Ciber-Resiliencia de los sistemas ATM

Enfocado en los riesgos de vulnerabilidad de los ANSPs

Del 4 al 6 de Diciembre 2018
Ciudad de México

Índice

¿Quiénes somos?

- Corporativo

1

Corporativo

Indra es la multinacional de consultoría y tecnología líder en España y Latinoamérica.
Agrupamos nuestra oferta en las áreas de **Transporte**, **Tráfico Aéreo**, **Defensa & Seguridad** y toda nuestra oferta TI en **Minsait**.

La empresa en cifras…

- **3.011M€** en ventas
- Inversión en I+D entre **5% al 8%** de las ventas
- Más de **200 acuerdos** con centros de investigación y Universidades
- Presencia con proyectos en **160 países**
- Con Oficinas en **45 países**
- **77 Centros** de Excelencia y SW-Lab

Talento Global…

- **97** Nacionalidades
- **40.000** profesionales
- **80%** profesionales de alta cualificación

Portafolio ATM

- Soluciones para tránsito aéreo
- Automatización
- Comunicación
- Navegación
- Vigilancia

2

Soluciones para tránsito aéreo

Conectamos personas, lugares y cielos, haciendo que todo funcione.

Player Global - Soluciones Innovadoras - Beneficios Ambientales

Automatización	Comunicación	Navegación	Vigilancia
			
Tu socio tecnológico en Tráfico Aéreo	Implementamos soluciones Full VoIP Dual Dissimilar VCCS	Facilitamos más de 100 millones de aterrizajes seguros	Hemos desplegado más de 400 sistemas de vigilancia

+4000

Instalaciones en más de 160 países

+100

Años de experiencia en soluciones ATM

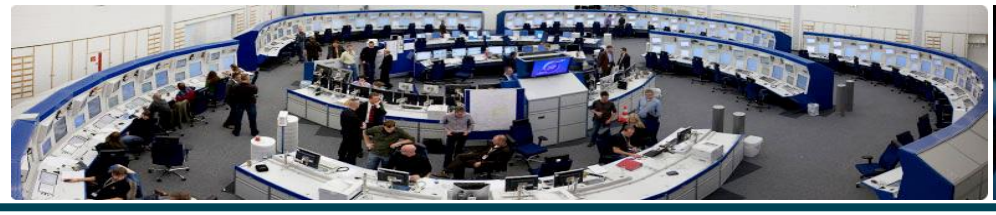
+85%

Pasajeros en el mundo viajan utilizando la tecnología de Indra, en algún momento del vuelo

Automatización

Creamos sistemas inteligentes y fiables en un entorno cada vez más complejo, cumpliendo las normas y prácticas recomendadas de la Organización de Aviación Civil Internacional (OACI), así como EUROCONTROL.

- Nuestros sistemas utilizan múltiples fuentes de vigilancia tales como SSR, PSR, SMR, MLAT/WAM, ADS-B y una avanzada fusión de datos multisensor para proporcionar una vigilancia completa de superficie del aeropuerto (TWR), aproximación (APP) o en ruta (ACC).
- Los sistemas de automatización y simulación, entre otros servicios (ej. AMHS, AIM, IFPS o ATFM), instalados por todo el mundo nos han posicionado como líderes globales, contando con la confianza para gestionar los espacios aéreos más congestionados y complejos, como por ejemplo las rutas de Europa.

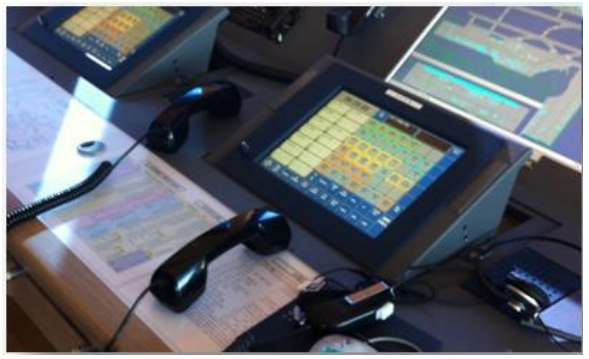


Comunicación

Proporcionamos soluciones de comunicación automatizada para los controladores y otros participantes del Tráfico Aéreo a través de nuestro sistema de control y comunicación por voz (VCCS)

Entre nuestros productos VCCS se encuentra la familia de sistemas VCCS GAREX, que ofrece la funcionalidad de comunicaciones de GTA completa, y ha sido desarrollada a lo largo de los 50 años que GAREX cuenta con la consideración en todo el mundo de proveedor de soluciones de comunicaciones funcionales, seguras y fiables.

- Sistema de comunicación: Familia GAREX
- Sistemas de grabación multicanal: Familia NEPTUNO



Navegación

Indra ha creado una completa gama de productos de ayuda a la navegación de la familia NORMARC que incluye la última generación de sistemas ILS , DME , DVOR y GBAS

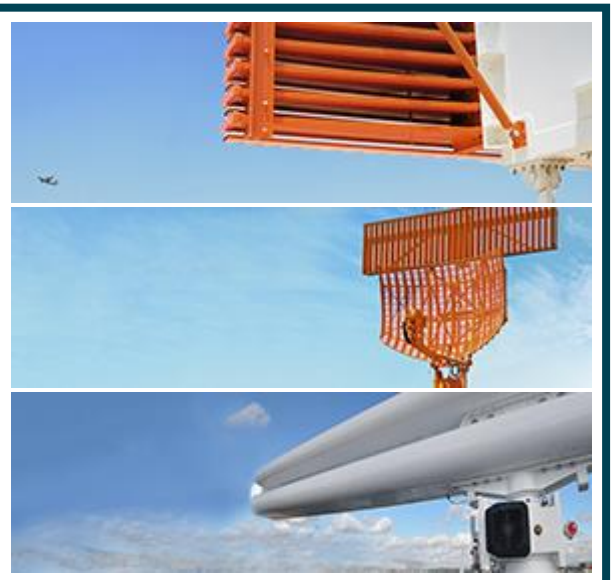
- Nuestros sistemas NORMARC ILS han sido una referencia industrial durante más de 20 años.
- Más de 100 millones de aterrizajes seguros con la ayuda de los sistemas de aterrizaje por instrumentos NORMARC en casi 1.200 aeropuertos de todo el mundo.
- Se han instalado los sistemas DVOR y DME de Indra más de 600 veces en todo el mundo y su reciente versión actualizada convierte a estos sistemas en los más avanzados del mercado.

Vigilancia

Nuestras soluciones de vigilancia mejoran la seguridad y eficiencia del tráfico aéreo creando soluciones de vigilancia avanzadas y fiables para nuestros clientes

Somos una de las pocas empresas del mundo que fabrica e integra toda la gama de sistemas de vigilancia que necesita el mercado de Gestión del Tráfico Aéreo (GTA), y contribuye activamente al desarrollo de la tecnología de vigilancia del futuro.

- Sistemas Radares Primarios/Secundarios/Superficie
- MLAT/WAM
- ADS-B
- Etc.



Oferta en ciberseguridad

- Capacidades
- Operaciones
- Soluciones tecnológicas
- Diseño de soluciones
- Capacitación y entrenamiento
- Explotación
- Respuesta

3

Capacidades

Nuestras capacidades en ciberseguridad

Gestionamos todo tipo de amenazas a través de soluciones innovadoras de ciberseguridad.

Operaciones	Soluciones Tecnológicas	Diseño de Soluciones	Capacitación & Entrenamiento	Explotación	Respuesta
• Asesoría & Consultoría de política y procedimientos • Acreditación y Certificación • Auditoría • Análisis de riesgos y vulnerabilidades	• Tecnologías y herramientas • Arquitecturas de seguridad • Sistemas de protección • Infraestructuras seguras	• Despliegue y configuración de sistemas • Despliegue de centro de operaciones de seguridad • Operación de servicios	• Concienciación • Programas de Formación y entrenamiento • Simulación de escenarios de Ciberseguridad	• Ciberinteligencia • Conciencia Situacional • Análisis y minería de datos • Big Data	• Respuesta a incidentes • Análisis Forense • Análisis de Malware • Herramientas de respuesta

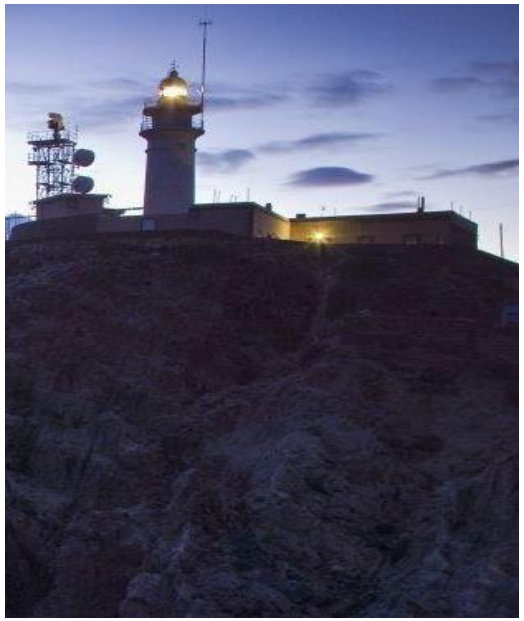
Indra ha sido seleccionada por la Agencia de Comunicaciones e Información de la OTAN (NCIA) para integrar la red de empresas que colaboran en materia de ciberseguridad.

