Mejores prácticas en ciberseguridad

para las empresas y sus sistemas SAP

NOVIS

Los ataques a los sistemas y las brechas de seguridad se incrementan cada año. El costo para las empresas también ha aumentado, junto con la inversión que deben hacer en ciberseguridad.

Sin embargo, hay algunos elementos clave que se deben tener en cuenta para que esta inversión sea mucho más efectiva, principalmente si se trata de resguardar sistemas de gestión empresarial como SAP.

Además, se debe trabajar de forma integral en todos los departamentos de la empresa, no sólo los relacionados directamente con el área de TI.

Prioridades de seguridad para las empresas

La seguridad de tus sistemas informáticos, antes que considerarse un gasto, debe verse como una inversión. Ten en cuenta que un ERP como SAP, que maneja una gran cantidad de información, no puede verse comprometido en una brecha de seguridad. En un caso así, incluso, podría afectar la continuidad del negocio.

La ciberseguridad debe ser parte central de la estrategia, ya que la información que se maneja diariamente implica datos privados de clientes y empleados, propiedad intelectual, datos financieros y corporativos.

Comprometer esa información le cuesta dinero, tiempo y pérdida de confianza a las empresas; algunas de ellas no han logrado recuperarse de ciberataques o ransomware.

Según una proyección, de la consultora Gartner, el gasto mundial para mantener la seguridad de la información y el manejo de riesgos de tecnología en 2021 pudo ser de 150,400 millones de dólares, lo que se consideró como un incremento de 12.4%

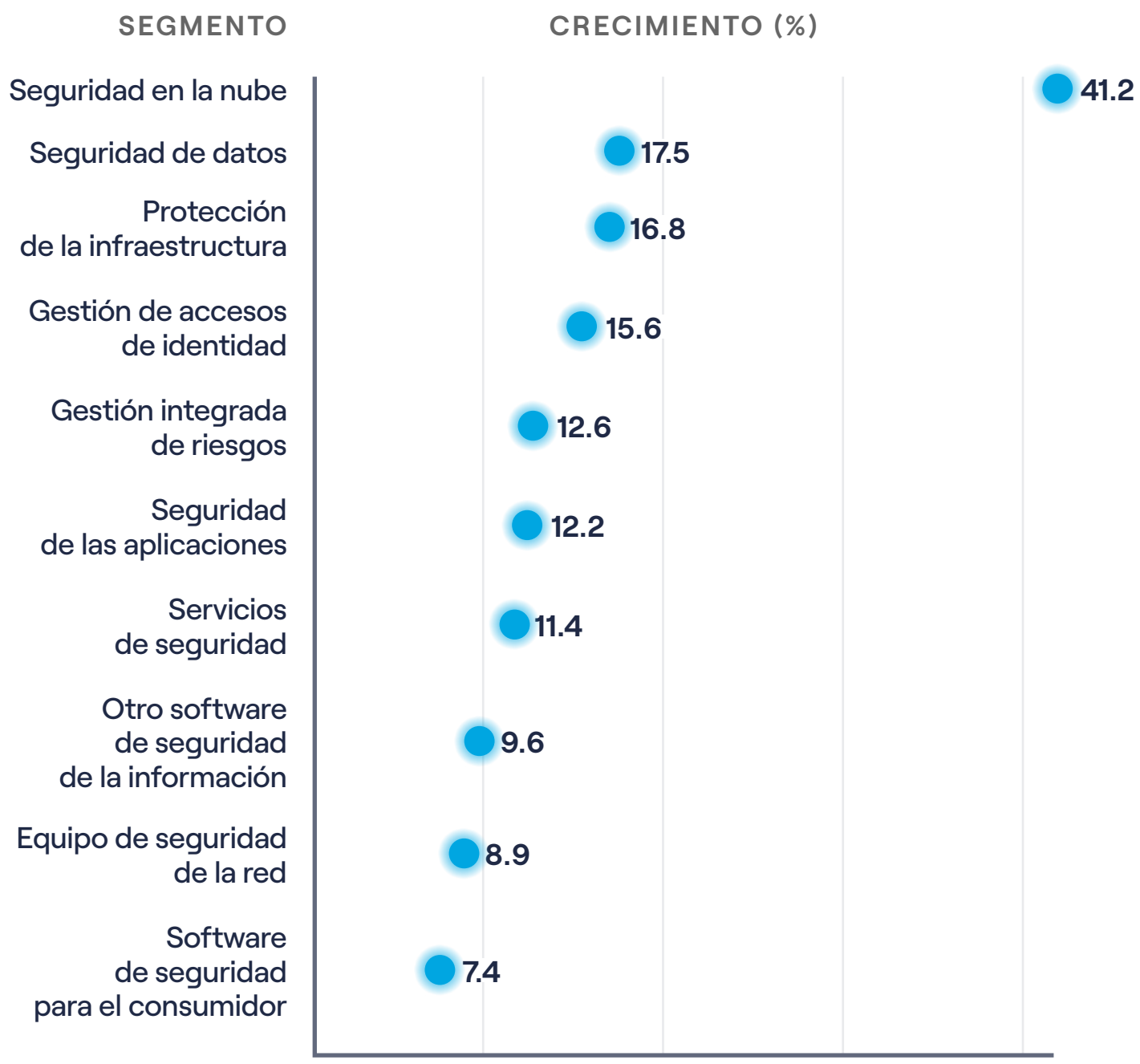
Lo que fue impulsado por el aumento de las necesidades de seguridad debido al trabajo remoto y a la migración de aplicaciones y servicios a la nube.

