

JORNADA STIC

CAPÍTULO COLOMBIA

Soluciones de comunicaciones
seguras en situaciones de
teletrabajo en movilidad



En colaboración con:





Roberto Casado Rodríguez

Indra

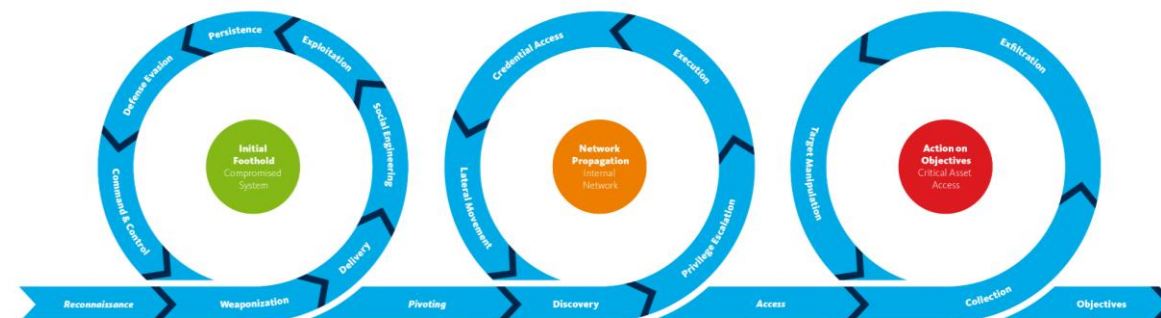
rcasador@Indra.es

Ciberseguridad

Pensamos que estamos preparados...

- ✓ Estrategias
- ✓ Procedimientos
- ✓ Herramientas

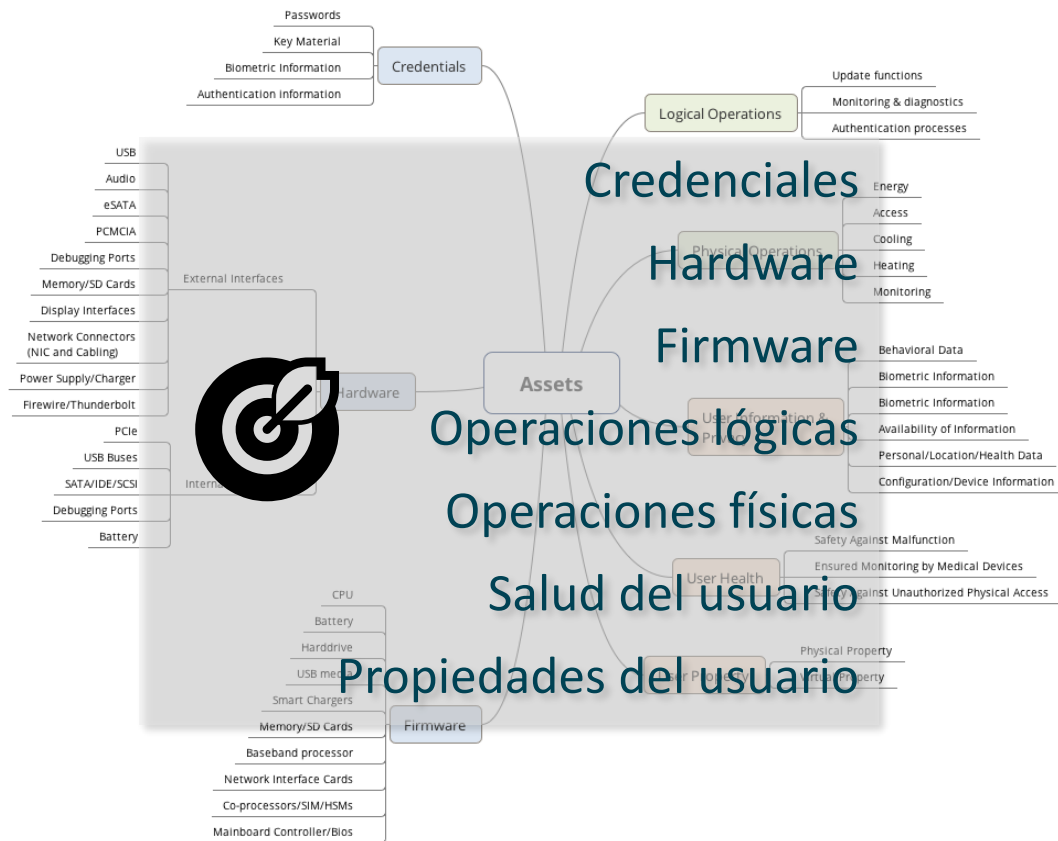
Marcos, planes de contingencia, movilidad, protección de datos...



Pero... ¿tenemos una falsa sensación de seguridad?

Múltiples activos, amenazas reales

Hardware, software, información, dispositivos...



Amenazas por tipos de activos. Fuente: ENISA

Don't use these Android VPNs. They Leak Your Credentials!