Operaciones

Nuestros expertos pueden desarrollar e implantar políticas, procesos, procedimientos y planes de seguimiento para monitorizar y garantizar el cumplimiento de los objetivos de seguridad.

Consultoría y Asesoría

- **Políticas** para el desarrollo de estrategias de alto nivel
- **Procedimientos** a seguir para evitar errores
- **Análisis y Gestión** de riesgos
- **Hacking ético y Auditoría** de vulnerabilidades
- **Certificación y Acreditación** de productos y sistemas
- **Metodologías y Herramientas** para el desarrollo, uso y administración de sistemas seguros



PARA CUMPLIR LOS OBJETIVOS

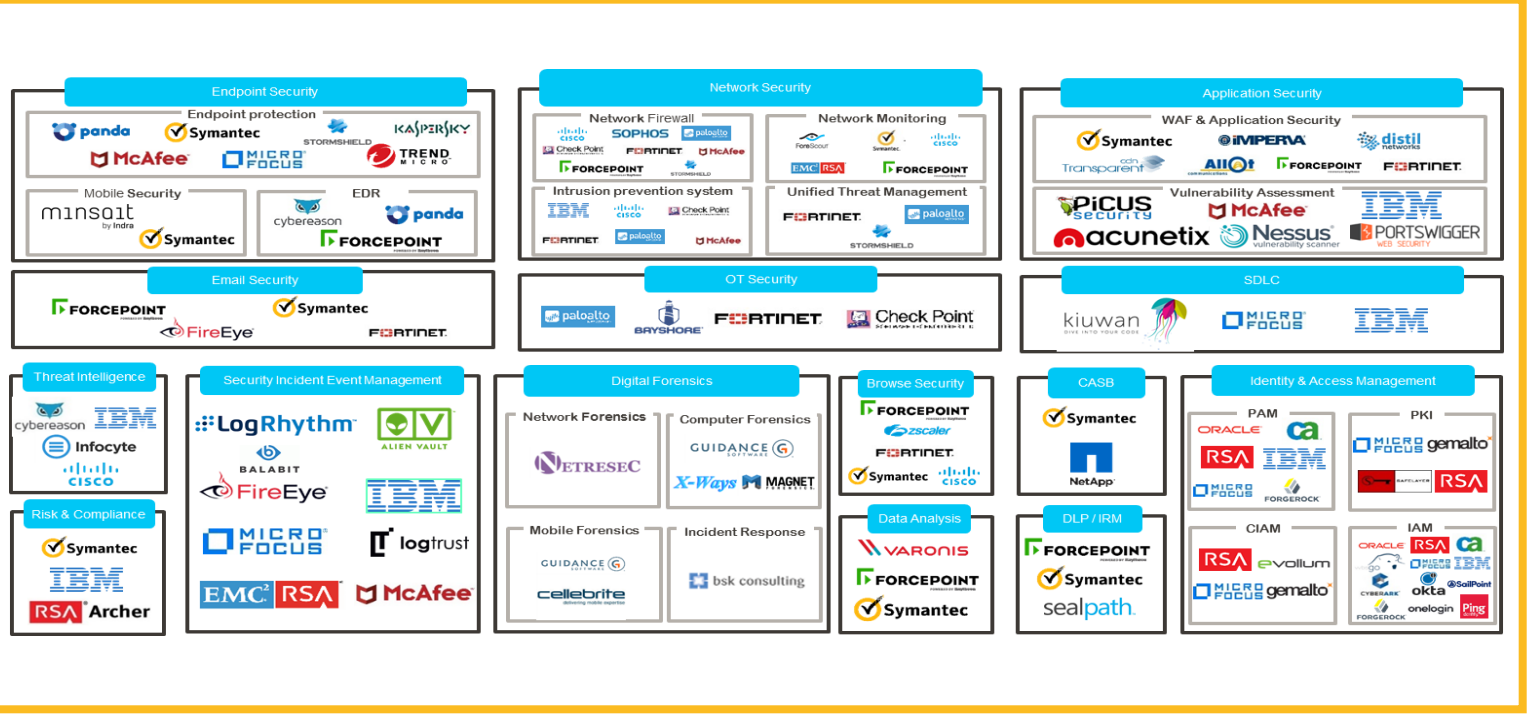
- **Asegurar y proteger los activos** informáticos
- **Minimizar los riesgos para los sistemas TIC**
- **Mejora continua en la postura de seguridad**

Soluciones tecnológicas

Indra diseña arquitecturas de seguridad personalizadas al entorno y a las necesidades de usuario

Diseño, instalación e integración de soluciones tecnológicas de Ciberseguridad:

- Sistemas de prevencion de ataques y protección
- Redes de sondas de detección
- Soluciones de almacenamiento y correlación de eventos
- Entornos de análisis y experimentación
- Herramientas de reacción, recuperación y respuesta

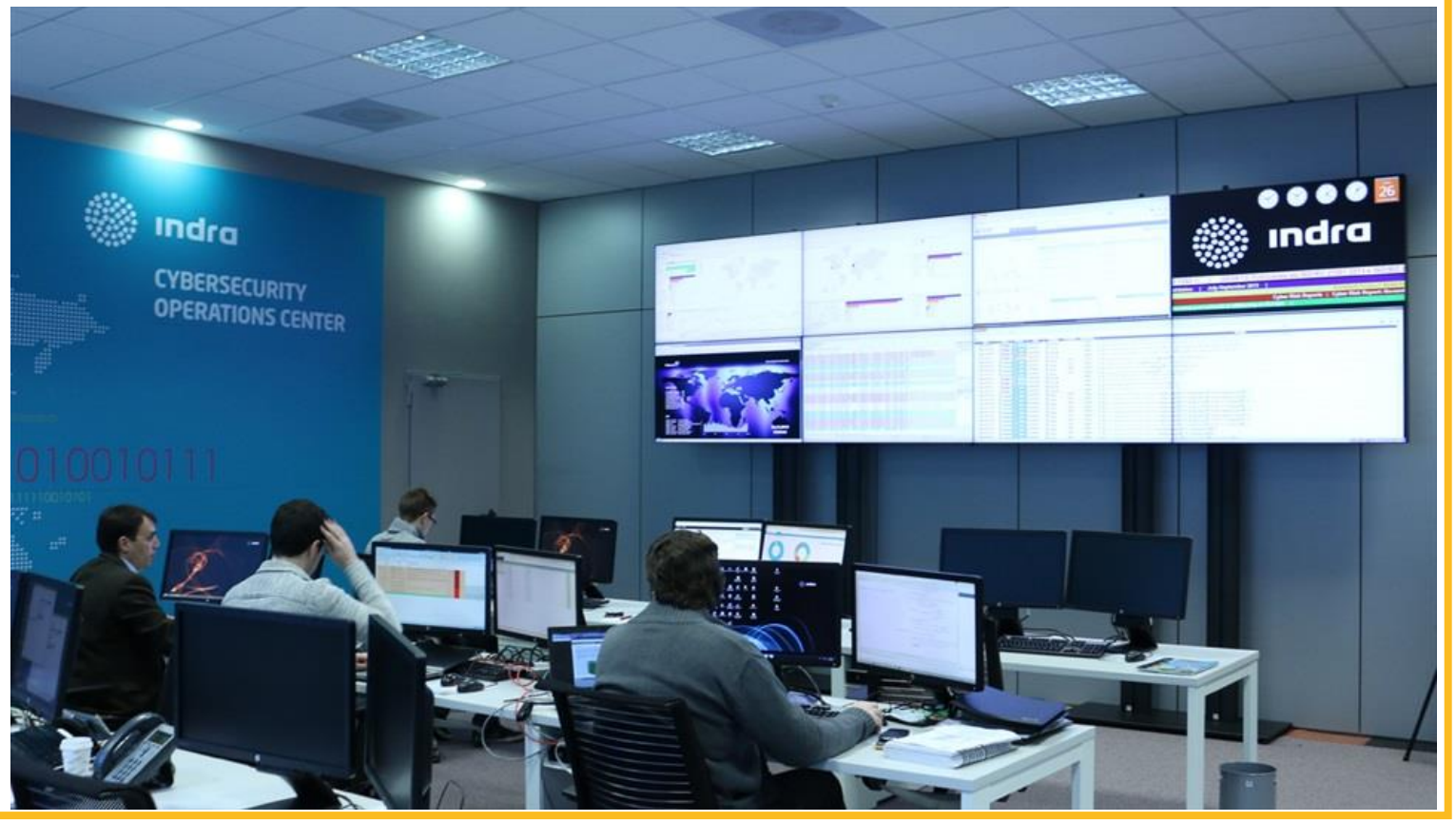


Diseño de soluciones

Indra diseña, instala e integra centros de Ciberseguridad (SOC / NOC)

Diseño, suministro e instalación de centros de Ciberdefensa

- Adecuación de instalaciones
- Protección fisica y control de acceso
- Infraestructuras seguras
- Redes y sistemas del centro
- Cloud y virtualización



Capacitación y entrenamiento

Cyber Range - Plataforma de formación y entrenamiento en entornos operativos reales

Es la plataforma de simulación de ciberseguridad de Indra.
Proporciona escenarios reales para ayudar a las organización a mejorar las destrezas, conocimientos y habilidades de sus ciber-equipos, tanto a nivel técnico como organizativo, por medio de una formación estructurada y ejercicios prácticos para enfrentarse a amenazas reales.

