LAC4
Latin America and Caribbean Cyber Competence Centre

Funded by the European Union

Nota conceptual
Evaluación de ciberseguridad y prioridades para las PYMES en la región Andina

Fecha: 13-15 de mayo 2026. **Formato:** Presencial
Borrador: 27 de febrero de 2026. **Contacto:** César Moliné Rodríguez (cesar.moline@lac4.eu)

Antecedentes:

Los ciberataques en la región Andina han ido en aumento en los últimos años, lo que refleja las tendencias globales donde los ciberdelincuentes atacan cada vez más a empresas, instituciones gubernamentales y particulares. La región ha experimentado un auge en la digitalización, acentuado por la pandemia de COVID-19, lo que la hace más vulnerable a las amenazas cibernéticas, a la vez que carece de una infraestructura robusta de ciberseguridad.

En la era digital actual, las pequeñas y medianas empresas (PYMES) se convierten cada vez más en blanco de ciberataques. Las amenazas de ciberseguridad, como las filtraciones de datos, el ransomware, el phishing y las amenazas internas, están impactando significativamente a las PYMES, provocando pérdidas financieras, daños a la reputación e interrupciones operativas. Sin embargo, a diferencia de las organizaciones más grandes, las PYMES a menudo carecen de los conocimientos y los recursos necesarios para protegerse eficazmente de estas amenazas.

Muchas PYMES también operan bajo la falsa suposición de que son demasiado pequeñas para ser blanco de los ciberdelincuentes, lo que resulta en una atención inadecuada y una falta de inversión en ciberseguridad.

Sin una evaluación de riesgos adecuada ni medidas de seguridad implementadas, las PYMES son vulnerables a ciberataques, lo que puede generar importantes desafíos operativos y financieros.

Además de los riesgos operativos, el incumplimiento de las medidas de ciberseguridad puede afectar las perspectivas de negocio de las PYMES. La reciente Ley de Ciberresiliencia de la Unión Europea regula que todos los productos y servicios digitales vendidos en la UE deben estar diseñados con sólidas medidas de ciberseguridad. Se están debatiendo requisitos similares en Estados Unidos. Por lo tanto, las empresas latinoamericanas que deseen operar en estos mercados deben cumplir con estas normas de "seguridad desde el diseño".

Resumen y objetivos:

Basado en la herramienta Marco para la evaluación del nivel de seguridad (F4SLE), desarrollada parcialmente en el marco del proyecto CHESS[1] de Estonia y Chequia, financiado por la UE, un taller presencial de evaluación de ciberseguridad de 2,5 días para PYMES reunirá a un grupo de emprendedores motivados de países centroamericanos con la ambición de expandir su mercado a la UE o EE. UU. para evaluar los riesgos cibernéticos de sus empresas y brindarles herramientas para establecer prioridades claras y planes de acción para mitigar dichos riesgos.

La herramienta F4SLE, compatible con la norma ISO/IEC 27001, la norma estonia de seguridad de la información E-ITS y las sugerencias del Informe del Panorama de Amenazas de ENISA, y brindará a los emprendedores la oportunidad de autoevaluar sus niveles de riesgo de ciberseguridad y obtener una visión general de su situación, además de centrarse en las dimensiones vulnerables de la gestión de la seguridad.

El modelo de prueba de concepto de F4SLE está disponible desde 2021 y se ha probado en Estonia y Chequia entre 2023 y 2024. La herramienta F4SLE también se utilizó para la evaluación de ciberseguridad como herramienta adicional en el proyecto piloto de transformación cibernética de PYMES NCC-EE, realizado por un evaluador (https://www.ria.ee/kuberturvalisus/riiklik-koordinatsioonikeskus-ncc-ee/kuberpoore .

Puede encontrar información adicional sobre el instrumento F4SLE en los siguientes enlaces:

- Entorno de prueba de la herramienta: https://mass.cloud.ut.ee/test-massui/#/
- Concepto base: https://link.springer.com/content/pdf/10.1007/978-3-031-05760-1_39.pdf?pdf=inline%20link
- Método de actualización: https://www.sciencedirect.com/science/article/pii/S0920548923000570
- Historias de usuario preliminares: https://dl.acm.org/doi/pdf/10.1145/3600160.3605045

Durante la capacitación presencial, se abordará la seguridad de la información desde una perspectiva multidisciplinar: además de los aspectos técnicos de la evaluación de riesgos, se impartirán conferencias temáticas sobre la cadena de suministro segura y los riesgos de la IA. Se prestará especial atención al contexto social, las barreras internas y la necesidad de concienciación sobre

[1] Centro de Excelencia en Ciberseguridad en Estonia y Moravia del Sur, Chequia, en asociación con universidades y centros nacionales de ciberseguridad de Estonia y Chequia.

ciberseguridad en la alta dirección como factores esenciales para generar un cambio impactante en la postura sobre ciberseguridad.

Además de limitar los riesgos comerciales y operativos, una sólida estrategia de ciberseguridad permitirá a las empresas operar en otros mercados importantes, como la UE..

Público objetivo

PYMES de países de la región andina: Bolivia, Colombia Ecuador y Perú:

- Con componentes digitales en sus productos o servicios o que dependen de soluciones digitales en su producción.

- Con alcance internacional e interés en expandir sus mercados a la UE y/o EE. UU.

El taller tendrá un máximo de 40 participantes. Dos personas de cada PYME (una con nivel técnico y otra con nivel empresarial/de gestión).

Antes del taller, es obligatorio completar la herramienta del marco F4SLE.

Duración: 2,5 días

Entregables

La capacitación tiene una duración de dos días y medio y consta de sesiones teóricas e interactivas.

Antes de la capacitación presencial, se recopilarán datos de los participantes para evaluar sus conocimientos sobre la materia. Es obligatorio completar el marco F4SLE.

Seis meses después de la capacitación, se realizará un seminario en línea con el público objetivo para evaluar su progreso y compartir las mejores prácticas.

Temas a tratar

El seminario abordará los siguientes temas clave:

- Introducción a la seguridad de la información
- Estándares y legislación en materia de seguridad de la información
- Resumen de la herramienta F4SLE y su aplicación
- Seguridad de la cadena de suministro
- IA y ciberseguridad
- Esquemas Zero trust