By CISOMAG - March 2, 2021

Microsoft Teams Vulnerability Let Hackers "Take Over Entire Roster of Teams Accounts"

Microsoft Teams Remote Code Execution Vulnerability

CVE-2020-17091

Security Vulnerability

Released: Nov 10, 2020 Last updated: Nov 12, 2020

WhatsApp And Telegram Flaw Exposes Personal Media To Hackers, Check Settings Now



Zak Doffman Contributor

Cybersecurity

I write about security and surveillance.



The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley

12 de febrero de 2021 5:00

Y un nuevo escenario

Pandemia + Teletrabajo

“mayor uso de soluciones en la nube, conexiones VPN, servicios de escritorio remoto virtual (VDI), redes de confianza cero y gestión de identidades, servicios y tecnologías para el acceso remoto, uso de herramientas colaborativas, aplicaciones de videoconferencia, etc.”

Fuente: [CCN](#)

Espionage

NSO Group points finger at state clients in WhatsApp spy

In court filing, Israeli spy operate technology it pr

Remote Threats to Remote Employees: How Working From Home Increases the Attack Surface

5 Ways Mobile Devices are the Biggest Threat to Cybersecurity

24 March 2020, 11:01 am EDT By Staff Reporter Tech Times

Home > Mobile Security

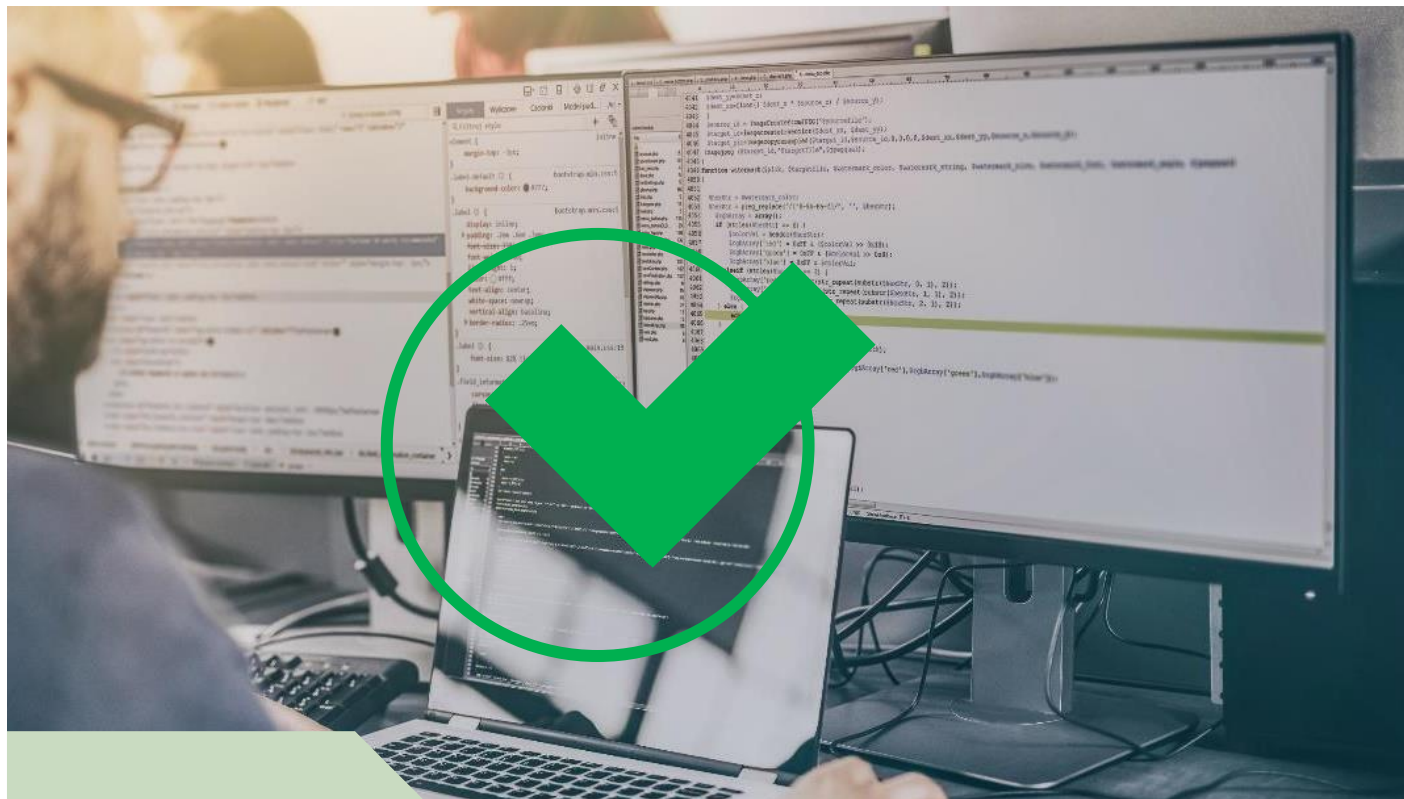


Hackers Can Manipulate Media Files Transferred via WhatsApp, Telegram

Empresas y Gobierno, desprotegidos ante el teletrabajo: "Faltan medios y ciberseguridad"

Be careful what you talk about on Slack! Firm releases a new policy that lets bosses read employees' direct messages WITHOUT their consent

Protegemos redes y equipos



Información e
infraestructura



**Ataques de red, esnifado de paquetes,
ataques *man in the middle***

¿Qué solemos proteger en un
Plan de Seguridad de una
organización?