En los próximos años, además, se espera una mayor adopción de tecnologías como *machine learning* que, en conjunto con la inteligencia artificial, serán un gran apoyo para combatir ciberataques y detectar amenazas, explica Lawrence Pingree, vicepresidente administrativo de investigación de Gartner.

En ese sentido, SAP va a la vanguardia, pues ya incorpora algunas de estas tecnologías, junto con otros candados para incrementar la seguridad del sistema.

La ciberseguridad es la principal prioridad para nuevos gastos en las empresas, de acuerdo con la encuesta *Gartner 2021 CIO Agenda*. 61% de los encuestados señaló que incrementaron la inversión en seguridad de la información este año.

SEGMENTOS QUE TUVIERON MAYOR CRECIMIENTO EN EL GASTO EN 2021



Fuente: *Gartner, mayo de 2021.*

¿En qué te debes enfocar para mejorar la ciberseguridad?

Un plan integral para mejorar la seguridad de tu información y tus sistemas debe incluir diferentes elementos clave, los cuales veremos a continuación.

PLAN Y POLÍTICAS DE SEGURIDAD

El primer paso es definir las políticas de seguridad que guiarán a todos los departamentos de la empresa. Esto es para que todos estén en sintonía, busquen alcanzar los mismos objetivos y se rijan bajo el mismo reglamento.

Además, hay que trazar un plan con dos vertientes principales:

- ¿Qué hacer para prevenir un ciberataque?
- ¿Qué se debe hacer después para recuperarse de él?

Aunque muchas empresas sufren brechas de seguridad en sus sistemas, muy pocas son las que cuentan con este tipo de planes, con base en una encuesta realizada por McAfee:

32%
tienen un plan para prevenir incidentes de seguridad

19%
tienen un plan para responder ante incidentes de seguridad

44%
tienen ambos planes

1%
no tienen ningún plan

3%
no saben si hay algún plan

Cabe destacar que solo 32% consideran que los planes son realmente efectivos, por lo que hay que realizar varias pruebas, antes de sufrir un ciberataque real.

Seguridad física de las instalaciones

Al igual que con los accesos al software o los sistemas propiamente, la entrada a ciertas áreas, como los servidores, también debe estar restringida, así como llevar un control de quién accedió, fecha y hora.

Es indispensable llevar un control de qué usuarios usan ciertas computadoras, desde cuáles redes, si son trabajadores remotos o si lo hacen a través de la red de la empresa.

Para el acceso a estas áreas o a ciertos sistemas generalmente se usan los datos biométricos de los usuarios, como lectura de huellas digitales, escaneo de rostro, retina o registro de voz.

El uso de la biometría permite una identificación rápida y mucho más segura del usuario que está accediendo a determinado sistema.

Seguridad de las redes

Las redes pueden estar abiertas para quien sepa cómo acceder a ellas. Además, con tantas conexiones a internet a través de computadoras, teléfonos o tabletas, este puede convertirse en un punto débil para las empresas.

