

	<p>Total estimated cost: EUR 3,998,959</p> <p>Total amount of EU budget contribution EUR 3,380,000</p> <p>This action is co-financed in joint co-financing by the Inter-American Development Bank (IDB) for an amount of EUR 618,959 This includes: EUR 279,903 from IDB Lab contingent recovery funding for investment, and EUR 339,056 corresponding to the counterpart provided by NUMU S.A. as the implementing body for the project.</p>
MANAGEMENT AND IMPLEMENTATION	
14. Type of financing	Indirect management with Inter-American Development Bank (IDB) IDB Lab

1.2 Summary of the Action

<p>El Salvador faces significant cybersecurity challenges, with cyber-attacks causing an estimated economic damage of 0.5-1 % of gross domestic product GDP. The lack of an adequate legal framework, limited infrastructure, and a shortage of specialized human resources are barriers to deal with these challenges efficiently.</p> <p>Improving the framework for better cybersecurity in El Salvador will have an important cross-cutting positive impact on the country's digitalization efforts, currently ongoing with significant EU support.</p> <p>The action will be implemented in indirect management with the innovation laboratory of the InterAmerican Development Bank (IDB Lab), which has already successfully implemented a similar action in Panama with EU private sector partners.</p> <p>The CYBERLAMARR project proposes to develop the ecosystem and create cybersecurity-related jobs in El Salvador, with an emphasis on improving women's participation in the sector and expanding access to reliable and affordable cybersecurity services for the productive sector in El Salvador, especially small and medium-sized businesses (SMEs). It will firstly implement capacity development on cybersecurity skills with a specific focus on young men and women. Secondly, it will promote the development of cybersecurity services in the country's private sector.</p> <p>The proposed solution consists of creating and expanding the Regional Cybersecurity Center of Excellence (CREC) to El Salvador, which has been operating in Panama since 2022, offering services for skills development, employability, cybersecurity services and cyber risk awareness. CREC has achieved important results to date, with a strategic innovation for Panama, including artificial intelligence as part of the training and service offer following the exponential growth of AI in all industries including of course SMEs.</p> <p>The action strategy consists of three pillars, based on the IDB Lab experience in Panama, including: (I) specialized training in cybersecurity and digital industries; (II) awareness raising and effective job integration strategies for the provision of cybersecurity services and the awareness of cyber risks; and (iii) strengthening El Salvador's cybersecurity ecosystem.</p> <p>The project is the first intervention in El Salvador focused on developing local cybersecurity talent, with a model tested in Panama. In addition, it seeks to provide cybersecurity services to SMEs and to develop a cybersecurity ecosystem with international standards. It also entails a gender strategy to promote closing the gap in women's participation in the technology industry.</p> <p>To support SMEs, the project will include a strategy and resources to raise awareness about the growing cyber risk and ways to prevent it with cybersecurity services based on feasibility analyses and the implementation of the first stage of a Regional Centre for Artificial Intelligence (RCAI). These efforts will target organizations from various sectors - with an emphasis on SMEs- and will be a key element of the project that will drive both the establishment of partnerships for training and employability, as well as commercial efforts to identify early adopters of the services. The program will also seek to develop the cybersecurity ecosystem through dialogue roundtables with the participation of public and private actors (including SMEs) to energize the sector, harmonize the vision, generate relevance of the importance of cybersecurity and generate inputs for an updated regulatory</p>
--