Sobre la plataforma, se proporcionan 3 capacidades diferentes que se pueden combinar:

Cyber Range Academy

Perfecciona los equipos de ciberseguridad a través de un proceso continuo y flexible de formación práctica
Maximiza los resultados con rutas de formación adaptables en base al conocimiento, habilidades y capacidades de cada individuo.
Todos los ejercicios y rutas de formación siguen el marco de trabajo de seguridad cibernética NICE (NCWF)

Cyber Range Challenger

Establece competiciones individuales o en equipos para evaluar y mejorar la capacidad de ciberseguridad para responder a las amenazas del mundo real.
Entrenamiento usando las tácticas, técnicas y procedimientos más comunes a los más recientes y más sofisticados de los adversarios

Cyber Range Battlefield

Practicas en escenarios de primera línea de fuego

Crea misiones que imiten el concepto de operaciones, probando la ciberseguridad en ejercicios competitivos y colaborativos, en un entorno personalizado con sistemas comerciales y ad-hoc al sector.

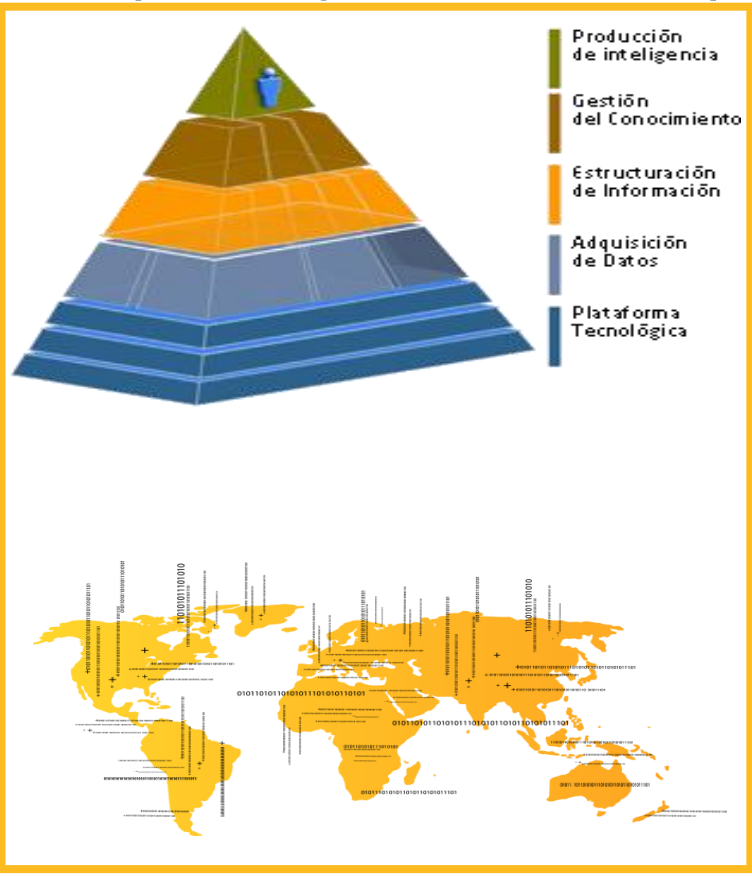
Explotación

Las soluciones de Indra en Ciberinteligencia y Conciencia Situacional se basan en productos propios de la empresa y nuestra amplia experiencia en sistemas

Ciberinteligencia y alerta temprana

Es una herramienta de inteligencia que ofrece la mejor calidad de información para facilitar la toma de decisiones:

- Tratamiento, clasificación y pre-análisis de información mediante un equipo de analistas
- Identificación temprana de ciberamenazas, análisis posterior y comunicación eficaz a los usuarios
- Clasificación y ponderación de la gravedad de las diferentes amenazas



Conciencia Situacional

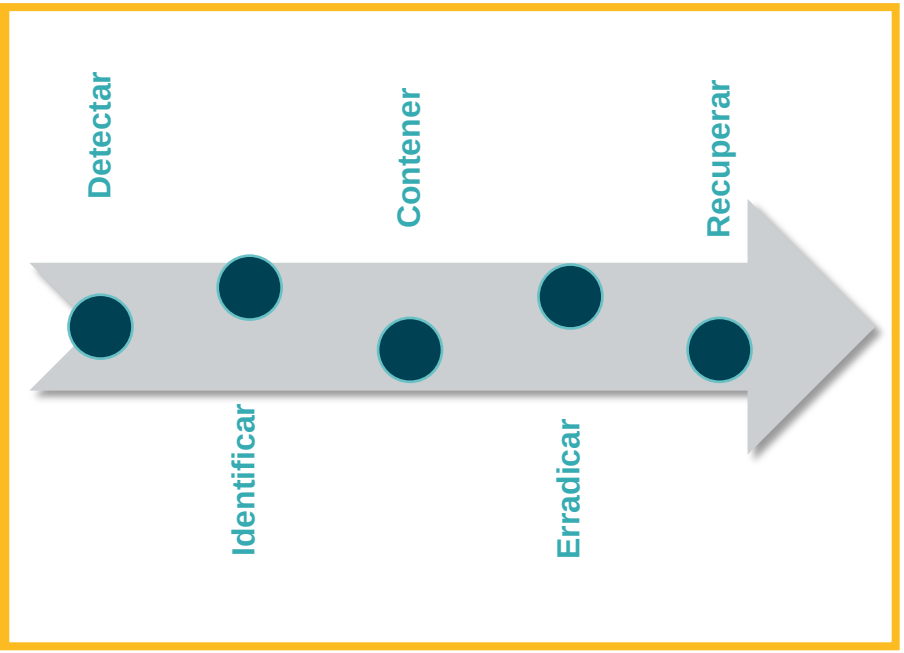
Análisis dinámico de riesgos ofrece una visión en tiempo real de las amenazas a las que los sistemas y redes están expuestas
Los varios elementos están integrados en una consola única de situación (CROP) para poder reaccionar ante amenazas

Respuesta

Completando el ciclo de vida de Ciberdefensa, Indra ofrece capacidades de reacción y respuesta contra ciberataques

Respuesta ante incidentes

- Equipos de Reacción Rápida para identificar, contener y erradicar el ataque
- Servicios y Herramientas de Análisis forense y malware
- Entornos dedicados de Análisis