A través de un firewall se puede gestionar el acceso o detener las intrusiones de otras redes; al mismo tiempo que se supervisa la comunicación de los diferentes equipos con internet.

El uso de una VPN (Virtual Private Network) también puede ayudar a mantener la información privada; mientras que los empleados o ejecutivos pueden conectarse a recursos corporativos de forma mucho más segura.

Proteger
el software

Al cierre de octubre de 2020, 10.18% de los usuarios de computadoras a nivel mundial experimentaron algún ataque de malware, de acuerdo con datos de Kaspersky.

En ese mismo periodo, virus troyanos responsables de ransomware atacaron a 123,630 usuarios corporativos, esto sin considerar pequeñas y medianas empresas.

El ransomware es una de las amenazas más peligrosas para las empresas. Implica que el atacante tiene información confidencial de la organización y solicita un pago por devolverla y no publicarla.

Para evitar intrusiones se debe contar con programas antivirus y antimalware; correrlos periódicamente en todas las computadoras que accedan a la red e incluso en los teléfonos móviles.

Además, deben estar siempre actualizados, porque diariamente salen nuevas variantes de virus o nuevas familias de troyanos.

Otra recomendación es usar la propia seguridad que ofrecen los programas o sistemas que se tengan instalados.

Para acceder a algunos de ellos se requieren contraseñas o permisos de acceso. Lo ideal es que se usen contraseñas complejas, con una combinación de caracteres alfanuméricos y especiales, con mayúsculas y minúsculas.

La combinación debe ser aleatoria, sin ninguna relación con palabras existentes, o números que puedan relacionarse con el usuario.

En SAP se crean diferentes roles y perfiles, con lo que se puede asignar diferentes niveles de autorización, dependiendo del usuario. El rol o perfil creado sólo puede acceder a la información que está relacionada con su trabajo directamente y queda excluido de otros datos que pueden ser mucho más sensibles.

Una recomendación adicional es usar doble autenticación. Para ello, además de la contraseña, se envía al usuario una clave, ya sea a través de un mensaje de texto o correo, que debe introducir al momento del acceso.

Con ello se tejen varias capas de seguridad, que irán haciendo mucho más complicado a los ciberdelincuentes acceder a los sistemas de la empresa.

Proteger tu información

El ransomware es una de las mayores dificultades a las que se pueden enfrentar las organizaciones porque implica no sólo la pérdida de la información, sino la posible amenaza de que se haga pública.

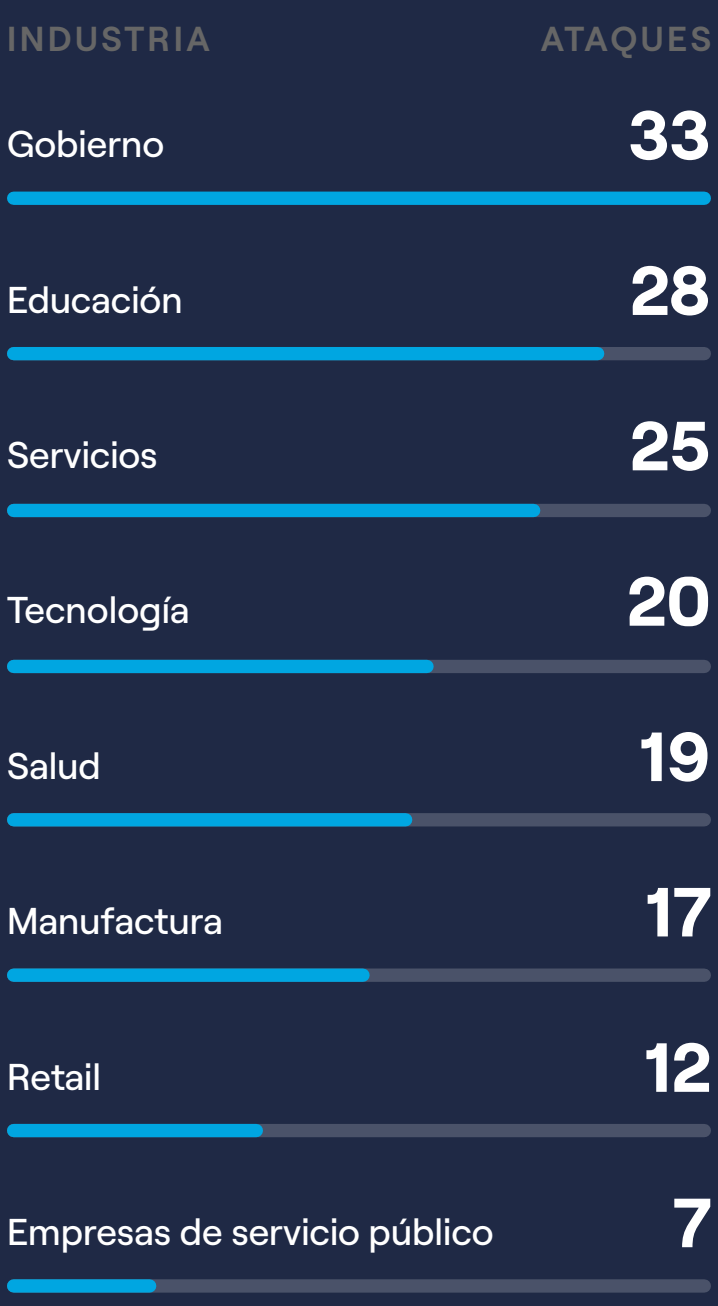
Si tienes en cuenta la gran cantidad de datos sensibles que se generan y manejan en tu sistema SAP, debes poner especial énfasis en este punto.

