CIBERSEGURIDAD PREDICTIVA

BDO y su visión hacia el Cyber SOC 4.0

CIT | Ciberseguridad y Gobierno Tecnológico
DRAS | DIGITAL ASSURANCE, AUDIT & COMPLIANCE SERVICES

01
NUESTROS NÚMEROS

	Global	Argentina
	Presente en más de 166 países y territorios	Presente en Buenos Aires, Córdoba, Santa Fe y Mendoza
OFICINAS	1.776	5
STAFF	+115.661	+900
INGRESO ANUAL	U$S14 Mil Millones	U$S35 Millones

FABIÁN DESCALZO

Socio de la práctica de Ciberseguridad, Gobierno Tecnológico y Digital Risk Advisory Services de BDO en Argentina y Líder de la práctica de ciberseguridad para LATAM, con 35 años de experiencia en el área de gestión e implementación de Gobierno de Seguridad de la Información, Gobierno de TI, Compliance y Auditoría de TI en Argentina y Latinoamérica, y asesoramiento para el cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio.

Docente Universitario y de Sistemas de Gestión IT, Seguridad de la Información en Universidad de Palermo y Auditoría IT para TÜV Rheinland. Conferencista internacional y columnista en medios especializados.

Autoridad del Comité de Seguridad Patrimonial y Seguridad de la Información en AmCham Argentina, Miembro Titular del Comité Directivo y Presidente de la Comisión de Educación de ISACA Buenos Aires Chapter, de la Asociación Latinoamericana de Privacidad, de la Asociación Argentina de Ética y Compliance, y del Comité Científico del IEEE (Institute of Electrical and Electronics Engineers)


BDO
Vigilar, proteger y garantizar la operación continua del negocio, nunca ha sido más importante para BDO que en la actualidad.


ERP
INDUSTRIA 4.0
Sistemas
Ciberfísicos
Internet de las
cosas
Redes
ACTUALMENTE


Ciberseguridad
Computación
Cognitiva
Computación
en la nube
Tecnologías
RFID
RFID
Tecnologías
Móviles
Internet
de las
cosas
IoT
4.0
Technology
Máquina a
máquina
M2M
M2M
Big Data/
Analítica
BIG
DATA
3D
Impresión 3D
Robots Autónomos

https://cybermap.kaspersky.com/es

- Durante 2021 y 2022, hubo un aumento significativo de los ciberataques.
- El 41% de las pymes en el país sufrieron algún tipo de ataque cibernético en el último año.
- Según el Foro Económico Mundial, se estima que el costo promedio global de un ciberataque grave puede alcanzar los $4.45 millones de dólares
- Tras el pago frente a un ransomware, únicamente un 36% recuperó todos sus datos

infobae

Trends Aeropuerto Southend Londres Air India Donald Trump Volodimir Zelensky Ivan

AMÉRICA LATINA >

Así fue el mayor ciberataque contra el sist de Brasil

Los hackers robaron 148 millones de dólares utilizando las credenciales de un emp sistemas vinculados al PIX y al Banco Central. Especialistas explican a Infobae el in ataq

20minutos

Filtran 16.000 millones de credenciales en la mayor brecha de la historia: Apple, Google y Facebook, entre los afectados

CIBERSEGURIDAD MARTA GASCÓN | NOTICIA | 20.06.2025 - 08:46H

Ha sido Cybernews quien ha dado la voz de alarma. Se trata de varias recopilaciones de conjuntos de datos que incluyen sobre todo información de registros de inicios de sesión.

- Google estrena en Europa una tecnología para demostrar tu edad sin revelar quién eres: así funciona

Las fallas de Bluetooth podrían permitir que los piratas informáticos espíen a través de su micrófono

Por Ionut Ilascu

29 de junio de 2025 12:03 p. m. 0

(1) Notificaciones | Link Fabian en el CISO noticias de ataques de Resumen con las noticias ANCAP

https://www.welivesecurity.com/la-es/2022/04/29/ancap-detecta-malware-software-utilizado-distribucion-combust

BDO BDO CRM CH API ManageEngine - AD... UP Blackboard Learn BDO Global Portal -... One BDO - Hom

welivesecurity BY eset Noticias, opiniones y análisis de la comunidad de seguridad d

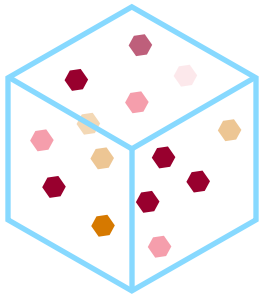
CONSEJOS DE SEGURIDAD SEGURIDAD PARA EMPRESAS INVESTIGACIONES TEMAS

Infraestructuras Críticas Seguridad Digital

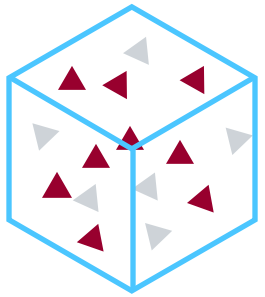
ANCAP detecta código malicioso en software utilizado para distribución de combustible

La compañía estatal uruguaya detectó la presencia de código malicioso en software utilizado para la distribución de combustible y monitoreo de vehículos oficiales. La amenaz estaba programada para ejecutarse más adelante.