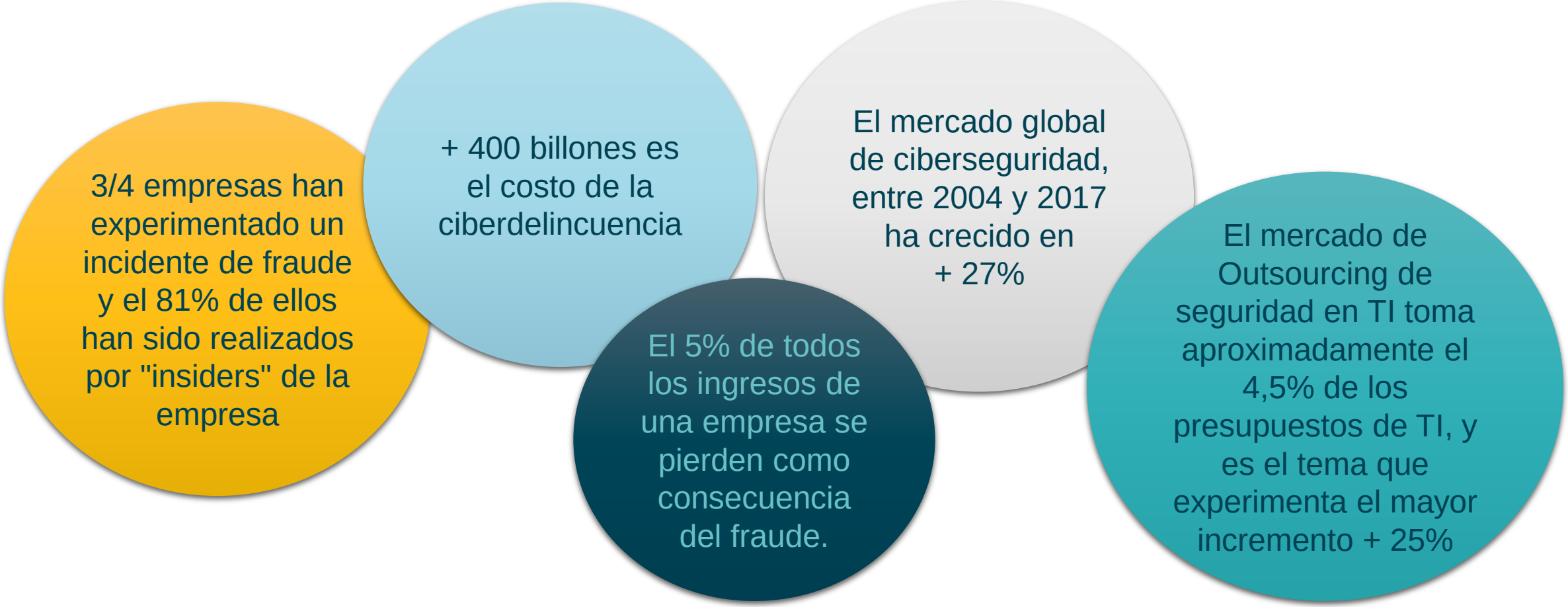
Ciberseguridad en ATM

- Situación actual
- Ciberseguridad 360
- i-CSOC MSSP
- Soluciones de seguridad

4

Situación actual

Aunque las inversiones en seguridad están creciendo, esto no es suficiente…



… los cibercriminales siguen encontrando nuevas formas de acceso

Situación actual

Problemática ATM

- Espacio aéreo complejo y saturados / redes interconectada de centros.
  - Cualquier problema importante afecta a otras partes de la red
- Las situaciones catastróficas pueden ... y ocurren
- La seguridad primero ... también los negocios
  - Retrasos, pérdidas económicas, sanciones regulatorias, imagen corporativa
- Planes de recuperación de desastres y continuidad de negocios son obligatorios.

Ciberseguridad 360

La ciberseguridad 360 se entiende como un conjunto de elementos diseñados para proteger la “huella digital”.

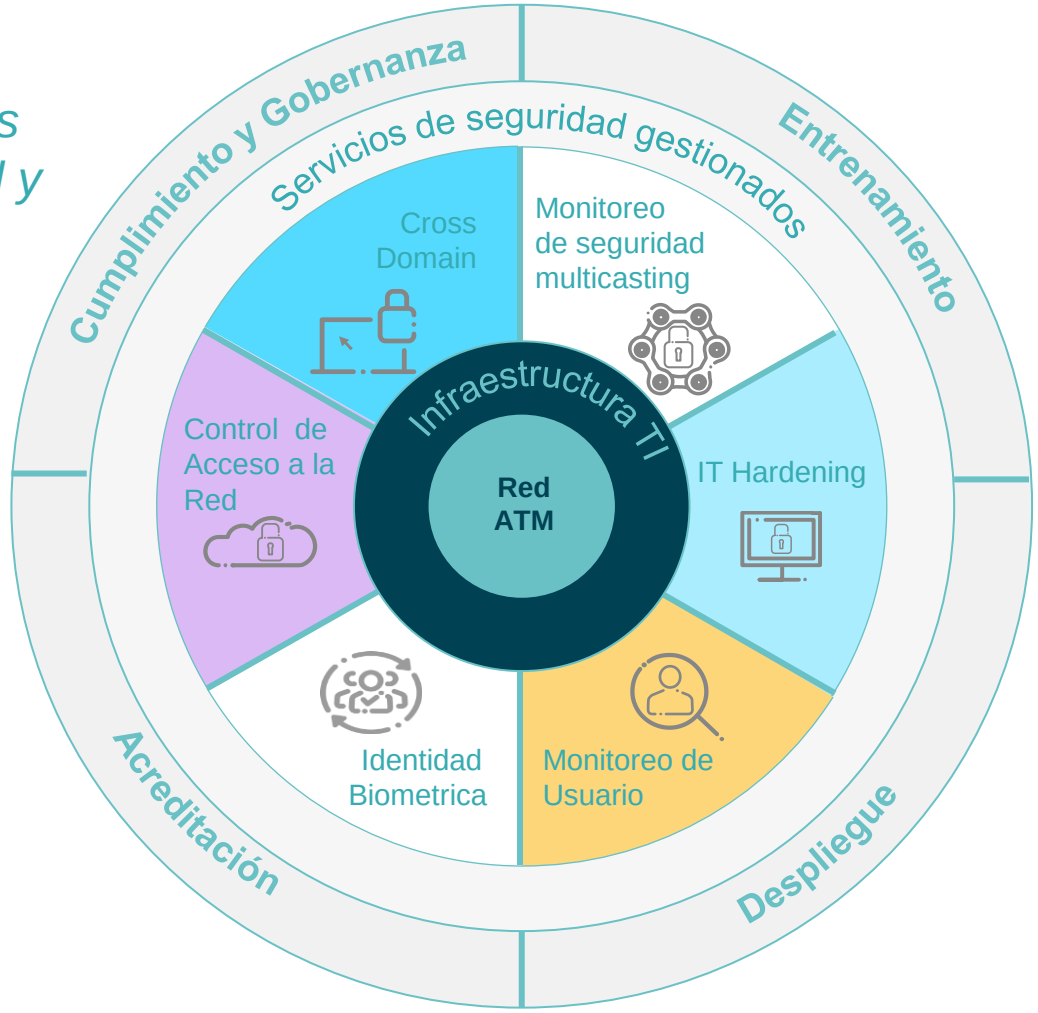
Un ecosistema de ciberseguridad ATM debe cubrir todos los requisitos clave para asegurar la confidencialidad, integridad y disponibilidad requerida para el negocio

Cumplimiento y Gobernanza
Definición de objetivos y pautas para los sistemas de seguridad a través del análisis y la prevención de riesgos que permiten mejorar los procesos y procedimientos de gestión de la información y sus políticas y requisitos legales, contractuales o específicos, que pueden aplicarse a la organización y sus sistemas de información, así como la verificación y evaluación. del grado de cumplimiento de requisitos.

Entrenamiento
Nuestro conocimiento de la industria nos permite ofrecer una capacitación y conciencia dirigida a profesionales de una organización en todos los niveles (estratégico, táctico y operativo).

Despliegue
Construcción de arquitecturas de seguridad con altas garantías con respecto a la funcionalidad implementada, utilizando métodos y herramientas que ayudan a la implementación en todo el proyecto, desde el diseño hasta la operación.

Acreditación
Planificar, gestionar y llevar a cabo los procesos de certificación y acreditación de sistemas en industrias criticas por la generación, administración y/o transmisión de información clasificada.



Ciberseguridad 360

Los servicios de gestión permiten a las empresas delegar el nivel de experiencia necesario para realizar tareas de seguridad continuas y servicios de valor agregado

3 Centros de operación de ciberseguridad

i-CSOC – Centros de Operaciones de Ciberseguridad Indra, trabajando de forma solidaria

Servicios de Gestión Ciberseguridad 360

24 x 7

Delegación de tareas de seguridad

- Monitoreo
- Análisis
- Alertas
- Respuesta
- Administración
- Gestión Tecnológica de Seguridad

Servicios de Valor agregado

- Ciber-vigilancia
- Ciber-inteligencia
- Prevención de Fraude
- Protección de Información

Consultoría | **Despliegue** | **Certificación y acceditación** | **Operación**

Functionalidades

- Monitoreo
- Ciber-vigilancia y ciber-inteligencia
- Gestión de seguridad “End-Point”
- Gestión de seguridad del entorno de servidores
- Gestión y anásis de vulnerabilidad
- Advertencias tempranas
- Pruebas de seguridad continua
- Administración
- Mitigación y detección
- Servicio de respuesta a incidente

i-CSOC MSSP

Provisión de servicios de seguridad gestionados

Prevención

Advertencia temprana
Identificación y análisis de amenazas, comunicaciones de vulnerabilidad aplicables a sistemas de clientes, mitigación y seguimiento de vulnerabilidades

Protección de servidores y end-points
FEE(P) Defensa Digital

Ciber-vigilancia
Búsqueda de información en fuentes abiertas orientado a organizaciones y personas.

Ciber-inteligencia
Detección y resolución de incidencias por actividades cibercriminales.

Fraude electrónico
Detección y prevención de fraudes unidos a tecnología tanto en Internet como en redes internas.

Detección y Contención

Operación y monitoreo
Monitoreo de sistemas y redes 24x7 (IPS / IDS, FW, AV, UTM, NAC, DLP, etc.) y registros de sistemas y aplicaciones.
Registros de correlación basados en SIEMs y retención de registros.

Administración
Administración 24x7, soporte y mentenimiento de dispositivos

Administración de incidentes
Detección y mitigación de incidentes, Contención y remediación.

Hacking ético y análisis de vulnerabilidad
Pruebas de penetración y análisis de vulnerabilidad.

Fraude electrónico
Pruebas de penetración continua, ejecutando pruebas cíclicas

Remediación

Equipo de respuesta rápida (RRT)
Asistencia de seguridad remota o “on-premise”, si es necesario para incidentes de seguridad, teniendo un equipo móvil y un kit para desbloquear ataques y recopilar pruebas para el análisis posterior.