- **Red corporativa:** Cortafuegos, DMZ, VPNs, IDS / IPS, etc.
- **Puestos de trabajo:** antivirus, identificación y roles, políticas de seguridad, cifrado de información, etc.
- **Seguridad de infraestructura:** cifrado de BBDD, controles de acceso a plataformas...

... pero ¿y los móviles?



¿Cómo hablan por teléfono nuestros directivos? ¿Qué app de mensajería usan? ¿Son apps corporativas o de consumo? ¿Tengo control sobre ellas?

- Los escenarios de movilidad hacen los sistemas más vulnerables a los ataques
- Se necesita **proteger canales de comunicación no controlados por la organización**

Dispositivos
móviles



Escuchas, suplantación, espionaje
industrial, pérdida de información...



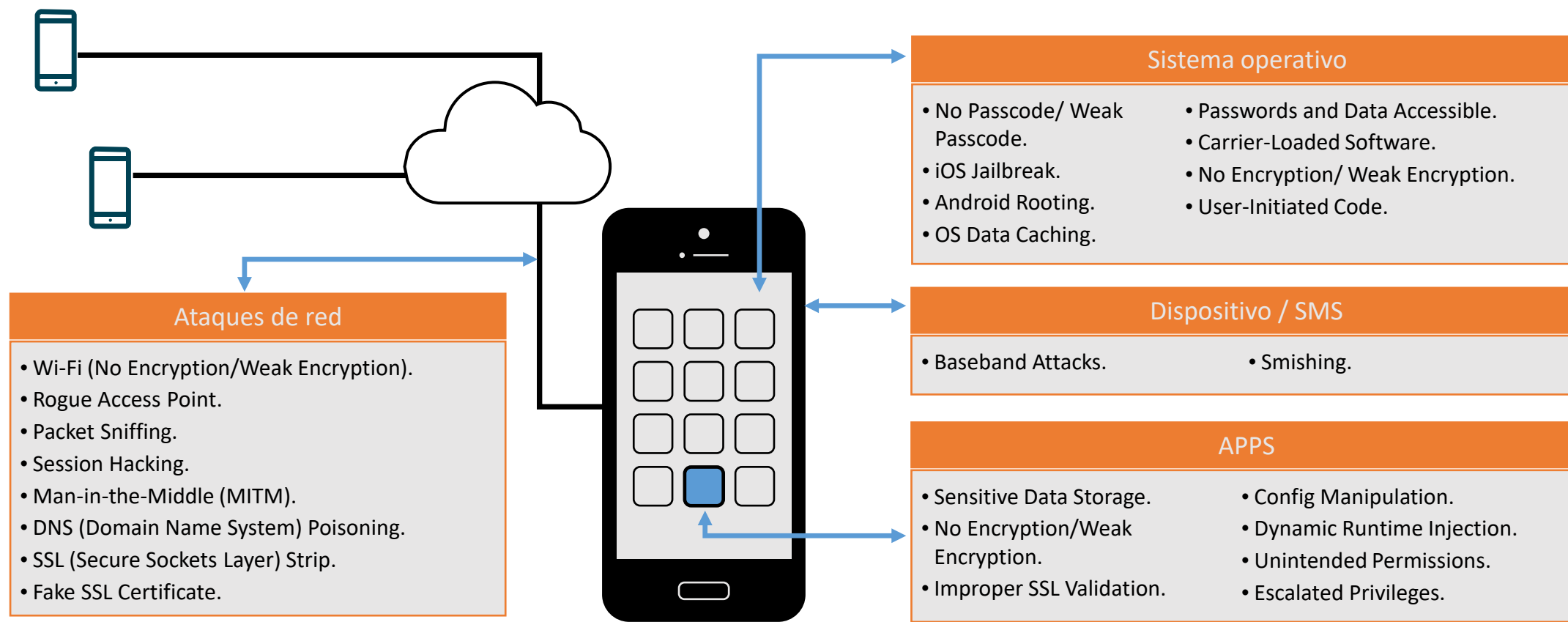
Comunicaciones y sus riesgos

Ámbitos *personal* vs *profesional*

	Comunicaciones PROFESIONALES	Comunicaciones PERSONALES	Riesgos principales
Publicidad, Malware	No	Posible	Ataques z-day, troyanos
Privacidad	Obligatorio	Muchas apps recopilan información personal, listas de contactos, información de red, ubicación, etc.	Brecha de información, espionaje industrial
Seguridad	Por diseño (servidor, app y protocolos). La seguridad no es sólo el cifrado	Incluida como “mejora”. La seguridad no es la prioridad.	Pinchazos