Otra modalidad de este tipo de ataques es que los ciberdelincuentes encriptan o hacen inaccesibles ciertos sistemas indispensables para la operación y sólo son liberados si se realiza un pago.

Si se trata de propiedad intelectual o secretos industriales, esto puede llegar a ser devastador para la organización.

En 2020, los sectores que sufrieron más ataques de ransomware a nivel global fueron manufacturación, Gobierno, servicios, educación y salud, de acuerdo con datos de la empresa especializada en ciberseguridad BlackFog, que realiza un rastreo de todos aquellos incidentes que se hacen públicos. Los sectores más atacados cambiaron en 2021:

ATAQUES DE RANSOMWARE POR INDUSTRIA (2021)



Fuente: *BlackFog, julio de 2021.*

Para proteger la información se emplean diversas estrategias. Deben realizarse copias de seguridad de las bases de datos de forma periódica; en caso de que ésta se vea comprometida, se recurre a la información almacenada y la pérdida no sería catastrófica.

Por otro lado, lo ideal es que toda la información sensible esté encriptada. Así, en caso de que haya una fuga de datos o haya sido robada, será difícil para los ciberdelincuentes acceder a ella o hacerla pública.

En ese aspecto, SAP permite crear copias de seguridad de las bases de datos de forma automatizada y almacenarla en la nube; asimismo permite la encriptación de cierta información para mayor seguridad.

Estrategias orientadas a los colaboradores

Muchas de las amenazas y las brechas de seguridad de las empresas vienen desde adentro, de sus propios empleados. Esto no significa que lo hagan de forma deliberada, a veces puede tratarse de algún error, desconocimiento de los procedimientos o falta de capacitación.

De acuerdo con el estudio *Insider Threat Report*, realizado por Verizon, existen cinco tipos de actores internos que pueden amenazar la ciberseguridad de las empresas:

EL EMPLEADO DESCUIDADO

Son aquellos que usan de forma indebida los recursos de la organización. Violan las políticas de seguridad, porque no las conocen o porque no las tienen muy presentes.

Por no ser cuidadosos, pueden instalar aplicaciones o software no autorizados por el área de TI, lo que crea puntos débiles en los que se puede recibir un ataque, aunque sus acciones no son maliciosas.

EL AGENTE INTERNO

Este puede ser un colaborador de otra empresa, ya sea que haya sido reclutado o sobornado por la competencia, para robar información de forma premeditada.

Su objetivo es filtrar información o vulnerar las defensas para que la entrada de ciberdelincuentes en los sistemas de la empresa sea mucho más fácil.

EL EMPLEADO DESCONTENTO

Personal que en un arranque de enojo, puede borrar información esencial para la organización o destruir otro tipo de datos, lo que derivaría en una interrupción de la actividad comercial.

