

INDRA PROTECTS THE CELL PHONES OF MORE THAN 12,000 EXECUTIVES AND AUTHORITIES AGAINST THE RISK OF BEING SPIED ON

- **Its COMSec solution offers end-to-end encryption for voice communications, messages and files. Easy and convenient to use, it is compatible with any operating system and smartphone model**
- **The company completes the protection of the terminal with a cyberintelligence and security service, monitoring the configuration of the cell phone and using biometric identification of the user's behavior to detect any anomalies or theft**
- **Hacking a cell phone is the cheapest and most effective way of spying on negotiations, gathering information about a person's movements, listening through the phone's microphone or spying through its camera**

Madrid, July 4, 2018. Indra protects more than 12,000 mobile terminals against the risk of being spied on, a growing problem, which has become the most effective and cheapest way of spying on the telephone negotiations between companies, gathering information about a person's movements, and accessing meetings unnoticed, simply by hacking the cell phone's camera and microphone.

Indra is the leading company in the field of secure communications and a provider of state-of-the-art market solutions aimed at guaranteeing comprehensive protection for the cell phones of executives and professionals who handle sensitive information about their company's business and operations.

Many business agreements, mergers and commercial strategies are discussed over a cell phone. Professionals use this device constantly to share information about the development of new products or the state of legal proceedings in progress. If this information were to be leaked, it would have a direct impact on the company's income statement as well as the success or failure of operations in which months of work have been invested. And yet people are generally unaware of the fact that the camera or microphone of a cell phone left on the table during a meeting can be activated remotely.

At the same time, smart terminals are becoming increasingly powerful. Their memory records the calls made and how long they last, as well as the user's movements, work agenda, messages, photos, documents and emails.

For cyber-delinquents they are the best way of finding out a company's plans, practically in real time: all they need to do is hack a professional's cell phone to follow internal work meetings and telephone conversations with customers.

There are also certain tech startups that are offering their services on the black market to hack cell phones remotely and listen to calls. It has therefore become essential for professionals who handle strategic information to protect their phones properly.

More than 12,000 senior executives and professionals of Ibex companies and authorities, as well as Spanish government officials, have chosen Indra's COMSec solution to do this. The application is compatible with any operating system and smartphone model, is very convenient and easy to use, and offers end-to-end encryption for voice communications, messages and files. It can be used to establish multi-conferencing and video calls and create communications rooms for holding secure meetings. It can use mobile, Wi-Fi or satellite communication networks and is compatible with all other cell phone applications, such as the agenda, camera or email apps.

Indra's system is so efficient that it can even improve the connection establishment process in countries or areas of low coverage and at times when the networks are saturated or out of service. It also reduces the cost of international calls since they are made by exchanging data packets.

To guarantee complete cell phone security, Indra also provides a cyberintelligence and mobile security service, monitoring the phone configuration, connections, degree of vulnerability, permissions granted to the apps installed, and much more.

The solution also analyzes how each person uses their cell phone to identify any anomalous situation. The purpose of this function is to learn about connection patterns such as the apps and devices used most frequently, therefore establishing genuine "behavior biometrics" to detect whether the cell phone has been stolen or is being accessed by third parties. In providing this solution and related services, the company relies on the work of its digital transformation business unit, Minsait, which employs one of the most highly acclaimed teams of cybersecurity experts in the country and has an international network of advance cybersecurity centers, or I-CSOC, that are operational 24/7/365.

Lastly, to protect the security of cell phones in high-risk countries, the solution includes geolocation systems which the user can activate if necessary so that Indra can monitor the phone to prevent hacking.

About Indra

Indra is one of the world's top technology and consulting companies and a technology partner for the key operations of its customers' businesses worldwide. It is a leading worldwide provider of proprietary solutions in niche areas in transport and defense markets and the absolute leader in IT in Spain and Latin America. It offers a comprehensive range of proprietary solutions and cutting-edge services with a high added value in technology based on a unique culture of reliability, flexibility and adaptability to its customers' needs. Indra is a world leader in the development of end-to-end technology solutions in fields such as Defense and Security, Transport and Traffic, Energy and Industry, Telecommunications and Media, Financial Services, Electoral Processes, and Public Administrations and Healthcare. Minsait is Indra's digital transformation business unit. In 2017, Indra posted a revenue of €3.011 billion, employed 40,000 professionals, and had a local presence in 46 countries plus sales operations in more than 140 countries.