Análisis forense
Identificación, recopilación, integración, normalización, almacenamiento, análisis y presentación de pruebas electrónicas relevantes que podrían requerirse en una investigación interna o para respaldar los procedimientos judiciales

Serviciso del “Tiger Team”

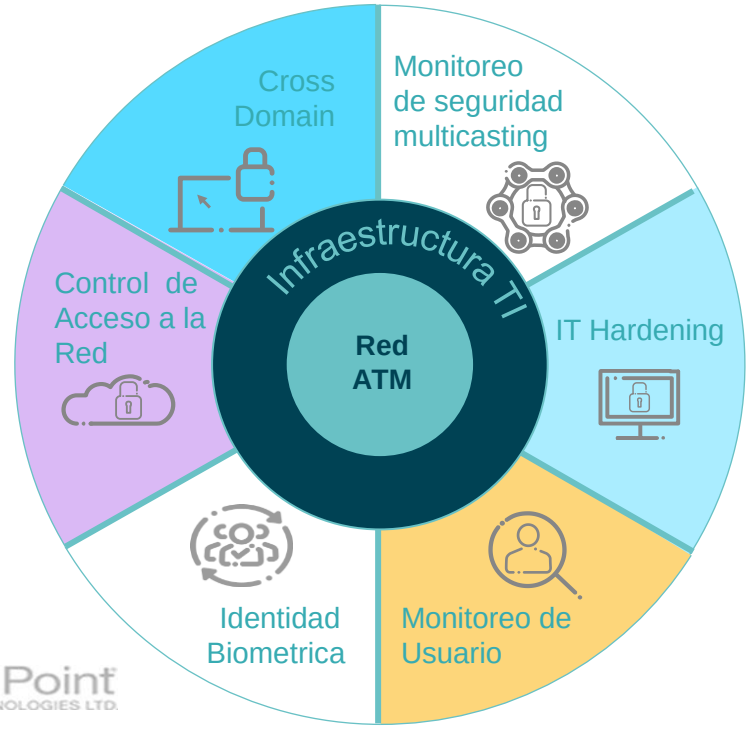
Análisis de ciberseguridad

Ciberseguridad 360

Indra proporciona una solución completa de arquitecturas de seguridad basadas en tecnologías propias y/o de terceros.

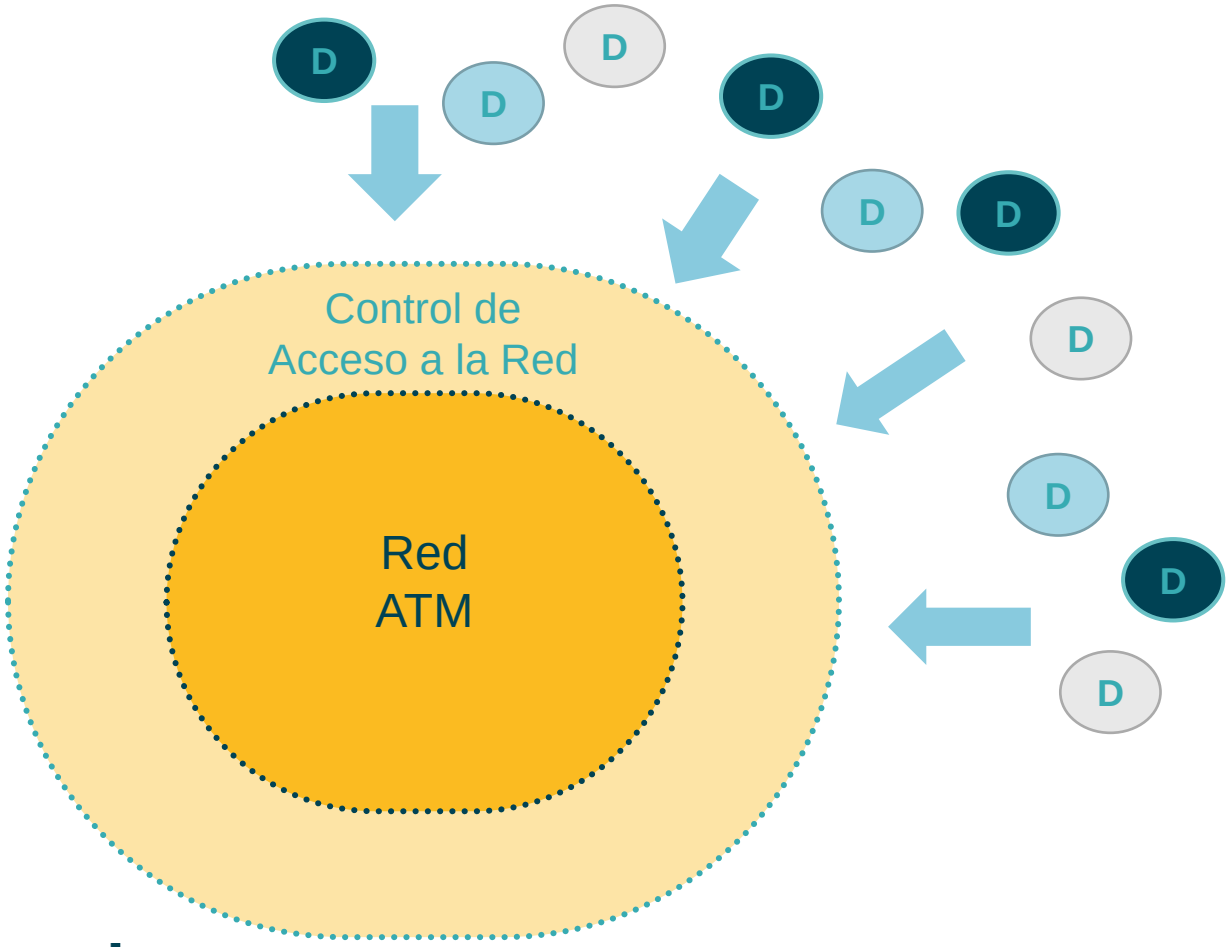
Simulación de entornos de producción. Ejecutando prueba de tecnologías de pre-despliegue. Contacto continuo con los departamentos de ingeniería de los proveedores.

- Almacenamiento de datos de seguridad, tanto archivos “short-cycle” como largos. Integridad de archivos y durabilidad de los datos.
- Cortafuegos, sistemas de prevención de intrusiones, control de acceso a la red, WAF, AntiAPT ...
- Cifrado de datos, archivos o repositorios.
- DLP / IRM (Data Loss Prevention / Information Rights Management).
- Infraestructuras de clave pública (PKI) y servicios avanzados (plataforma de firma, cifrado, autenticación), etc.
- Soluciones de identidad digital. Seguridad de la información Sistemas de gestión y sistemas antifraude.
- Directorios corporativos y metadirectorios.
- Soluciones de provisión de identidad.



Solución de seguridad de la red

La solución de seguridad de red identifica y evalúa los dispositivos de red en el instante en que se conectan a la red ATM



Identificar

Quien?	*se está conectando a su red* • *Dispositivo Gestionado* • *Dispositivo No-gestionado* • *Dispositivo IoT*
Cómo?	*se están conectando (cableado, inalámbrico o* VPN)
Cuando?	*se están conectando*

... y permite, deniego o limita el acceso a la red basado en la situación del dispositivo y sus politicas de seguridad

Despliegue y acciones

- Despliegue típico
- Acciones posibles

5

Despliegue típico

Fases conceptuales de una implementación de Ciberseguridad

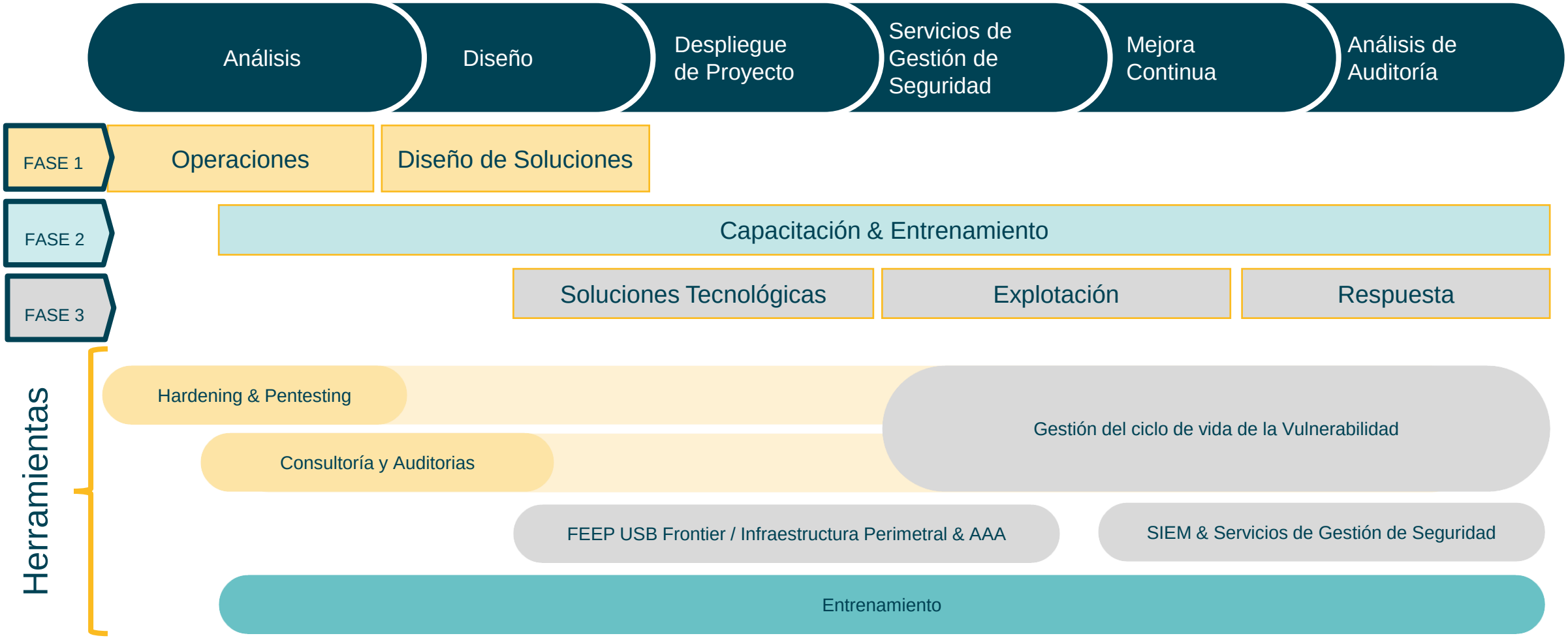
	Objetivos	Acciones
FASE 1 Consultoría	• Conocer las capacidades actuales tanto humanas como tecnológicas. • Conocer en detalle la infraestructura existente • Diseñar la arquitectura y modelo de seguridad	• Consultoría en campo por personal experto de Indra • Ayudar a definir el Plan Director de Ciberseguridad • Diseño del Plan de Formación Activo (Fase 2) • Diseño de la solución a implementar en (Fase 3)