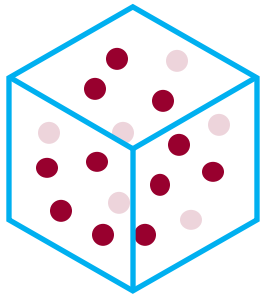
Capas de ciberseguridad a monitorear



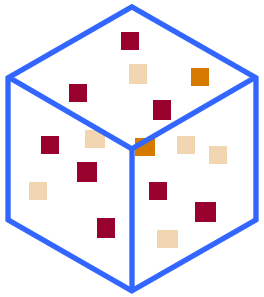
Capa Física
CCTV, Control de accesos



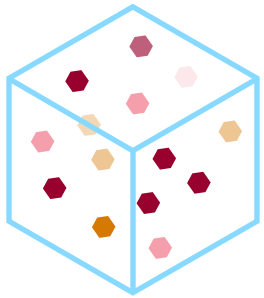
Capa de red
Firewalls, IDS/IPS



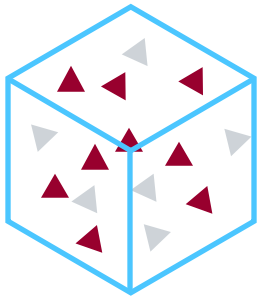
Capa de perímetro
Filtros web, protección DDoS, Gateways



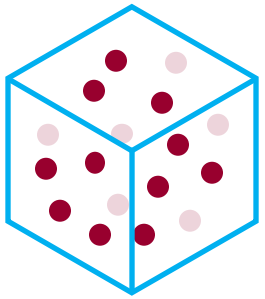
Capa App
WAF, revisión de código, actualizaciones



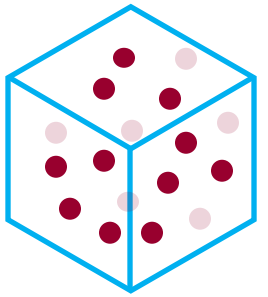
Capa de dispositivos
PCs, móviles, servidores, Antivirus, EDR, cifrado



Capa de datos
Cifrado, DLP, control de acceso



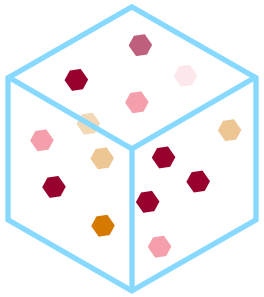
Capa humana
Concientización, pruebas de phishing, políticas



Capa marca
Concientización, pruebas de phishing, políticas

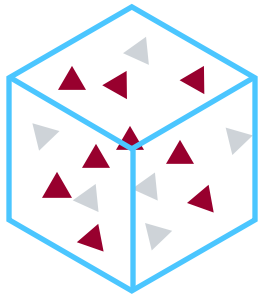

SOC 4.0
SOC 3.0
SOC 2.0
BDO

Modelos de Seguridad Gestionada



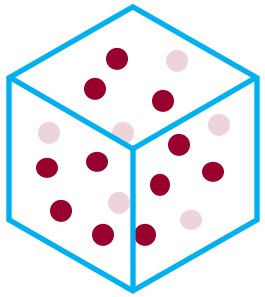
Seguridad Reactiva

Se refiere a las medidas y acciones que se toman en respuesta a incidentes de seguridad después de que estos ocurren. La seguridad reactiva se enfoca en detectar, responder y mitigar los daños una vez que un incidente ha sucedido.



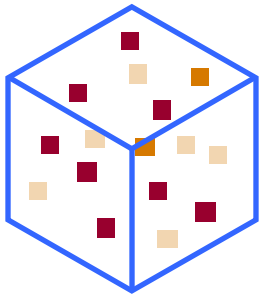
Seguridad Proactiva

Se refiere a las acciones y estrategias que se implementan para prevenir incidentes de seguridad antes de que ocurran. La seguridad proactiva identifica vulnerabilidades, detecta amenazas tempranas y fortalece el ecosistema para evitar ataques.



Seguridad Preventiva

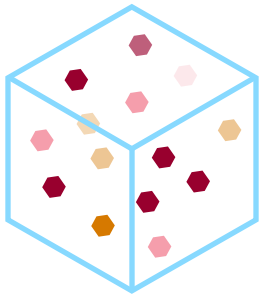
Es un enfoque de seguridad centrado en tomar medidas y establecer controles para evitar que ocurran incidentes o ataques antes de que estos sucedan. Es una parte fundamental de la estrategia de seguridad, busca reducir riesgos y proteger los activos desde el inicio.