EL EMPLEADO MALICIOSO

Es aquel que tiene acceso a información corporativa y que puede robarla para su propio beneficio. No necesariamente es que la vaya a entregar a la competencia, sino que puede usarla en el futuro para obtener alguna ganancia.

Generalmente tienen mayores privilegios para acceder a cierta información, que el común de los colaboradores.

EL EXTERNO IRRESPONSABLE

Se trata de algún socio comercial externo, que tiene acceso a la información de la empresa, y que hace un uso indebido de ella, puede ser deliberado o por negligencia.

Identificar a cada uno de estos colaboradores, te permitirá tomar acciones o medidas preventivas, para no sufrir un ataque o pérdida de información.

Asimismo, tu sistema SAP permite otorgar permisos específicos para cada usuario que tenga acceso, con ciertos niveles de seguridad, dependiendo de cuáles son las actividades que debe realizar.

El plan de seguridad de la empresa debe contemplar un reglamento interno que es necesario que sigan los colaboradores.

Debe ser del conocimiento de todos los empleados, sin importar su nivel, y debe estar firmado junto con los otros documentos, que se les entregan al momento de ser contratados.

Además, deben ser orientados sobre las buenas prácticas para mantener la seguridad de los dispositivos y software que tienen a su cargo. Hay que evitar dar por hecho que las personas saben cómo hacerlo.

LOS PRINCIPALES ELEMENTOS A CONSIDERAR SERÍAN:

- En los dispositivos de la empresa solo se usen los correos corporativos y se evite el uso de correos personales, porque estos últimos son mucho más difíciles de rastrear.

- Debe evitarse la descarga de cualquier tipo de software sin la autorización del área de TI, que es la encargada de proporcionar los programas que los colaboradores requieran para su trabajo diario.

- Otra recomendación es que se evite acceder a redes sociales en los dispositivos de la empresa. Esta es una de las principales brechas por las que pueden entrar los ciberdelincuentes.

- Evitar abrir enlaces de remitentes desconocidos que lleguen al correo o al teléfono móvil. Incluso, aunque el remitente sea conocido, si no se está esperando recibir nada de él, primero hay que preguntar qué está enviando y si es seguro acceder a él.

- Para ciertas industrias o departamentos, sobre todo aquellos involucrados con propiedad intelectual o tecnología, debe limitarse el uso del teléfono móvil personal dentro de las instalaciones.

El futuro de la ciberseguridad

Los delincuentes cibernéticos también se han vuelto mucho más sofisticados, por lo que las empresas deben recurrir a los avances tecnológicos que sean mucho más efectivos.

Para mantener la seguridad se emplean herramientas como *machine learning* de la mano con inteligencia artificial para crear patrones de uso y conexión de los usuarios. Si llega a presentarse alguna anomalía, se detecta de inmediato y se informa de una posible brecha a los administradores del sistema.

Con el internet de las cosas, también pueden identificarse los dispositivos interconectados y su ubicación. Si se identifica algún dispositivo irregular o una ubicación no reconocida, está es bloqueada de inmediato.

SAP también puede configurarse con estos niveles de seguridad para resguardar mucho más la información que se maneja dentro del sistema.

Mantener la seguridad de la información y datos de tu empresa es indispensable, por lo que nunca debe minimizarse el riesgo potencial.

Si necesitas un socio estratégico que te ayude a optimizar la seguridad de tus sistemas SAP, puedes contar con nosotros. En Novis, tenemos un equipo certificado con las mejores prácticas para manejar tu sistema y sacarle el mayor provecho.

Acércate a nosotros y permítenos diseñar una estrategia justo a la medida de los requerimientos tecnológicos que tiene tu negocio.

Fuentes:

- *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*
- *https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem*
- *https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf*
- *https://f.hubspotusercontent40.net/hubfs/1624046/2021_SoCIO_ExS_R2.pdf*
- *https://go.forrester.com/what-it-means/ep231-rise-of-ransomware/#*
- *https://enterprise.verizon.com/resources/executivebriefs/insider-threat-report-executive-summary.pdf*
- *https://www.blackfog.com/the-state-of-ransomware-in-2021/#July*
- *https://www.blackfog.com/the-state-of-ransomware-in-2020/*

NOVIS

www.novis.com.mx

/NovisMexicoSAP /novis-corp