FASE 2
Formación Activa
	• Evaluación de las aptitudes y conocimientos del alumnado elegido y selección de Talento.
	• Formación teórica y práctica del equipo encargado de la Ciber-seguridad de acuerdo al Plan de Formación Activo.
	• Formación Activa en tecnologías SOC y de Respuesta
		• Formación mediante la plataforma Cyber Range en modo Servicio:
		  • Herramientas SIEM
		  • Gestor de Vulnerabilidades
		  • Herramientas de Ciberinteligencia
		  • Capacidades de Respuesta
		  • Laboratorio Ciberdefensa
		• Servicios de SOC para la infraestructura TI con participación de la Fuerza Ciber del Ejército para formación activa

FASE 3 Implementación	• Implementación de las soluciones finalmente necesarias • Puesta en servicio del SOC y Laboratorio de Ciberdefensa • Implementación de la Plataforma Cyber Range	• Adquisición del hardware y software necesario para la implementación del SOC y del Laboratorio de Ciberdefensa • Adquisición de la Plataforma Cyber Range • Instalación, pruebas y puesta en servicio • Formación específica de gestión de herramientas seleccionadas

Despliegue típico

Fases de implementación de una arquitecturas de ciberseguridad



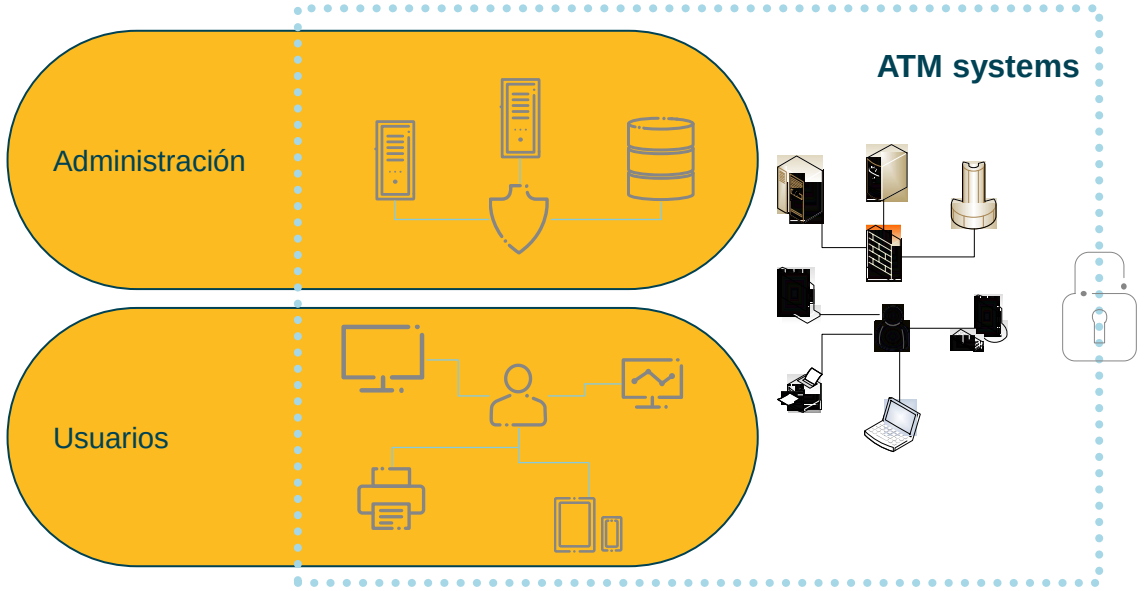
Acciones posibles

Hardening & Pentesting

Hardening: Conjunto de actividades que se realizan para reforzar al máximo posible la seguridad de sus sistemas.

Sistemas ATM “Hardening”, permite la funcionalidad completa del usuario; Usando las mejores prácticas de mercado, reglas oficiales y regulaciones propias y guías.

- “Hardening” de elementos ATM de LAN&WAM
- “Hardening” de elementos COTS
- “Hardening” en protocolos de comunicación
- “Hardening” en procesos técnicos (ej. Autentificación, Autorización y Contabilidad)



Acciones posibles

Hardening & Pentesting

Pruebas de penetración: son prácticas para poner a prueba un sistema, red o aplicación para encontrar vulnerabilidad que un atacante podría explotar.

Pruebas de penetración: pruebe la solidez de su infraestructura de TIC para medir su nivel de seguridad técnica contra su política de seguridad.

Diseño/ejecución de pruebas y análisis de seguridad de aplicaciones.

Auditorías técnicas: hacking ético, análisis de vulnerabilidad.

- **Caja Blanca:** Revisión manual del código fuente en busca de patrones o errores en el código que puedan presentar vulnerabilidades explotables por parte del atacante. Útil para encontrar el enfoque de errores y errores comunes: casos límite, problemas de validación, violaciones de invariancia, etc.
- **Caja negra:** Se ejercen interfaces externas de software para intentar violar las propiedades de los mismos o los objetivos de seguridad. Uso de herramientas fuzzing para inyectar interfaces no estructuradas a software externo con el fin de explotar datos de vulnerabilidades potenciales.
- **Caja gris:** Busque los defectos de la estructura inadecuada o el uso inadecuado de las aplicaciones, conociendo parcialmente la estructura interna, que incluye el acceso a la documentación de las estructuras de datos internas.

Informática forense.

Acciones posibles

Servicios de consultoría y auditoría

Nuestros expertos pueden desarrollar e implantar políticas, procesos, procedimientos y planes de seguimiento para monitorizar y garantizar el cumplimiento de los objetivos de seguridad.

Consultoría

- Establecer el SMP (Plan de administración de seguridad), definiendo los principales roles y responsabilidades para las funciones de seguridad relevantes para su organización.
- Realización de análisis y evaluación de la información y las aplicaciones comerciales principales de nuestros clientes (Informe SRA +).
- Diseño e implementación de procesos de seguridad.

Auditoria

- Auditorías a las regulaciones: ISO / IEC, Leyes de protección de datos personales, CiP EU ...
- Auditorías Técnicas: Hacking Ético, Análisis de Vulnerabilidad, Pentesting.
- Auditorías de políticas internas. Diseño, identificación y cumplimiento de la normativa correspondiente.

Entrenamiento

- Sesiones de capacitación con expertos que brindarán un enfoque práctico para prevenir, detectar, reaccionar y responder a los ciber-ataques.
- Formación teórica y práctica, tanto a nivel conceptual básico como avanzado.

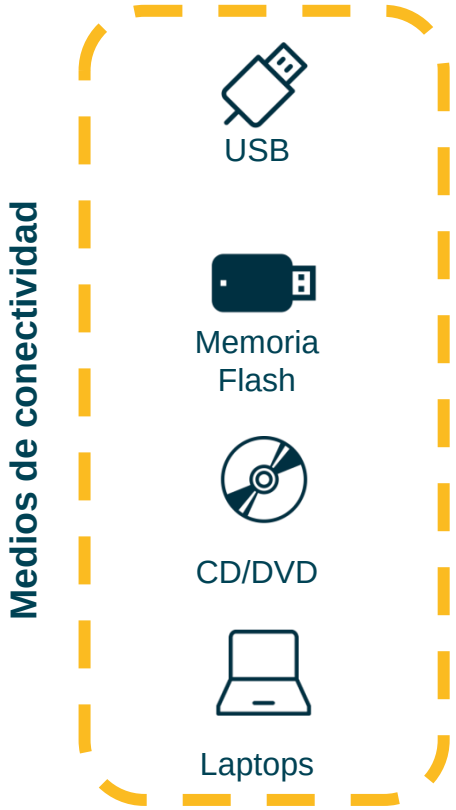
Acreditaciones

- Credenciales (Criterios Comunes, FIPS 140…).
- Servicios de emisión de acreditación: Nacional, OTAN, UE, ESA, OCCAR, ...

