAP deben estar alineadas con las políticas de la empresa, por ejemplo, con su nivel de cumplimiento del marco legal y fiscal, con los niveles de seguridad para cierto tipo de información y con los accesos que algunos usuarios puedan tener a estos datos.

Asimismo, la empresa debe tener protocolos de seguridad que deben ser conocidos por todos los usuarios y empleados, ya que de no seguirlos, alguno de ellos puede provocar una brecha de seguridad por desconocimiento o ignorancia.

ADMINISTRA LOS PARCHES NECESARIOS

Los sistemas SAP deben estar siempre actualizados, pero hay algunas dificultades al administrar los parches que se requieren para ciertas soluciones. Por ejemplo, los administradores del sistema pueden no conocer todos los parches necesarios para alguna vulnerabilidad del sistema previamente detectada.

Cualquier parche debe probarse antes de la implementación para identificar algún comportamiento inesperado, al mismo tiempo, deben establecerse evaluaciones de qué tan conveniente ha resultado un parche y si lo que se ha obtenido de él es lo que se esperaba.

CREA UN PROCEDIMIENTO DE EMERGENCIA

Sólo 44% de las empresas cuentan con planes para prevenir incidentes de seguridad de TI y responder a ellos, de acuerdo con el reporte de McAfee y CSIS. De éstas, únicamente 32% consideran que estos planes son realmente efectivos.

Las empresas deben contar con un plan de seguridad, en primer lugar, para prevenir los posibles ataques, pero también para responder en caso de que haya un incidente.

Esto incluye quién debe responder en primera instancia, cuáles son los pasos que se van a seguir para contener el ataque y qué deberá hacerse posteriormente, considerando diferentes escenarios, como pérdida de datos, o el que haya información comprometida en mano de los ciberdelincuentes.

USA LAS HERRAMIENTAS DE SAP

SAP ofrece diferentes soluciones de seguridad, dependiendo de los requerimientos de la organización:

SAP Cloud Identity Access Governance

SAP Code Vulnerability Analyzer

SAP Enterprise Threat Detection

SAP Governance, Risk, and Compliance

SAP Identity Management

Algunas de ellas funcionan para gestionar los permisos y datos que se migran a la nube, otras para detectar de forma oportuna alguna brecha de seguridad o un ataque, en tiempo real.

Además, existen otras soluciones para la auditoría y monitoreo de accesos, así como la revisión de ciertos usuarios a las bases de datos u otras herramientas de SAP.

Lo ideal es que cada organización establezca las soluciones que más se apeguen a su sistema SAP y a sus políticas de seguridad.

REVISIONES Y MONITOREO

Cada cierto tiempo debe analizarse el desempeño en la seguridad de los sistemas de SAP, para hacer los ajustes que se requieran de forma oportuna, antes de que se presente una brecha.

Lo mismo debe tenerse en cuenta para los accesos de los usuarios, la segregación de funciones y la creación de roles y perfiles de SAP, lo ideal es que los diferentes niveles de acceso se adapten a los cambios que pueda haber en las plantillas de usuarios de la organización.

AUDITORÍA DE TU SISTEMA SAP

Recurrir a una auditoría de seguridad para SAP, de forma preventiva, te dará mucha más visibilidad de cuál es el estado de salud de tus sistemas, así como las principales vulnerabilidades a las que se enfrenta.

Aunado a esto, la auditoría revisa de forma integral diferentes aspectos a tener en cuenta, como la asignación de roles y perfiles, si los parches y las soluciones que usas se encuentran actualizadas y cuáles son las herramientas de seguridad más adecuadas para el perfil de tu negocio.

Checklist
de la seguridad de tu sistema SAP

De acuerdo con la información anterior, te dejamos una lista de todos los puntos que debes evaluar para verificar que la seguridad de tu sistema SAP sea la óptima:

- ☐ **Infraestructura de tus sistemas.**
- ☐ **Personalización de configuración de soluciones SAP.**
- ☐ **Parches actualizados.**
- ☐ **Encriptación de la comunicación entre interfaces.**
- ☐ **Segregación de funciones.**
- ☐ **Niveles de accesos establecidos.**
- ☐ **Revisión de accesos de los diferentes usuarios**
- ☐ **Revisión del código personalizado.**
- ☐ **Accesos otorgados a administradores y personal de soporte.**
- ☐ **Gestión de permisos de los diferentes usuarios.Soluciones SAP alineadas a las políticas de seguridad de la empresa.**
- ☐ **Existencia del procedimiento de emergencia antes y después de una brecha de seguridad.**
- ☐ **Establecer el calendario para las revisiones del desempeño de la seguridad de los sistemas SAP.**

Por último, ten en cuenta que la seguridad de los sistemas informáticos de las empresas deben ser responsabilidad de cada una de las personas que hacen uso de ellos dentro de la organización, para que puedan funcionar de forma efectiva.

La empresa debe contar con políticas de seguridad, para el tratamiento de la información y con reglas de confidencialidad, que todos dentro de la organización deben conocer y seguir.

Si requieres incrementar los niveles de ciberseguridad, considera a Novis como tu aliado estratégico para gestionar de forma óptima la seguridad de tus sistemas SAP. Nuestros expertos cuentan con certificaciones en las mejores prácticas, para el manejo y gestión de las soluciones SAP.

Fuentes:

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

https://rsmus.com/what-we-do/services/risk-advisory/top-10-sap-audit-and-security-risks.html

https://www.sap.com/about/trust-center/security.html

https://learning.sap-press.com/sap-security#sap-cloud-identity-access-governance

https://blogs.sap.com/2021/07/16/sap-solutions-for-cyber-security-and-data-protection/


NOVIS