Seguridad Predictiva

Es un enfoque avanzado, utiliza tecnologías de análisis de datos, IA y aprendizaje automático para identificar potenciales amenazas o vulnerabilidades. En lugar de reaccionar o prevenir ataques conocidos, este modelo se anticipa a riesgos emergentes mediante la detección de patrones y tendencias.

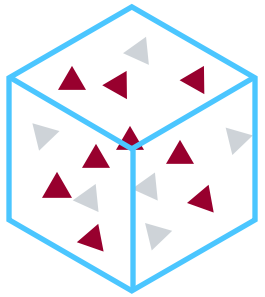
Paralelismo
Modelos de Seguridad vs Versiones SOC



SOC 1.0

Ventajas:
- Permite responder a incidentes específicos
- Es útil cuando no hay una estrategia sólida

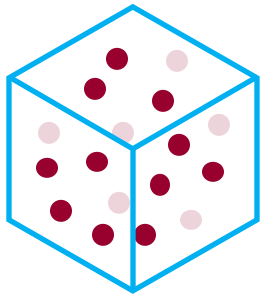
Desventajas:
- No previene futuros ataques
- Puede resultar en mayores costos y daños.



SOC 2.0

Ventajas:
- Reduce riesgo de incidentes.
- Minimiza costos tras ataque.
- Mejora postura de seguridad.

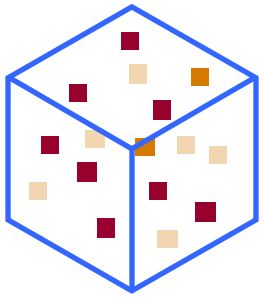
Estrategias:
- Sistemas avanzados (EDR).
- Segmentación de redes.
- Gestión de parches.
- Políticas estrictas y control de accesos.



SOC 3.0

Ventajas:
- Reduce eventos de seguridad.
- Disminuye costos tras ataque.
- Mejora la confianza en sistemas y datos.

Ejemplos:
- Configurar firewalls.
- Política de contraseñas fuertes y cambios periódicos.
- Auditorías de seguridad.
- Capacitar al empleado sobre amenazas comunes.



SOC 4.0

Ventajas:

Alerta y detección temprana.
Mejora la capacidad de respuesta.
Reducir el tiempo y los costos asociados.
Ayuda a priorizar recursos en zonas vulnerables.

Ejemplos:

Sistemas UEBA y de predicción basado en tendencias.
IA para identificar malware avanzado o polimórfico.


4.0

Definicion 4.0

El término "SOC 4.0" es ambiguo y puede tener diferentes significados en distintos contextos. No existe una definición o estándar universalmente aceptado que lo designe específicamente como "SOC 4.0".

En el sector de la ciberseguridad, "SOC 4.0" podría representar una evolución o nueva generación de centros de operaciones de seguridad que integran tecnologías de vanguardia como IA, BI, SOAR y UEBA para detectar y combatir amenazas de forma más eficiente.

A veces, "4.0" se utiliza en relación con la Industria 4.0, que describe la cuarta revolución industrial caracterizada por la digitalización, el IoT (Internet de las Cosas) y las fábricas inteligentes.

En este contexto, "SOC 4.0" se refiere a sistemas de seguridad o monitorización en entornos de la Industria 4.0.