Acciones posibles

FEEP USB Frontier

Es la barrera más efectiva contra amenazas que utilizan medios de conectividad indirecta como su vector de propagación



Funcionalidad

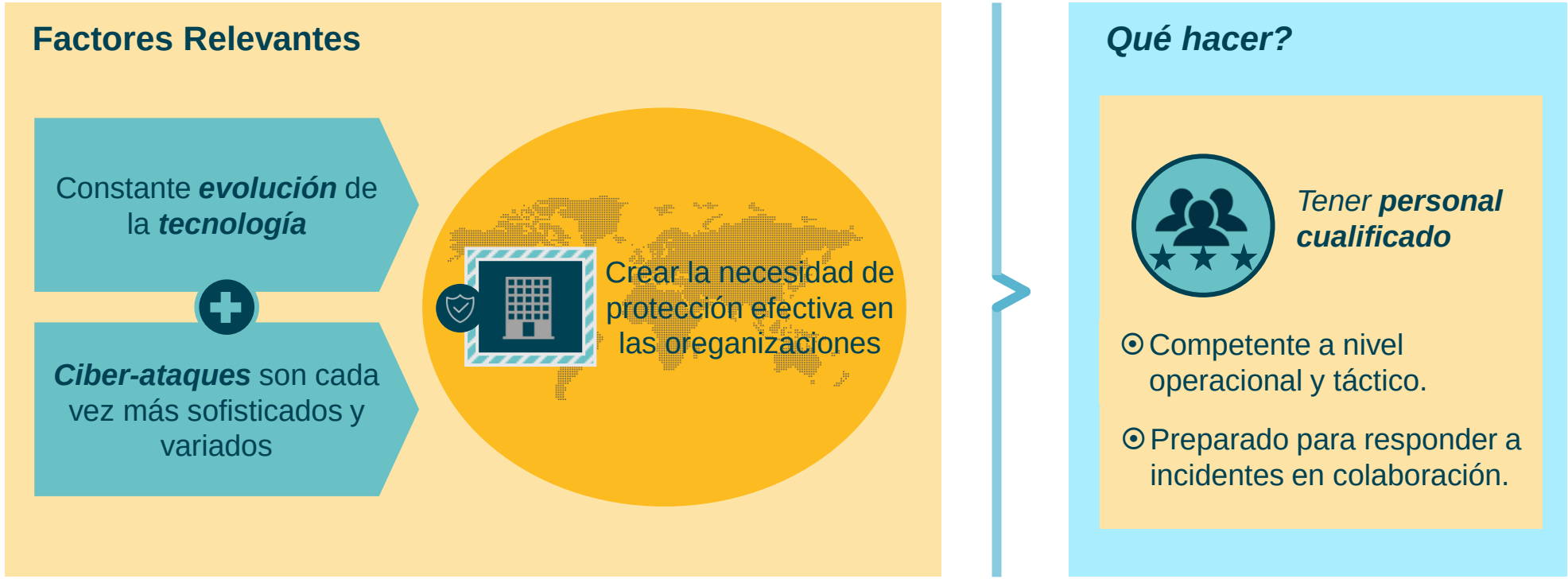
USB FRONTERA

Análisis de lista blanca	⊙ Análisis y comparación utilizando una lista blanca con más de 40 millones de entradas actualizables. ⊙ Verificación de la firma digital de los archivos firmados.
Análisis de listas negras	⊙ Análisis de archivos con hasta 30 motores de detección antivirus opcionales.
Cuarentena de archivos infectados	⊙ Los archivos de malware se copian y analizan en un entorno controlado (la opción de enviar muestras al iCSOC para una investigación adicional)
Control del dispositivo	⊙ Inventario y administración de dispositivos USB que puede mejorarse con sistemas de protección de endpoint
Verificación de integridad	⊙ Control de la integridad del archivo y verifica los cambios posteriores que ocurrieron después del análisis.
Borrado seguro	⊙ Capaz de eliminar completamente los datos contenidos en una unidad USB, sin posibilidad de recuperación.
Multi-dispositivo	

Acciones posibles

Entrenamiento

En la actualidad, desarrollar y mejorar la capacidad de la fuerza laboral humana se convierte en una acción estratégica para las organizaciones.

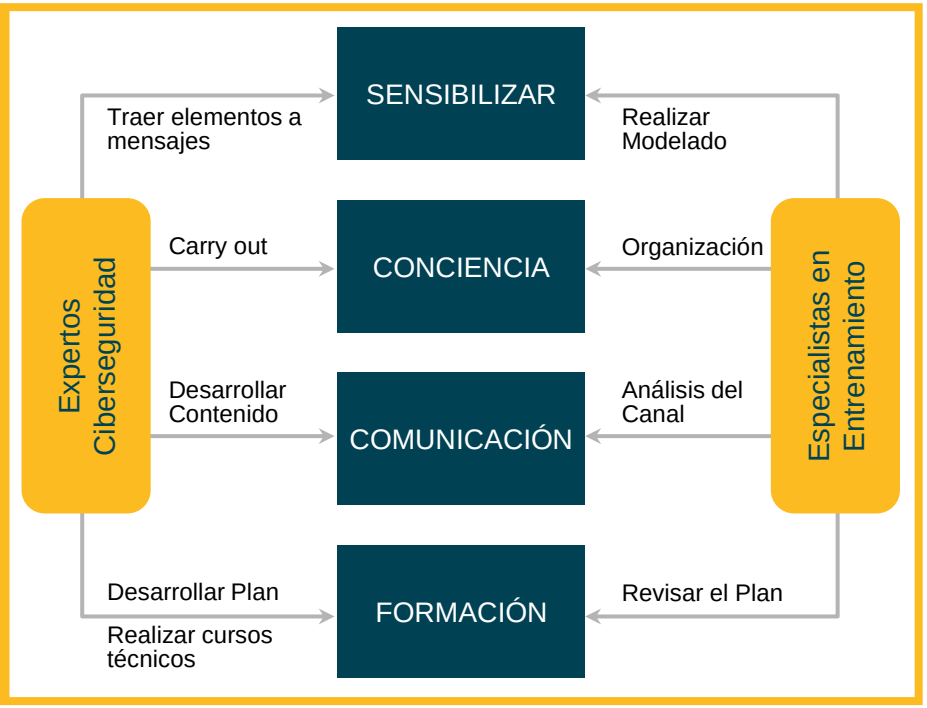


Acciones posibles

Entrenamiento

Nuestro conocimiento de la industria nos permite ofrecer una capacitación y concientización centrada en los profesionales de una organización en todos los niveles (estratégico, táctico y operativo).

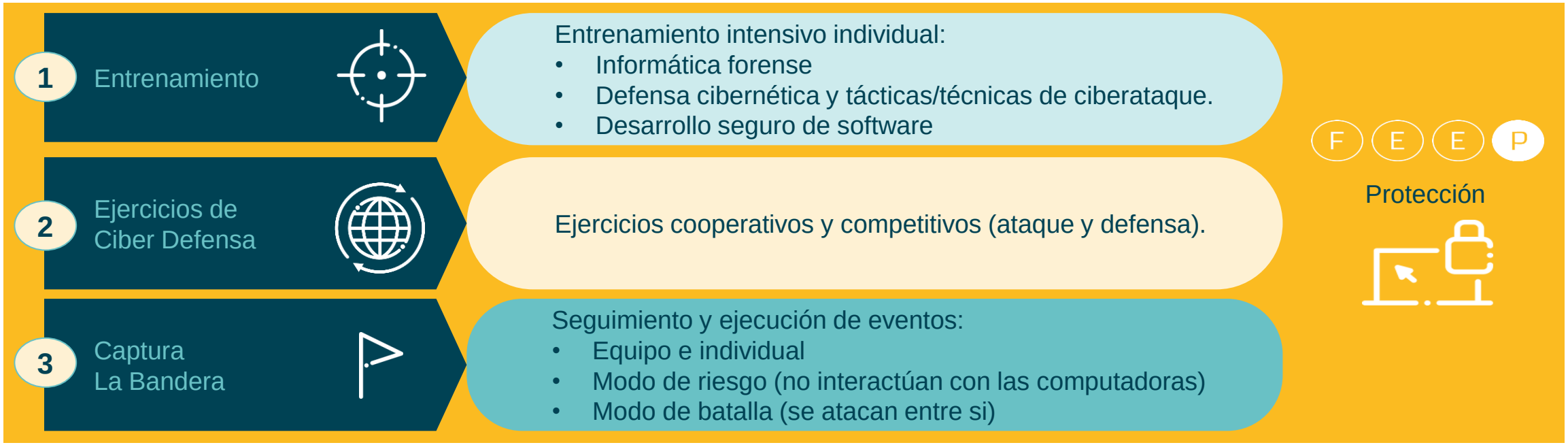
- Desarrollo de planes de formación, divulgación y sensibilización.
- Cursos y seminarios impartidos.
- Diseño e implementación de planes y sensibilización específica.
  - Reportes informativos
  - “Phising” ético / Ciber-juegos
  - Sesiones de concientización para directivos.
- Pautas de uso. Definición de arquitecturas de seguridad aprobadas. White Papers desarrollo seguro y procedimientos de configuración segura (PoS).
- Servicios de formación y conciencia situacional.
  - Sesiones de entrenamiento con expertos que mostrarán en la práctica cómo prevenir, detener y reaccionar a los ataques.
  - Desarrollo de ejercicios colaborativos y competitivos ciber-ataque / defensa.