Configuración del Servicio	Posible (control de acceso, servicios, roles, etc.)	No	Experiencia limitada no ajustada a uso
Calidad de Servicio	Obligatorio y certificado	Mejor esfuerzo	Servicio inadecuado o pobre
Soporte Técnico Especializado	Disponible	No	Caída de servicio, ausencia de SLA
Infraestructura	Información disponible, o servidores instalados en el centro de datos del cliente	Información <u>no</u> disponible. Los servidores <u>no</u> pueden ser controlados por el cliente.	Dependencias no controladas, violación de GDPR, propiedad intelectual
Auditorías	Permitidas	No	Acceso a metadatos, espionaje empleados
Actualizaciones	Pueden ser controladas por el cliente	Automáticas, por el market público.	Caída de servicio, pérdida de funcionalidad

Riesgos en el móvil

Necesitamos un enfoque global que proteja todas las superficies



Solo estamos seguros si protegemos todos los niveles



Qué es COMSec (Indra)

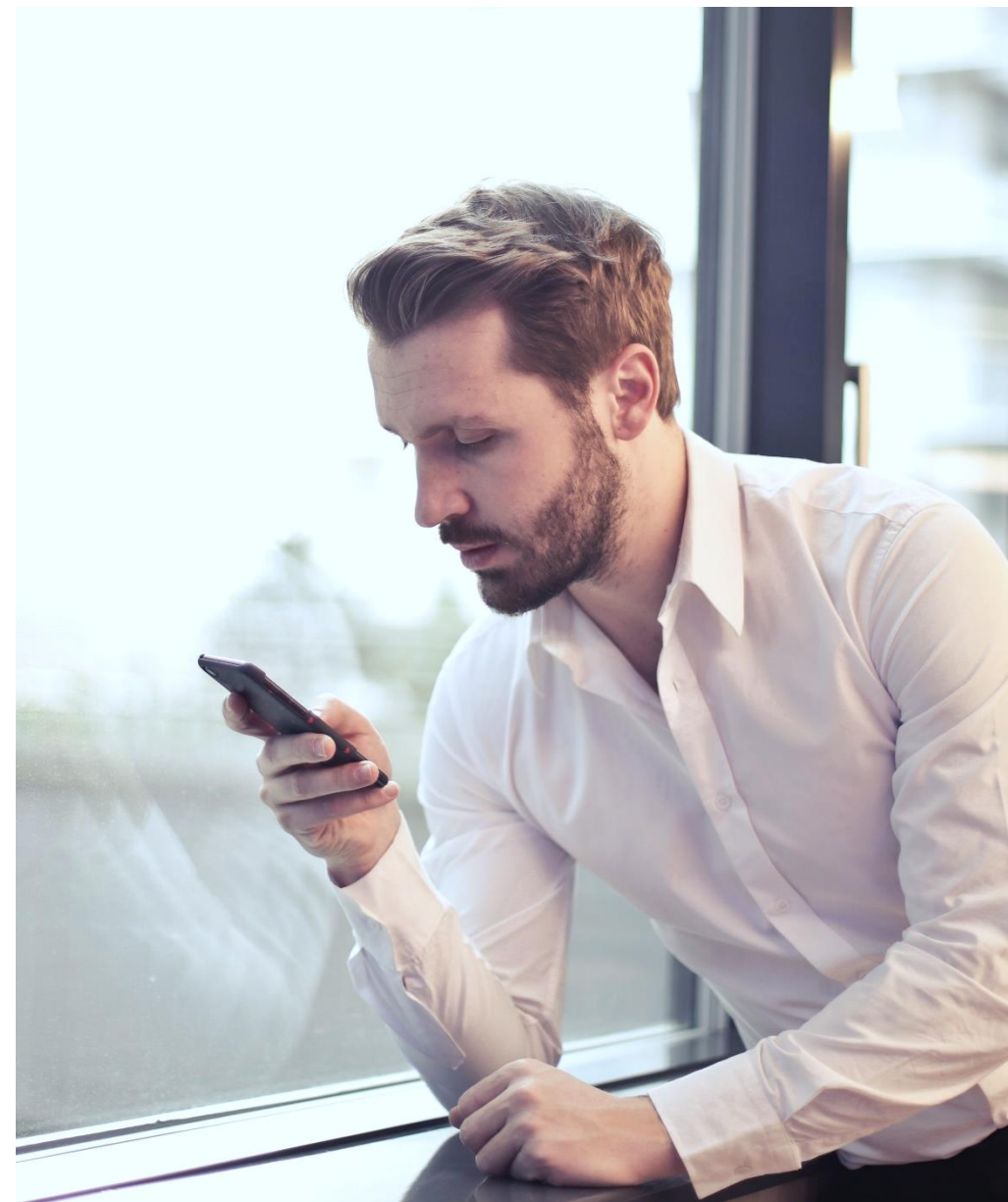
Comunicaciones seguras de voz, vídeo, mensajería instantánea e intercambio de ficheros. El sistema está diseñado y optimizado para plataformas móviles.