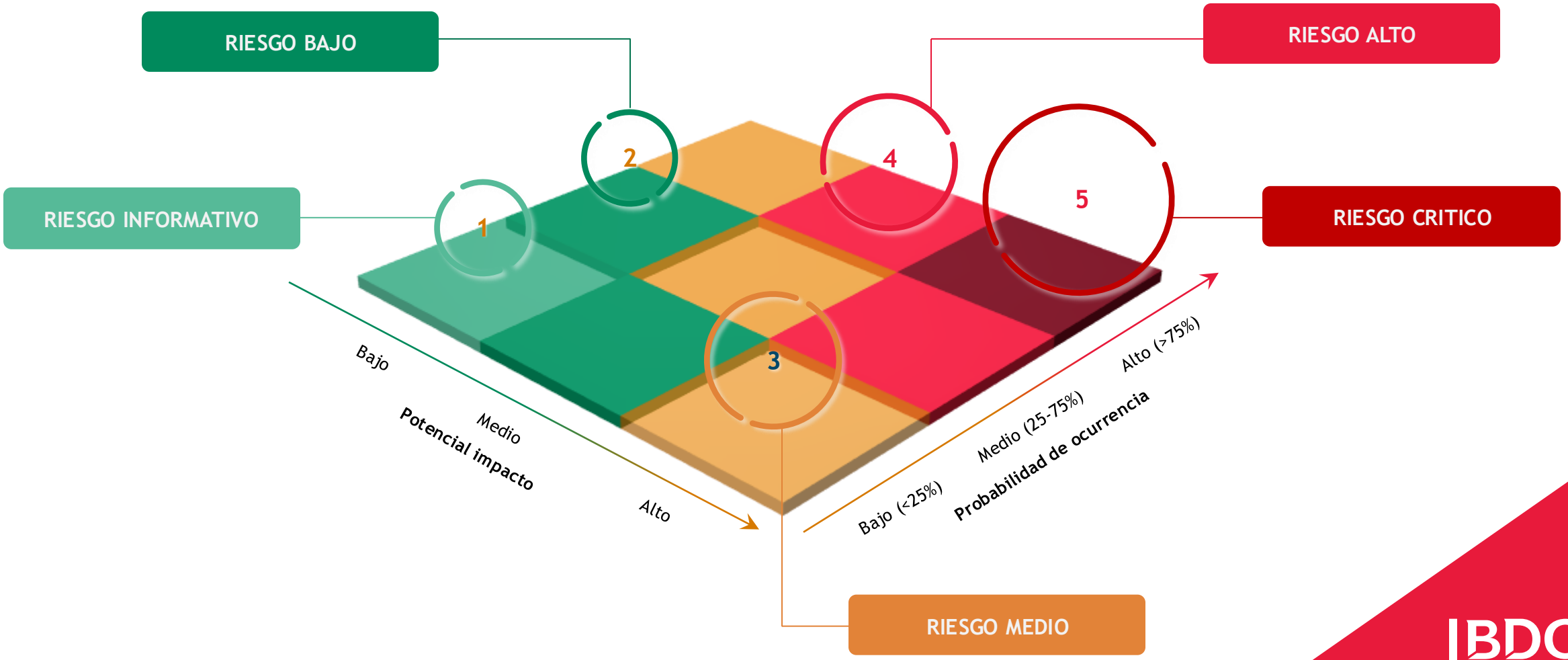
BDO

Características SOC 4.0

- Automatización y Orquestación
- Inteligencia Artificial y Aprendizaje Automático
- Análisis en Tiempo Real
- Integración Total de Tecnologías
- Enfoque Proactivo

