TECNODATA

TECNODATA: PORTAFOLIO DE SOLUCIONES

Resiliencia y Continuidad operativa

Alfonso Chagoyán 8-Enero-2026

Situación Actual

El panorama global en 2025 está marcado por tensiones geopolíticas, el auge de tecnologías emergentes —como la inteligencia artificial— y la creciente interdependencia de las cadenas de suministro.

Los ataques cibernéticos son un gran negocio, con ingresos estimados hasta por 10.5B de Euros en 2025 (según datos de EY)

Los impactos de un ciberataque en la empresa pueden ser:

- Pérdidas extraordinarias por fraudes, robos de información o interrupciones operativas.
- Gastos no previstos por reparación de sistemas, consultorías externas, abogados y multas regulatorias.
- Reducción de ingresos por caída de operaciones, pérdida de clientes o cancelación de contratos.
- Impactos financieros de pólizas y gastos preventivos

Tecnodata

“Nuestra misión y pasión es poner la tecnología al servicio de las personas y los negocios, creando organizaciones más humanas, eficientes, rentables y resilientes, siendo aliados estratégicos y asesores de confianza para directores y ejecutivos.”

Firma de tecnología y ciberseguridad enfocada en resiliencia, continuidad operativa y control del riesgo.

Visión estratégica y ejecutiva
Experiencia en entornos críticos
Acompañamiento de largo plazo

Tenemos alianzas con la principales marcas de Ciberseguridad y de tecnologia como Oracle.

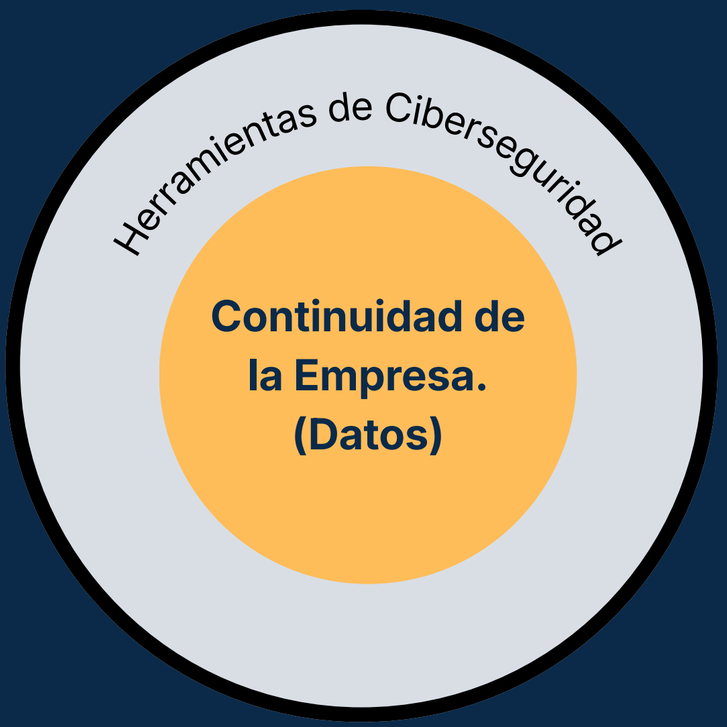
Formamos parte de ALAPSI (Asociación Latinoamericana de Profesionales en Seguridad Informática)

Nuestro Enfoque

Personas

Procesos

Tecnología



NIST Cybersecurity Framework

Servicios y Consultoría por profesionales de la industria.

Modelo de Resiliencia Operativa

	Prevención	Contención	Recuperación
Objetivo:	Reducir ataques y fraudes de manera proactiva.	Detener el incidente antes de que su impacto escale	Garantizar la continuidad del negocio.
Acciones:	Bloqueo de los principales vectores de ataque. Proteccion de los activos críticos del negocio.	Detección temprana de ataques avanzados que lograron vulnerar el perímetro.	Evita el pago de rescates (Ransomware) Recuperar la operación en minutos, no en semanas Restaura completa de información crítica, sin necesidad de respaldos.
Soluciones:	Sophos: Firewall, email Protection Double Octopus, Data Loss Prevention. Security Packs: Oracle Database	EDR/XDR: Sophos, Crowdstrike, Sentinel One, Microsoft Defender Halcyon	Halcyon

Plataforma de ciberseguridad: Firewall, Endpoints (EDR/XDR) y protección de correo electrónico.

Sophos, Crowdstrike, SentinelOne y Ms. Defender.

El EDR reduce el riesgo operativo protegiendo red, usuarios y correo desde una sola plataforma.

LLa plataforma de Sophos incluye: Firewall, EDR (protección a endpoints servidores y computadoras y protección a correo electrónico.

Todo desde una plataforma y portal unificado.