El sistema se compone de:

Aplicación cliente COMSec, instalada en el smartphone de los usuarios (Android, iOS) o PC (Windows)

Operador virtual IMS, encargado de interconectar los usuarios

Servidor de Telefonía Unificada STU, una pasarela para integrar COMSec con la PBX corporativa



+15 años de
experiencia en
Comunicaciones
Seguras de alto nivel



COMSec



COMSec Admin+



Difusión Limitada



Common Criteria



NATO Restricted

Qué puedo hacer con COMSec

Usabilidad estándar



Audio

- Voz cifrada E2E
- Protección hacia números públicos
- Salas de conferencia seguras o salas de crisis



Vídeo

- Videollamadas cifradas E2E
- Transmisión cifrada de vídeo



Chat

- Mensajería instantánea individual y de grupo
- Fotos, vídeos, ficheros, notas de voz, ubicación
- Mensajes especiales

Protección de información sensible



Cifrado de extremo a extremo
para proteger las llamadas de COMSec a COMSec, e impedir la interceptación de la comunicación usando algoritmos de máxima seguridad (AES-256, Curvas elípticas, SHA-2, ECDHE, RNG cumpliendo FIPS-140...).

Arquitectura inhouse

La infraestructura COMSec puede ser desplegada en el centro de datos del cliente.

Defensa en profundidad

El sistema soporta varias capas de seguridad, uso de contenedores, modo kiosco, seguridad lógica por un MDM, protección de la comunicación por COMSec y un APN privado, protección del propio dispositivo (Samsung Knox por ejemplo), etc.

Certificaciones:

- Common Criteria.
- **ENS-ALTO** (Nivel alto para información sensible a nivel nacional)*
- Certificación nacional [**Difusión Limitada**], para información clasificada**
- **NATO Restricted.**



* CCN-STIC 105 – CPSTIC Catálogo de productos de seguridad TIC del CCN.

**CCN-STIC 1407 – Procedimiento de empleo seguro COMSec.

Por qué COMSec tiene una gran aceptación



Fácil de usar.

Interfaz intuitiva, adaptada a cada plataforma siguiendo sus reglas de diseño.

Sobre el propio terminal del usuario.

Sistema multiplataforma, con versiones específicas para Android, iOS y PC. COMSec es compatible con las aplicaciones del teléfono (contactos, correo, agenda, cámara, etc.).

Rápido y fiable.

Establecimiento casi instantáneo de la llamada, muy baja latencia, y funciona incluso con redes muy lentas.

En cualquier lugar del mundo.

Con terminales 2G/3G/4G/WiFi, COMSec se puede utilizar en cualquier país. Soporta también redes satelitales como Iridium, Inmarsat, etc.

Económico.

Coste de las comunicaciones casi nulo con tarifas nacionales. Costes muy limitados en roaming por el muy bajo ancho de banda necesario.

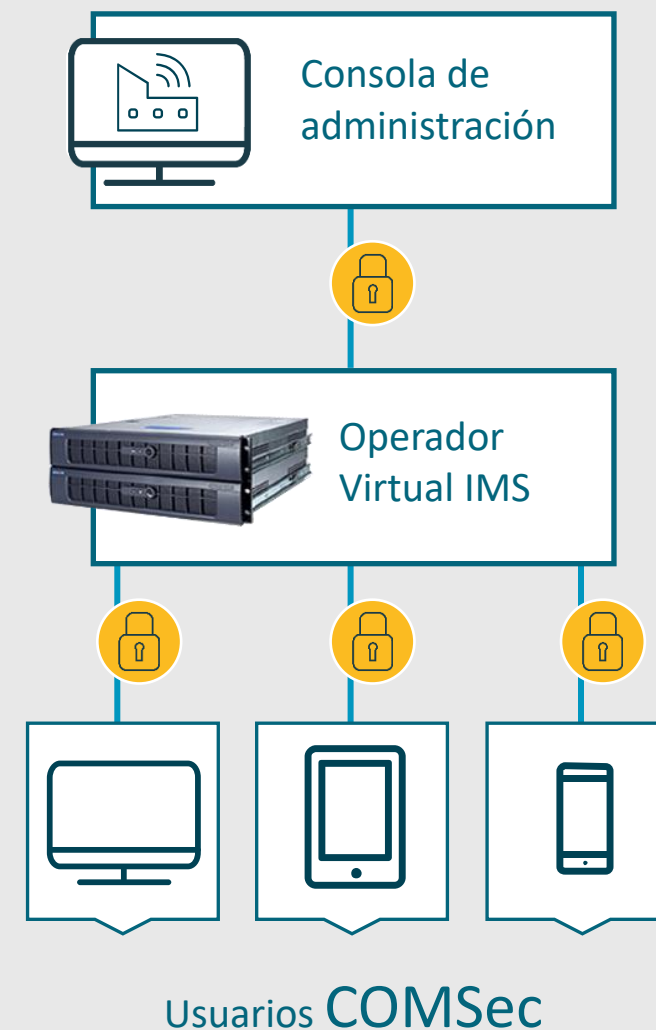
Personalizable.