Acciones posibles

Entrenamiento

Cyber Range ofrece un conjunto de productos sin igual con un enfoque práctico integral para crear y perfeccionar las habilidades y el conocimiento de la ciberseguridad del personal ...



…para detectar, reaccionar y responder a los ciberataques

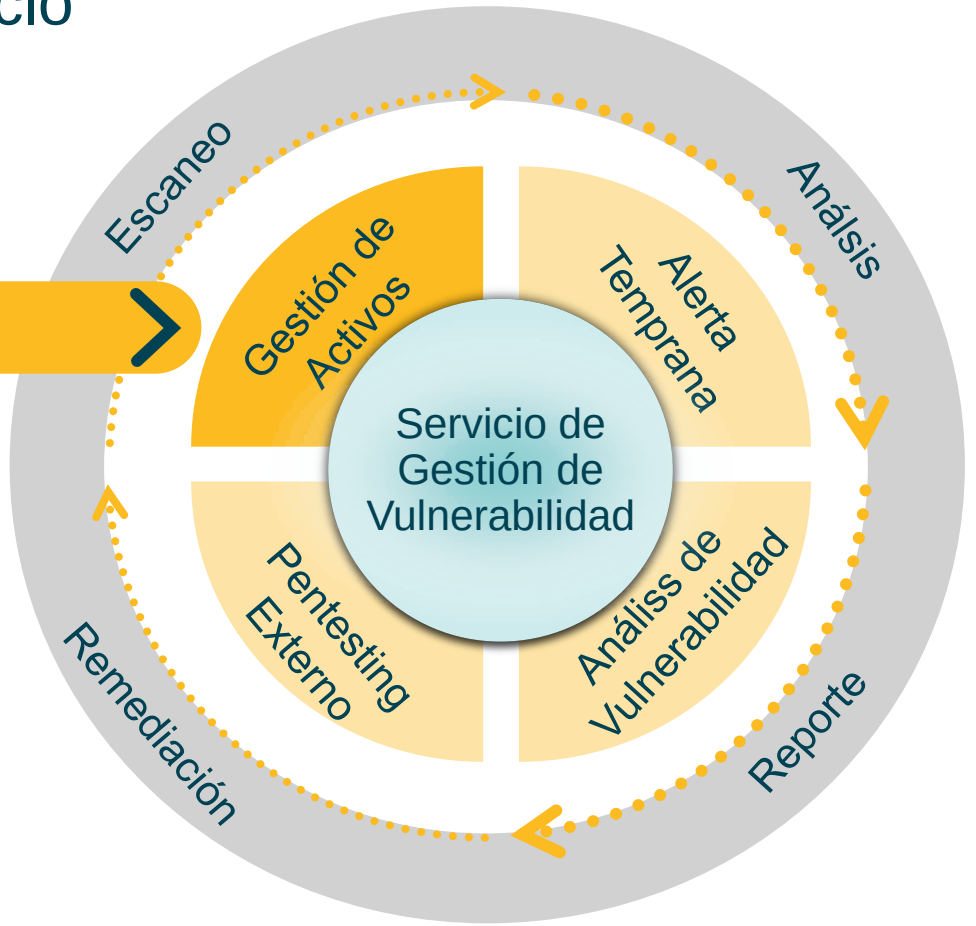
Acciones posibles

Servicio de gestión del ciclo de vida de la vulnerabilidad

Gestión completa de la vulnerabilidad del ciclo de vida, basada en el inventario de clientes

Inventario

Incluyendo
- Servidores, CWPs
- Applicaciones
- Dispositivos de Red
- Infraestructura de Seguridad
- Software: OS, Firmware
- Arquitecturas



Acciones posibles

Servicio de gestión del ciclo de vida de la vulnerabilidad

Servicio de Alerta temprana

Conclusiones

- Beneficios
- Referencias seleccionadas

6

Conclusiones

Beneficios

- Mayor resiliencia,incluso con múltiples fallas en la infraestructura, por ejemplo:
  - La mayoría de las fallas individuales son totalmente transparentes para la continuidad del servicio
  - Eventos catastróficos improbables: recuperación sin problemas en segundos (ej. cambio automático)
  - Ciberataques masivos: reanudación en minutos (copia nueva y / o versión sw anterior)

- Escalabilidad y flexibilidad
  - Se pueden aprovisionar recursos adicionales cuando sea necesario
  - Independencia de ubicación: centros de datos virtuales y visualización remota
  - Los recursos de repuesto y de contingencia se pueden utilizar fácilmente para admitir el sombreado, la transición, el entrenamiento, etc.

Conclusiones

Beneficios

- Eficiencia de la infraestructura (por ejemplo, reducción de costos y espacio)

- Mejora de la continuidad para la red ATM
  - La pantalla remota y la configuración operativa dinámica permitirían la recuperación de ATSU en minutos
  - Los sectores de contingencia y la interoperabilidad permitirían la recuperación de ANSP vecinos

- Aumento de capacidad de respuesta bajo demanda
  - Escalable al instante para responder a las demandas cambiantes.

Conclusiones

Referencias seleccionadas: SESAR 2020

SESAR es el programa de modernización de la infraestructura de control del tráfico aéreo europeo. SESAR apunta a desarrollar el sistema de gestión de tráfico aéreo de nueva generación capaz de garantizar la seguridad y la fluidez del transporte aéreo en todo el mundo durante los próximos 30 años.

Objetivos

Proporcionar una capa de seguridad sobre el nuevo diseño de FCI (Future Communication Infrastructure)

Indra ha participado en las siguientes tareas relacionadas con ciberseguridad para dar soporte a los diferentes WPs:

- Configuración del sistema y “hardening” (SWIM)
- Procedimientos de operaciones de seguridad
- Metodología de análisis de riesgo
- Pruebas de penetración sobre PENS&SWIM
- Especificaciones de los requisitos de seguridad del sistema

Experiencia en ATM

Referencias seleccionadas: iTEC - NATS

Indra implementó el Sistema de Seguridad Lógica en Sistemas de Navegación Aérea (iTEC) para NATS.

Objetivos

Gestionar ciberseguridad para el programa de operaciones basadas en la trayectoria PCUA en NATS-iTEC

- Proporcionar soporte para el diseño y la implementación de la estrategia de administración de seguridad, en lína con ISO/IEC 27001
- Diseño e implementación de tecnología AAA, IAM e IDM (NetIQ)
- “Hardening” del sistema (HW & SW, incluidas las aplicaciones COTS y BeSpoke)
- Apoyo a las fases FAT y SAT
- Apoyo a terceros en pruebas de penetración
- Entrenamiento de seguridad

NATS

NATS comisionó a Indra para respaldar el despliegue del sistema iTEC en Prestwick Center Upper Airspace.
El proyecto permitirá la introducción del concepto de operación basado en la trayectoria de SESAR en el Reino Unido.

Experiencia en ATM

Referencias seleccionadas: iCAS – Procesos de ciberseguridad

Indra es el socio tecnológico en iCAS (iTEC Center Automation System) para DFS y LVNL. PANSA y Oro Navigacija han firmado en el WAC'16 una Carta de intenciones para ingresar al Grupo iTEC DFS.

Objetivos

Indra realiza las siguientes actividades de ciberseguridad para los objetivos del proyecto en la Fase II de iCAS:

- Diseño e implementación de la estrategia y plan de gestión de ciberseguridad
- Evaluación de riesgos de seguridad
- “Hardening” del sistema (HW&SW, incluidas las aplicaciones COTS y BeSpoke)
- Apoyo a las fases de desarrollo, FAT y SAT.
- Auditoria de seguridad
- Entrenamiento en ciberseguridad

DFS Deutsche Flugsicherung

Luchtverkeersleiding Nederland
Air Traffic Control the Netherlands

Experiencia en ATM

Referencias seleccionadas: Otras experiencias - iTEC

Los clientes ATM están comenzando a incluir ciberseguridad en sus proyectos, e iTEC proporciona medidas iniciales.

Las medidas de ciberseguridad en SACTA incluyen:

- Seguridad perimetral (firewalls) con monitoreo de seguridad centralizado para todos los sitios (5 Centros y> 40 APLICACIONES / Torres).
- Sistema inicial de “hardening”
- Apoyo a la auditoría de seguridad

Las medidas genéricas de ciberseguridad integradas en iTEC incluyen:

- Seguridad perimetral (firewalls)
- Control de acceso (AAA)
- Sistema “hardening” estándar.

Contacto:
Rodrigo San Martin
rasan@indracompany.com
ATM Internacional

Av.Isidora Goyenechea
2800, Piso 12
Las Condes – Santiago
Chile

+56 2 2810 3600