- Plataforma unificada: Red, endpoints y correo operan de forma coordinada, no como herramientas aisladas.
- Respuesta automática entre capas: Una amenaza detectada en un endpoint puede aislarse desde el firewall en segundos.
- Visibilidad centralizada: Un solo panel para entender riesgos, usuarios, dispositivos y ataques activos.
- Prevención y contención antes de que el incidente se propague.
- Correo, usuario y red: los tres puntos más explotados por ransomware y phishing.
- Escalabilidad empresarial

Double Octopus

Autenticación sin contraseñas para continuidad y seguridad empresarial

Las contraseñas siguen siendo el principal punto de entrada a incidentes de seguridad, ransomware y fraudes. Además, generan fricción operativa, costos ocultos y dependencia constante de soporte técnico.

Double Octopus, es una plataforma de autenticación sin contraseñas (passwordless) que elimina el uso de credenciales gestionadas por usuarios en todo el entorno empresarial, incluyendo aplicaciones legacy, VPN, accesos remotos y privilegios críticos.

SEGURIDAD

- Elimina el principal vector de ataques y ransomware
- Autenticación resistente a phishing y robo de credenciales
- Tokens efímeros cifrados en lugar de contraseñas persistentes

CONTINUIDAD

- Protege accesos críticos sin rediseñar la infraestructura
- Funciona en entornos híbridos: on-prem, cloud y legacy
- Reduce riesgos operativos asociados a accesos privilegiados

EFICIENCIA

- Hasta 67 % menos tickets de soporte por accesos
- Sin resets de contraseñas ni bloqueos de cuenta
- Implementación rápida y transparente para el usuario

COSTO / ROI

- Reduce costos de gestión de contraseñas y múltiples MFA
- Menor carga operativa en IT y Service Desk
- Retorno de inversión claro y medible en corto plazo

Data Loss Prevention.

Autenticación sin contraseñas para continuidad y seguridad empresarial

Las contraseñas siguen siendo el principal punto de entrada a incidentes de seguridad, ransomware y fraudes. Además, generan fricción operativa, costos ocultos y dependencia constante de soporte técnico.

Double Octopus, es una plataforma de autenticación sin contraseñas (passwordless) que elimina el uso de credenciales gestionadas por usuarios en todo el entorno empresarial, incluyendo aplicaciones legacy, VPN, accesos remotos y privilegios críticos.

SEGURIDAD

- Elimina el principal vector de ataques y ransomware
- Autenticación resistente a phishing y robo de credenciales
- Tokens efímeros cifrados en lugar de contraseñas persistentes

CONTINUIDAD

- Protege accesos críticos sin rediseñar la infraestructura
- Funciona en entornos híbridos: on-prem, cloud y legacy
- Reduce riesgos operativos asociados a accesos privilegiados

EFICIENCIA

- Hasta 67 % menos tickets de soporte por accesos
- Sin resets de contraseñas ni bloqueos de cuenta
- Implementación rápida y transparente para el usuario

COSTO / ROI

- Reduce costos de gestión de contraseñas y múltiples MFA
- Menor carga operativa en IT y Service Desk
- Retorno de inversión claro y medible en corto plazo

Halcyon

Detecta, Previene y Detiene el Ransomware.

Solución única contra el ransomware, se compone de:

Licenciamiento: Incluye modelos de Machine Learning (AI), Intercepción de Llaves Criptográficas y Detiene la Exfiltración de datos.

Servicios de monitoreo 7x24x365 días

Evita que el cibersecuestro se ejecute.

Elimina la necesidad de pagar un rescate.

Detiene las filtraciones de datos y los intentos de “doble extorsión”.

Recuperación del cibersecuestro sin copias de seguridad en minutos, no en semanas.

Servicios de Base de Datos Oracle

La Base de Datos más segura y confiable

Configuración de los packs de seguridad de Oracle como Advanced Security, Transparent Data Encription.

Así como assessment sobre la utilización de licenciamiento y la protección a la inversión.

Afinación de bases de datos transaccionales.

Servicios de Consultoria

Evaluamos el estado real de seguridad y exposición al riesgo para ayudar a la dirección a priorizar acciones, inversiones y controles, con los siguientes assessments:

Ciberseguridad:
Penetration Test
Vulnerability Test
Security Wireless Test
Revisión de Información filtrada en dark web.

Evaluación Sistemas de ERP: SAP, Netsuite, Microsoft.

Análisis de Hardening para la nube de Microsoft Azure.

“La ciberseguridad no es un gasto en TI; es una decisión financiera para proteger operaciones, flujo de efectivo y valor empresarial.”

Seguridad

Protege el flujo de efectivo y el valor del negocio

Continuidad y Eficiencia

Garantiza continuidad operativa y estabilidad financiera

ROI

Convierte riesgo en eficiencia y retorno de inversión (ROI)

La ciberseguridad efectiva se construye con decisiones informadas.

Los ejecutivos deben tener un enfoque preventivo a uno reactivo. (OPEX vs CAPEX)

- Conversemos sobre cómo priorizar su estrategia
- Inicie con un diagnóstico claro
- Evaluemos juntos el punto de partida adecuado

Contáctanos: Alfonso Chagoyán. alfonso.chagoyan@tecnodata.mx