Customización de la app para adaptarse a la imagen corporativa

IMS

Operador virtual privado, núcleo del sistema

- Gestión de los usuarios.
- Control de acceso.
- Visibilidades.
- Prioridades.
- Control de las llamadas.
- Transferencia de mensajes.
- Administración del sistema.
- Plan de numeración personalizado.
- Cumplimiento de LOPD.
- Registro y autenticación en tiempo real.
- Servidor de presencia.
- Gestión de señalización.
- Gestión de IPs dinámicas.
- Gestión de políticas de contraseñas.
- Independencia del dispositivo.
- Sin necesidad de número público.



STU

Servidor de Telefonía Unificada, protege también llamadas a teléfonos normales

Llamadas protegidas hacia cualquier teléfono de la red pública

Los usuarios COMSec pueden **llamar a teléfonos normales** marcando simplemente su número.

Llamadas protegidas a extensiones corporativas

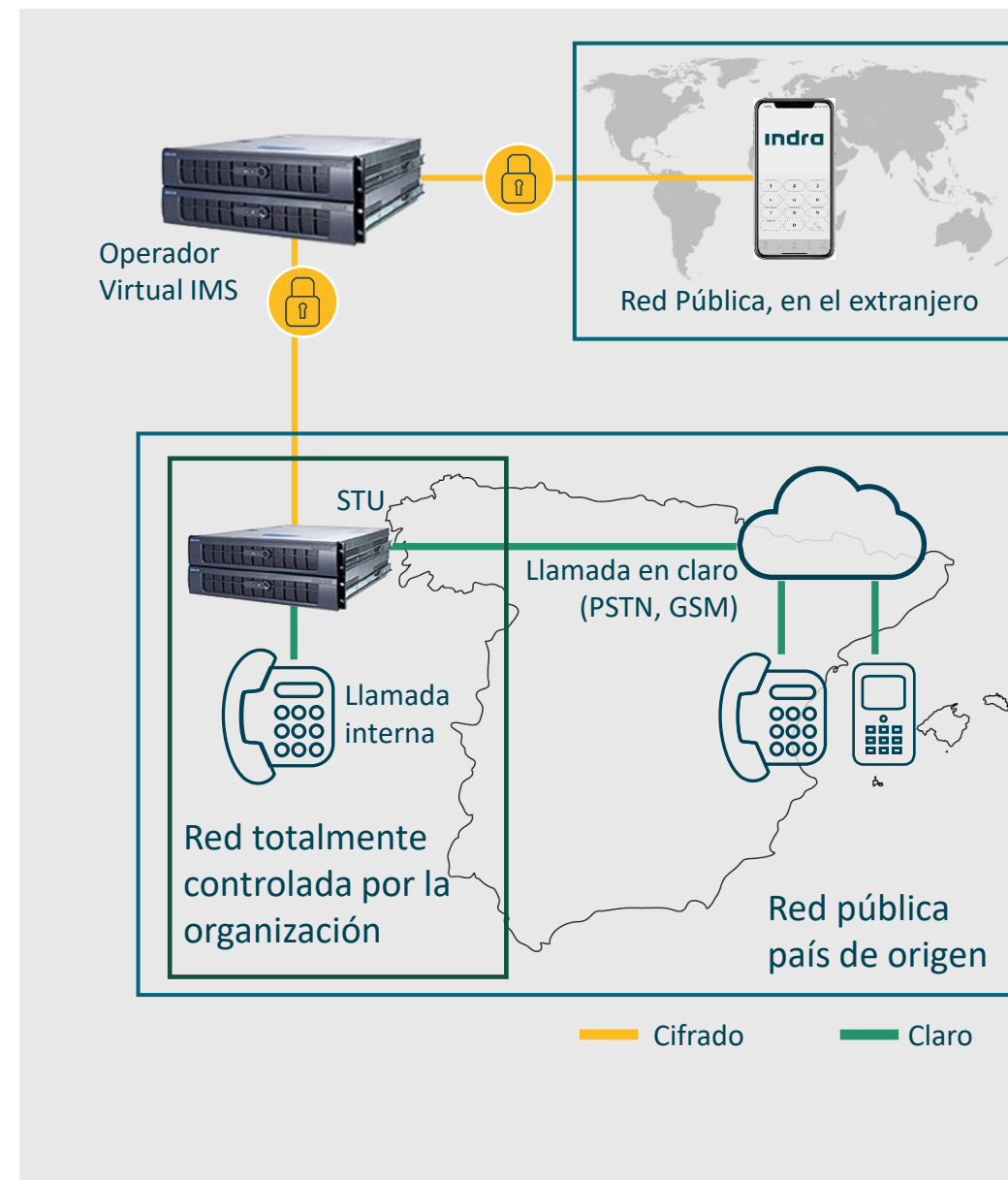
Permite llamadas entre COMSec y cualquiera extensión interna de la organización.