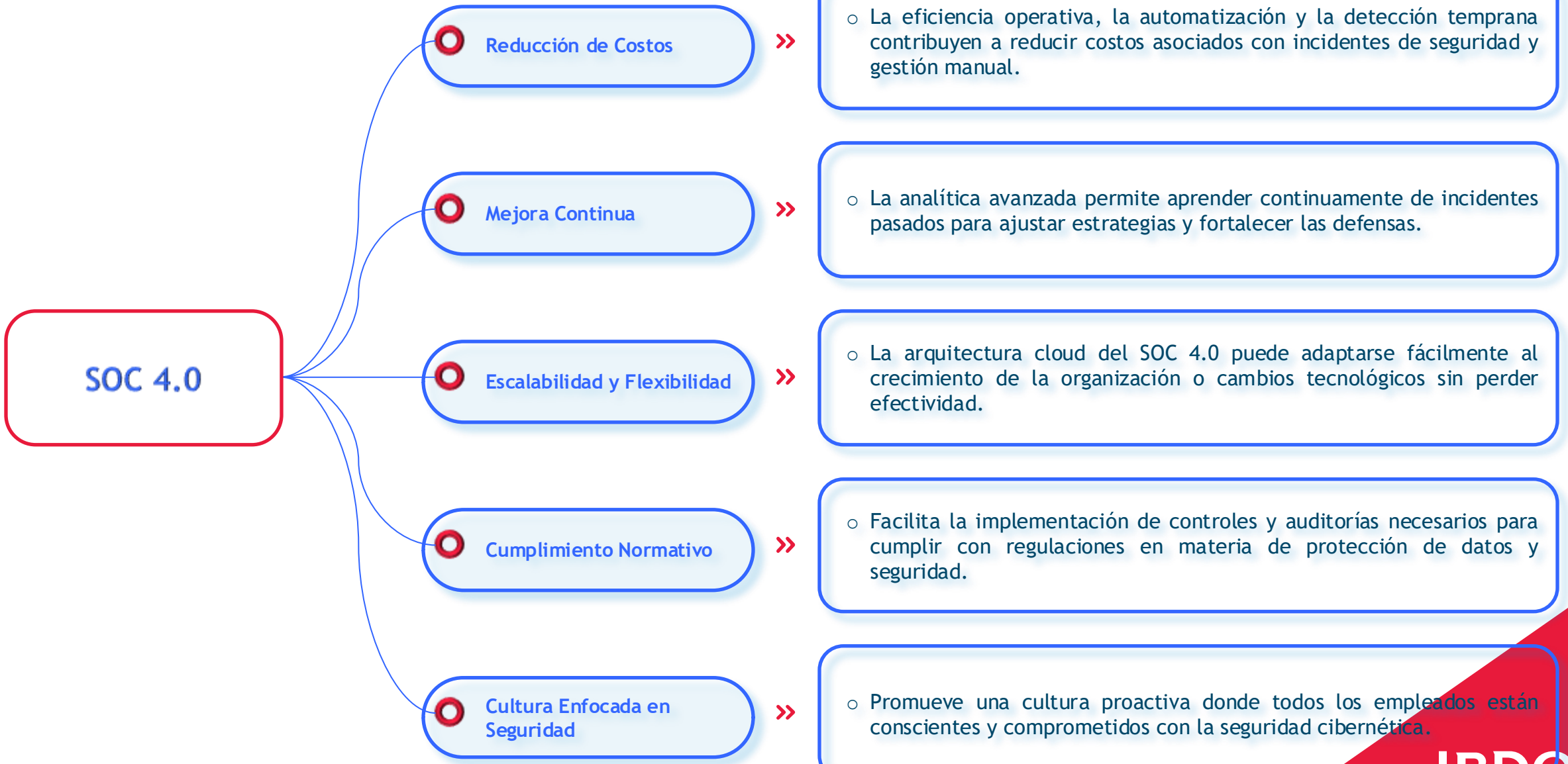
- Capacidades Predictivas
- Personalización y Escalabilidad
- Colaboración y Compartición de Información
- Cultura de Seguridad Integrada
- Uso Extensivo de Cloud y Big Data

Enfoque basado en Matriz de Riesgo



Beneficios 4.0

Beneficios 4.0



Ventajas 4.0

PREVENCION

- Alerta temprana
- Auditoria de código fuente
- Gestión de vulnerabilidades
- Vigilancia reputacional
- Gestión de versiones
- Retorno de la inversión

OPERACION

- Monitoreo SOC 24x7
- Gestión de firewalls
- Aplicación de parches
- Gestión de controles
- Soporte del fabricante
- Operación simplificada
- Reducción de esfuerzos

INTERVENCION

- CSIRT capacitado
- Laboratorio forense
- Laboratorio de malware
- Auditorias de seguridad
- Equipo de hunters experto
- Emulación ofensiva
- Emulación defensiva
- Evaluación de riesgos
- Diseño seguro

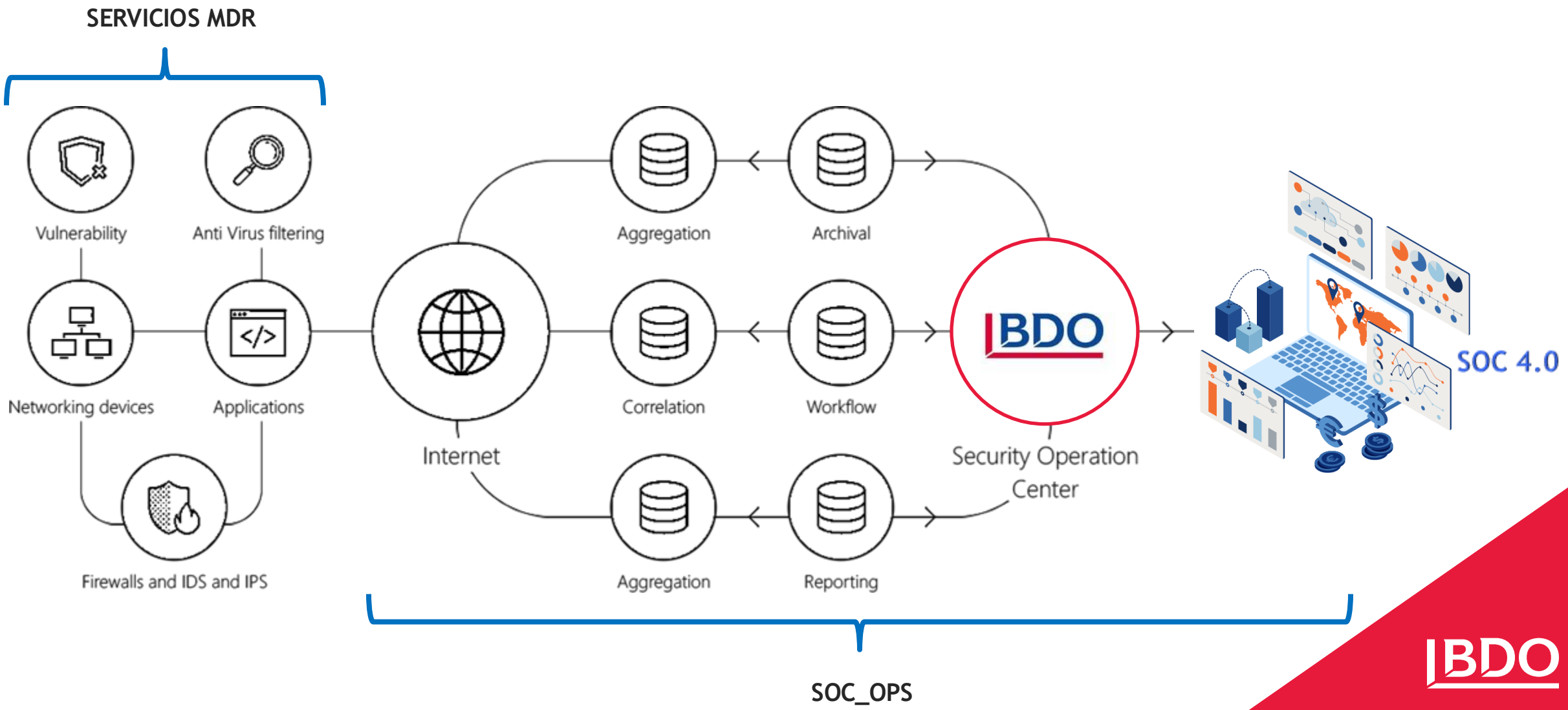
EVOLUCION

- Tecnología de vanguardia
- Entornos aislados [QA]
- Diagnóstico avanzado
- Tecnología SOC propia
- Seguridad Zero Trust
- Seguridad TI, OT, IoT, IIoT
- Criptografía avanzada

INNOVACION

- Inteligencia Artificial
- Aprendizaje Automático
- Blockchain
- Automatización & orquestación
- Agnosticismo de marcas
- Tecnologías de nicho

Arquitectura del SOC 4.0



Perspectiva 4.0

VISIBILIDAD

On Premisse

Punto Final

Ecosistema Cloud

Dato en Transito

Registros y Logs

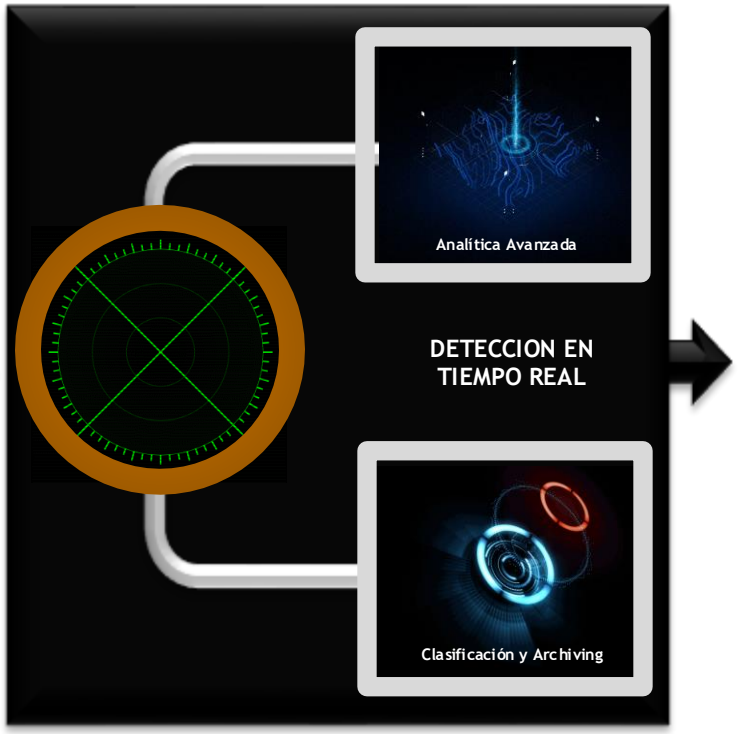
Trafico de Red

La plataforma CIOC depura los datos inyectados, luego los procesa, los complementa, los clasifica e indexa.

La optimización y enriquecimiento de datos permite reducción de costes operativos y duplicar la información.

Inteligencia de Amenazas
Contexto BIZ

ANALITICA AVANZADA



Reglas | Patrones
Modelos DS

INTERVENCION

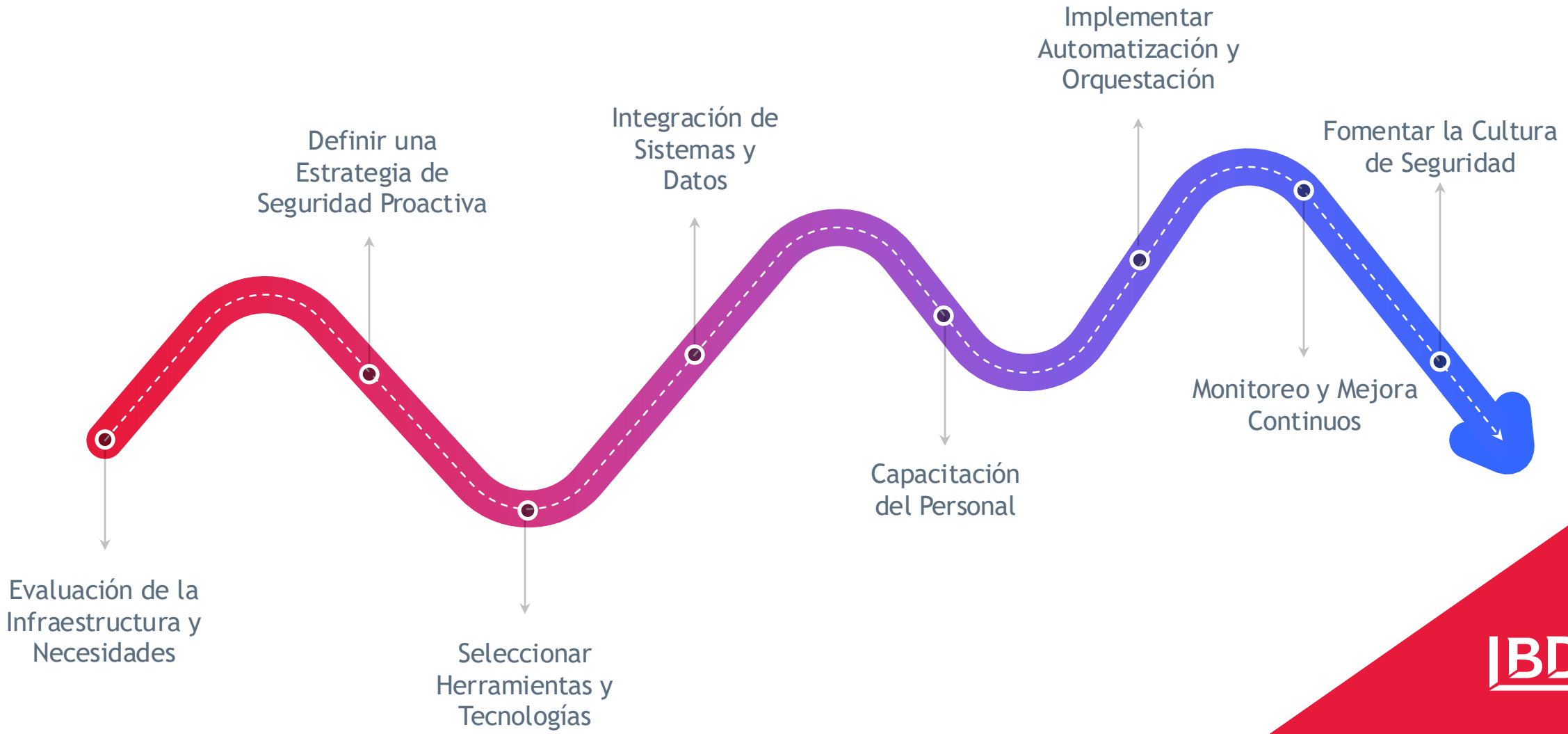
Informes | Feeds
IoC's

BDO

Tecnologías 4.0

- Inteligencia Artificial
- Machine Learning
- Automatización (SOAR)
- Tecnologías IoT
- Nube Híbrida
- Big Data Analytics

Fases de Implementación 4.0



Metodología BDO de Implementación

PASO 1: DIAGNÓSTICO INICIAL

- Realizar una auditoría de tu infraestructura y procesos actuales.
- Identificar principales vulnerabilidades y necesidades.

PASO 2: DEFINICIÓN DE OBJETIVOS

- Establecer qué se quiere lograr con el SOC (alerta y detección temprana, respuesta rápida, cumplimiento normativo).

PASO 3: SELECCIÓN TECNOLOGICA

- Basado en los recursos y necesidades, seleccionar las herramientas clave (SIEM, SOAR, OLP, IDS, EDR, XDR, IA).

PASO 4: DISEÑO DEL PROCESO

- Definir los flujos de trabajo para monitoreo, análisis y respuesta a incidentes.
- Crear playbooks automáticos para respuestas comunes.

PASO 5: IMPLEMENTACIÓN GRADUAL

- Se comienza con un piloto en áreas críticas.
- Se escala progresiva-mente integrando más sistemas y funciones.

PASO 6: CAPACITACIÓN Y CULTURA

- Entrenar al capital humano en nuevas tecnologías y procedimientos.
- Promover una cultura transversal de seguridad

PASO 7: MONITOREO Y MEJORA CONTINUA

- Evaluar regularmente el rendimiento del SOC.
- Ajustar las estrategias según los resultados, las tendencias de riesgos y cambios tecnológicos.

¿Porqué BDO?

En resumen, tercerizar la gestión de ciberseguridad es una estrategia que puede mejorar significativamente la protección de los activos digitales, optimizar recursos y garantizar un cumplimiento efectivo con las normativas vigentes.

Sin embargo, es importante seleccionar cuidadosamente al proveedor para asegurar una relación basada en confianza y competencia técnica adecuada.

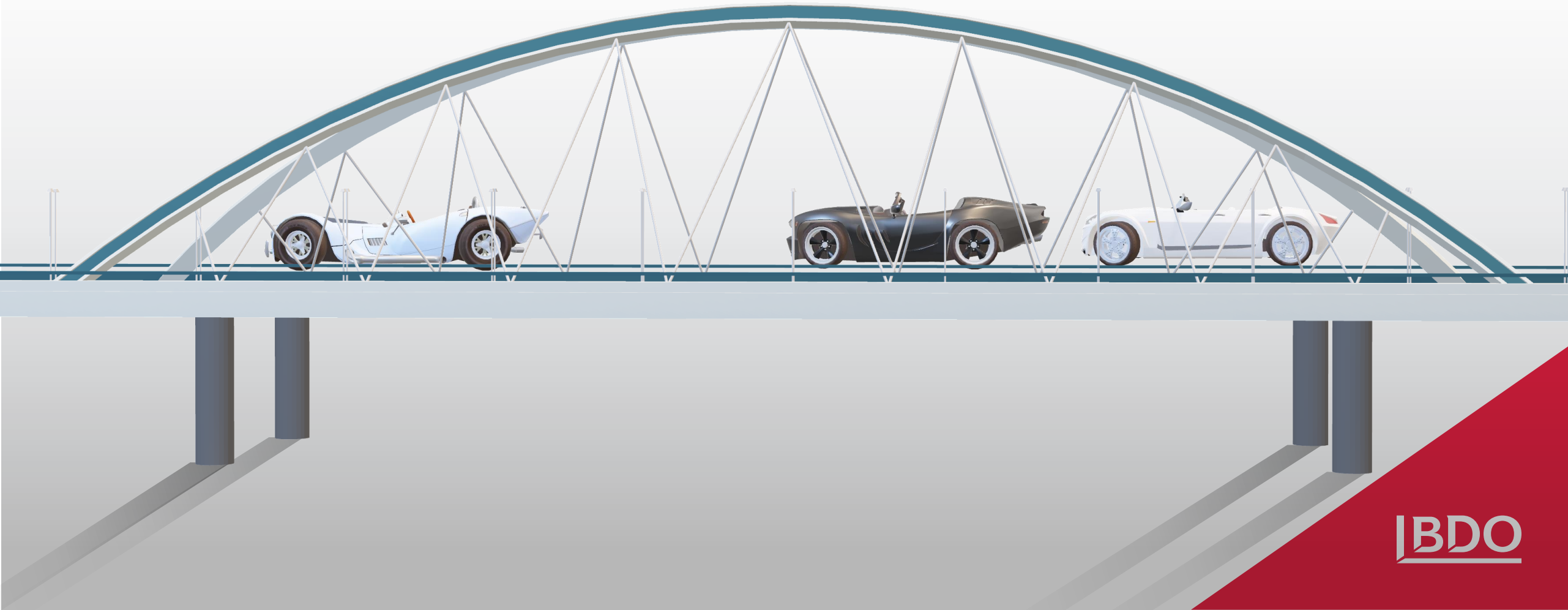
- Acceso a especialización y tecnología avanzada
- Reducción de costos
- Enfoque en el core business

- Respuesta experta ante incidentes
- Cumplimiento normativo y gestión de riesgos
- Actualización continua

- Adaptación a nuevas amenazas
- Escalabilidad y flexibilidad
- Mejora en la gestión y respuesta ante crisis


Beijing
Tokyo
Los Angeles
New York
London
Berlin
Moscow
Cyber Security Operations Center
REMOTE SENTRY WEAPON SYSTEM
Rounds Remaining
247
TIME AT 100%
16.53
BDO

En cyber competencias, sacamos ventaja…



Un puente solido hacia una cyber transformación exitosa…

BDO

NIST
CLOUD
BIA
ISO20000
BCRA
EVALUACIÓN Y AUDITORÍAS
SANS
BYOD
COBIT5
GPDR
SWIFT Security Framework
GOBIERNO, RIESGOS Y CUMPLIMIENTO
IoT
CIBERSEGURIDAD
PRIVACIDAD DE DATOS
DRP
CONSULTORÍA TI
ISO22301
GESTIÓN DE LA CONTINUIDAD
COMPLIANCE
PCI-DSS
ISO27001
GESTIÓN DE INCIDENTES
COSO
ISAE3402
ERP
ITIL
BCP
ISO38500
SERVICIOS GESTIONADOS

Fabián Descalzo
Socio
fdescalzo@bdoargentina.com

CIT | Ciberseguridad y Gobierno Tecnológico
DRAS | DIGITAL ASSURANCE, AUDIT & COMPLIANCE SERVICES