Protección total en el extranjero

Evita la interceptación por operadores extranjeros al llegar cifrado hasta la infraestructura corporativa.

Llamadas de datos sin trazabilidad

Pasando desapercibido ante posibles sniffers de red.



Federación

Comunicación entre organizaciones gracias a la federación de sus IMS

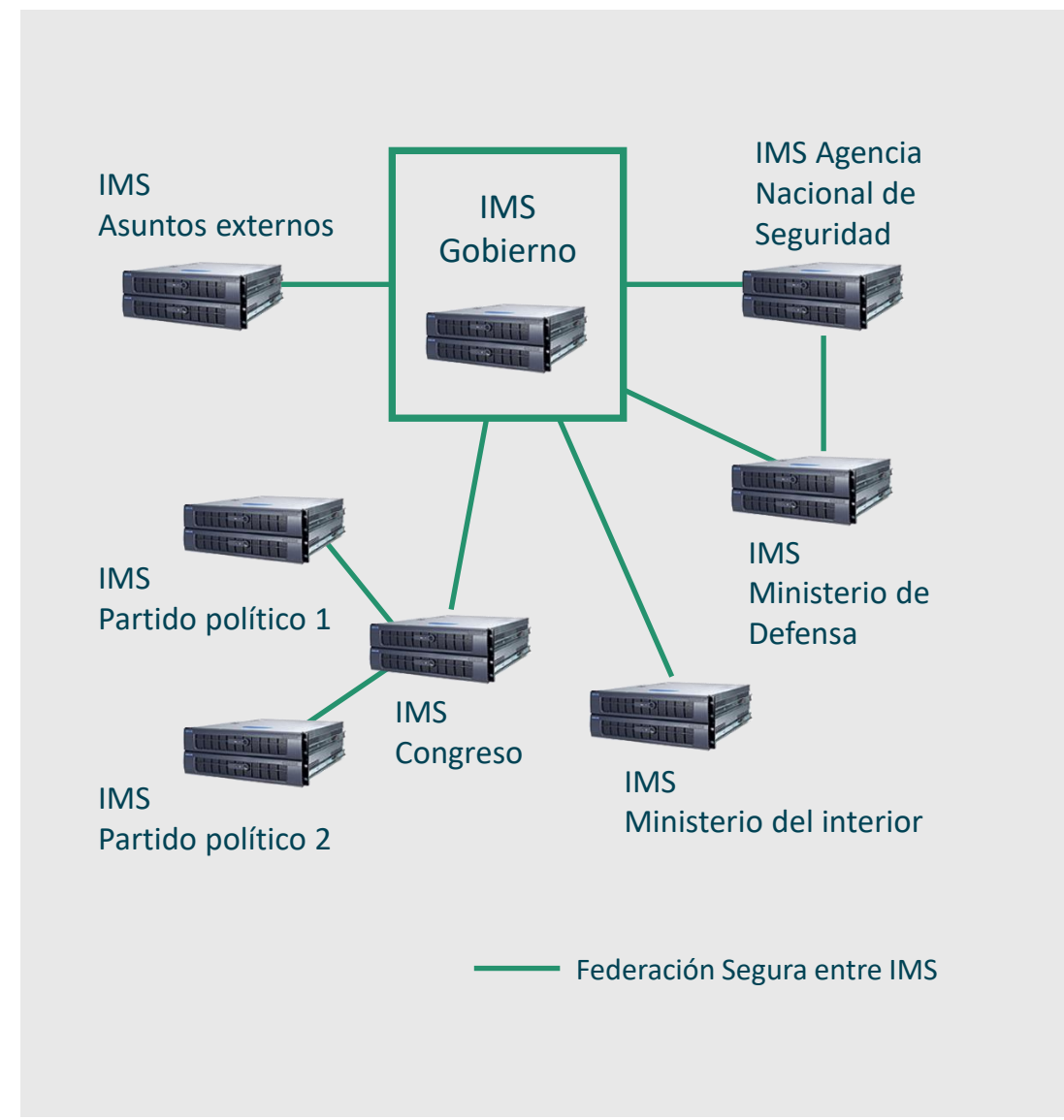
Comunicaciones seguras con determinados usuarios de otros IMS

Permite realizar comunicaciones con otros organismos o empresas con los que se tengan negocios en común.

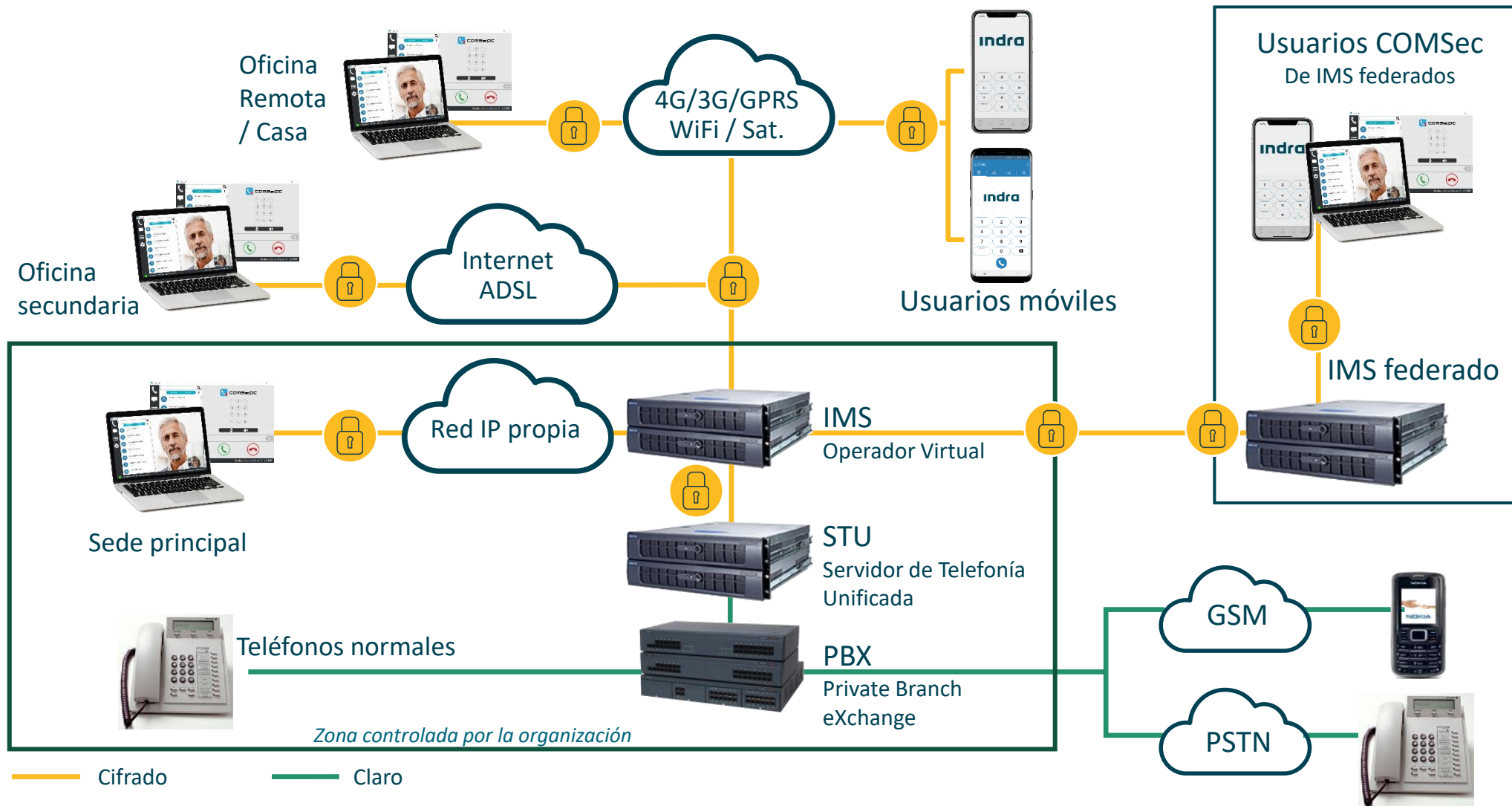
El administrador local conserva el control total de su IMS

Un acuerdo mutuo entre los administradores local y remoto es requerido para definir cómo conectar los usuarios importados desde un IMS remoto (**visibilidad simétrica o asimétrica**).

El acuerdo puede ser revocado en cualquier momento, desde cualquiera de los administradores (local o remoto).



Arquitectura global



Características

Arquitectura in-house, totalmente controlada por el cliente

Privacidad total para los usuarios, no se transmiten datos personales del teléfono (agenda, contactos, etc.)

Sin trazabilidad de llamada con protocolos y señalización propietarios

Integración con PBX del cliente para conexión con la red pública y el resto de la organización.

Cifrado de tu mensajería instantánea corporativa desde tu móvil o PC

Información no en claro en ningún punto del sistema ni accesible por los administradores

Federación gestionada con otros servidores COMSec, manteniendo el control total de la red COMSec propia

Protección de información ENS Alto y hasta **Difusión limitada**

Criptografía asegurada por entidades independientes de referencia.

No se encuentra en markets públicos por seguridad del código, desplegándose mediante MDM o portal de descarga privado.

Defensa en profundidad: compatible con MDM, Samsung Knox, para una protección adicional



JORNADA STIC

CAPÍTULO COLOMBIA

GRACIAS



En colaboración con:

