SEGURIDAD AMÉRICA.com

ciberseconsultorias

Contenido público

QUIÉNES SOMOS

SEGURIDAD AMÉRICA.COM
cibersec consultorias

SEGURIDAD AMÉRICA.COM
Fortaleciendo Internet

ostec
Segurança digital de resultados

CERTIFICACIONES QUE DAN CREDIBILIDAD A NUESTRAS OFERTAS

Nuestros servicios de consultoría están certificados según las normas **ISO/IEC 27001** y **27701**, lo que refleja nuestro compromiso con la seguridad y privacidad de los datos.

CERTIFICATE OF APPROVAL

No. QMS-02274

This is to certify that the Management System at

SEGURIDAD AMÉRICA SSL LIMITADA

of

Rua Luis Pedro Oliveira - 541, Tubarão SC 88704-290
Brasil

Has been examined by assessors of QMS Certification and found to be conforming to the requirements of:

ISO/IEC 27001:2022

Information Security Management System

In respect of the following activities:

IAF Code: N/A
Information privacy management system for consulting, management, administration, maintenance, operation and provisioning of information security, cyber security and privacy services and solutions. Version of the Statement of Applicability: v.02. This certificate is part of the certification scope granted to the organization OSTEC CONSULTORIA E SERVIÇOS EM SEGURANÇA LTDA / DECONVE TECNOLOGIA LTDA ME / SEGURIDAD AMÉRICA SSL LIMITADA / DÉDALO INTELIGÊNCIA EM SEGURANÇA DA INFORMAÇÃO LTDA / ENORX LTDA

This certificate is valid from **06/24/2025** to **06/23/2028**
Original certification date: **06/24/2025**
Issue Date: **06/24/2025**

This registration is subject to the company continuing to maintain an effective control of the above mentioned management system, which shall be monitored by QMS Certification.

Neifer Franca, Chief Executive Officer

QMS CERTIFICATION I 145 Fagundes Filho Av, Suite 31/32 SP I BR
To verify the validity of this certificate, please visit: https://www.iafcertsearch.org

CERTIFICATE OF APPROVAL

No. QMS-02275

This is to certify that the Management System at

SEGURIDAD AMÉRICA SSL LIMITADA

of

Rua Luis Pedro Oliveira - 541, Tubarão SC 88704-290
Brasil

Has been examined by assessors of QMS Certification and found to be conforming to the requirements of:

ISO/IEC 27701:2019

Privacy Information Management System

In respect of the following activities:

IAF Code: N/A
Information privacy management system for consulting, management, administration, maintenance, operation and provisioning of information security, cyber security and privacy services and solutions. Data Processor and Controller (PII Controller. Version of the Statement of Applicability: v.02. Certificado de extensão do certificado nº QMS-02274 (ISO/IEC 27001:2022). This certificate is part of the certification scope granted to the organization OSTEC CONSULTORIA E SERVIÇOS EM SEGURANÇA LTDA / DECONVE TECNOLOGIA LTDA ME / SEGURIDAD AMÉRICA SSL LIMITADA / DÉDALO INTELIGÊNCIA EM SEGURANÇA DA INFORMAÇÃO LTDA / ENORX LTDA

This certificate is valid from **06/24/2025** to **06/23/2028**
Original certification date: **06/24/2025**
Issue Date: **06/24/2025**

This registration is subject to the company continuing to maintain an effective control of the above mentioned management system, which shall be monitored by QMS Certification.

Neifer Franca, Chief Executive Officer

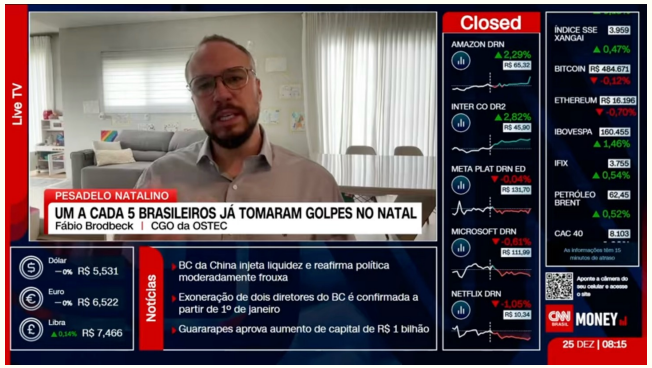
QMS CERTIFICATION I 145 Fagundes Filho Av, Suite 31/32 SP I BR

QUIÉN SOY

FABIO BRODBECK

- COO en Seguridad América Cibersec Consultorías;
- CGO en OSTEC Business Security;

- MBA Cybersecurity Governance & Management;
- MBA Project Management



RESILIENCIA CIBERNÉTICA_

CÓMO PREPARARSE PARA LOS RIESGOS DE LA ERA ACTUAL

09 DE ABRIL DE 2026

SEGURIDADAMÉRICA.COM
ciberseconsultorias

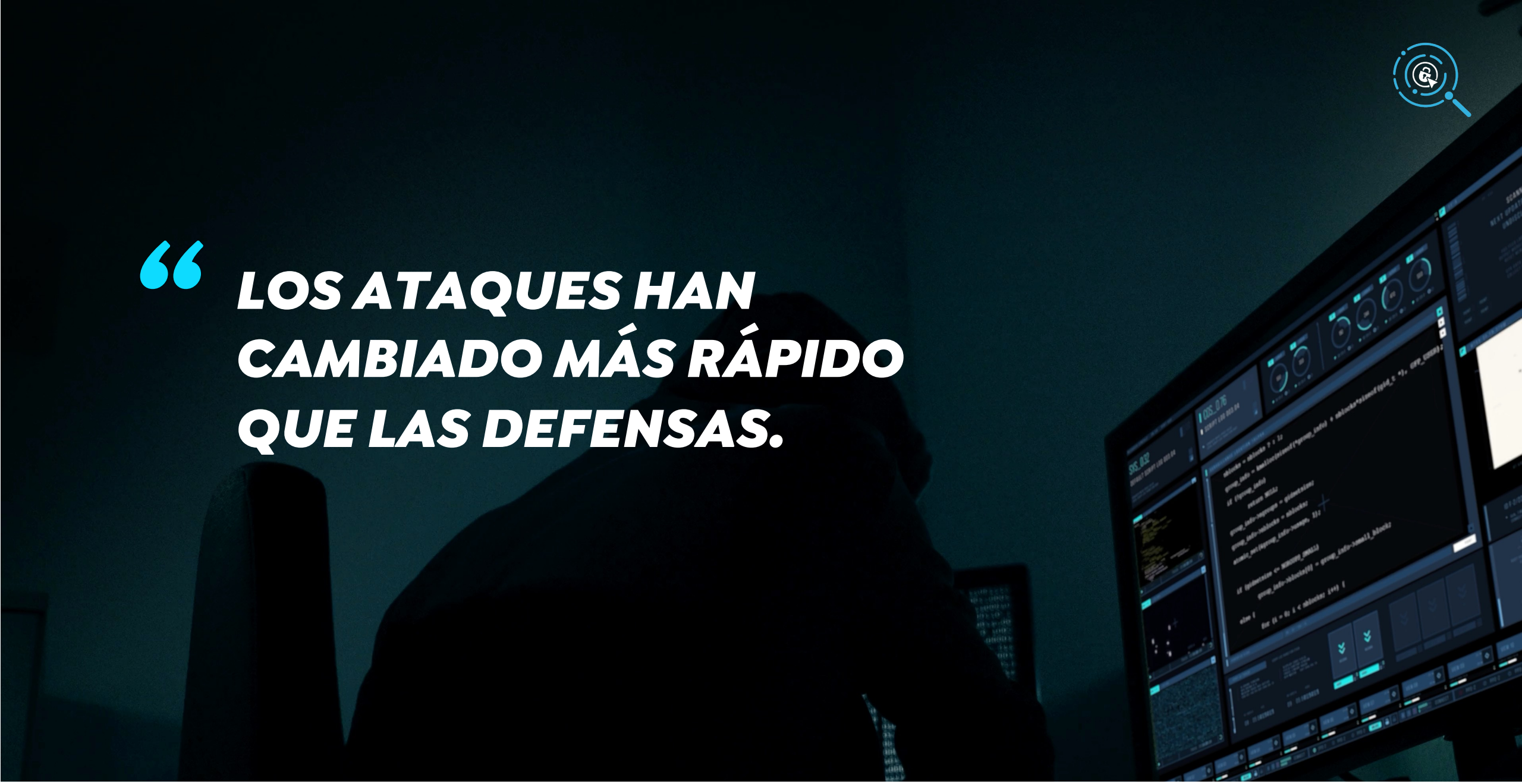
AGENDA

- El mundo ha cambiado;
- Nuevo perfil de ataques y riesgos;
- Resiliencia Cibernética;
- Cómo crearla y mantenerla
  - Tecnologías
  - Procesos
  - Personas

PÁGINA PARA PRESENTAR DATOS QUE JUSTIFIQUEN LA IMPORTANCIA DE LA CIBERSEGURIDAD

> Algo aumentó un **78%** en comparación con el año pasado, lo que representa el triple del aumento de los últimos 5 años.
>
> Fuente: Un sitio web confiable

> En Latinoamérica, algo ha empeorado un **238%** en los últimos dos años.
>
> Fuente: Algún portal de noticias


“ LOS ATAQUES HAN CAMBIADO MÁS RÁPIDO QUE LAS DEFENSAS.

EL MUNDO HA CAMBIADO_

> *Durante muchos años, las empresas han hecho bien su trabajo:*

_ ***Firewall*** *de nueva generación;*

_ ***Antivirus*** *más modernos;*

_ ***Backups con inmutabilidad****, off-site etc;*

_ ***Políticas****, normas y procedimientos;*

_ *Entrenamiento de* ***personas****;*

EL MUNDO HA CAMBIADO_

> *El escenario cambió debido a tres fuerzas principales:*

_ ***La IA democratiza los ataques**: cualquiera puede generar contenido creíble y lanzar ataques sin necesidad de conocimientos técnicos;*

_ ***Cibercrimen organizado** como sector, es altamente escalable y ofrece contratación bajo demanda;*

_ ***Aumento masivo de la superficie de ataque** (cloud, SaaS, integraciones etc.)*

EL MUNDO HA CAMBIADO_

> *Las defensas han evolucionado... pero los* ***ataques han evolucionado mucho más rápido;***

> *En general, las empresas han mejorado su seguridad, pero los* ***atacantes han cambiado las reglas del juego;***

> ***Los conocimientos básicos siguen siendo necesarios, ¡pero ya no son suficientes por sí solos!***

Y... HACER LO BÁSICO ¡YA NO ES FÁCIL!

NUEVO PERFIL DE ATAQUES

- La constatación de que **atacar nunca ha sido tan fácil**;
- Básicamente, **cualquiera puede**:
  - Crear el **phishing perfecto** usando IA (Worm/FraudGPT);
  - **Automatizar** ataques;
  - Comprar **acceso inicial** en la deep/dark web;

- El **perfil del atacante** ha cambiado:
  - Ya no necesitan **saber programar**;
  - **No explotan** vulnerabilidades complejas;
  - Han migrado de lo **físico a lo digital** (masificación);

- **Los objetivos** también están cambiando:
  - El ransomware sigue siendo efectivo, centrándose en la urgencia derivada del tiempo de inactividad (**ataque ruidoso**);
  - Cada vez hay más interés en la persistencia (**ataque silencioso**), el **valor añadido** de los datos y el contexto (fraude, malversación, extorsión);

“EL ATACANTE PROMEDIO DE HOY EN DÍA ES MÁS EFICAZ Y CAUSA MÁS DAÑO QUE EL DE HACE 5 AÑOS.

CAMBIO EN LOS RIESGOS_

NUEVAS PUERTAS DE ENTRADA

> ***La idea de ataques sofisticados, con un alto nivel de complejidad técnica, se limita a escenarios muy específicos: espionaje, guerra entre estados-nación, entre otros.***

> ***La mayoría de los incidentes comienzan de forma sencilla: explotando a las personas, los puntos de acceso y la confianza existente en entornos internos o externos.***

RESILIENCIA CIBERNÉTICA_

Acción: *iniciativas de aprendizaje (cambio cognitivo), ingeniaría del caos*

Resultado: *mejora progresiva*

Acción: *evaluación de riesgos, defensa en profundidad, redundancia, adaptabilidad (cambio conductual)*

Resultado: *extensibilidad flexible*

Acción: *evaluación de riesgos, defensa en profundidad, redundancia*

Resultado: *degradación flexible*

Acción: *sobrevive dentro de los límites de funcionamiento especificados*

Resultado: *colapso del sistema*

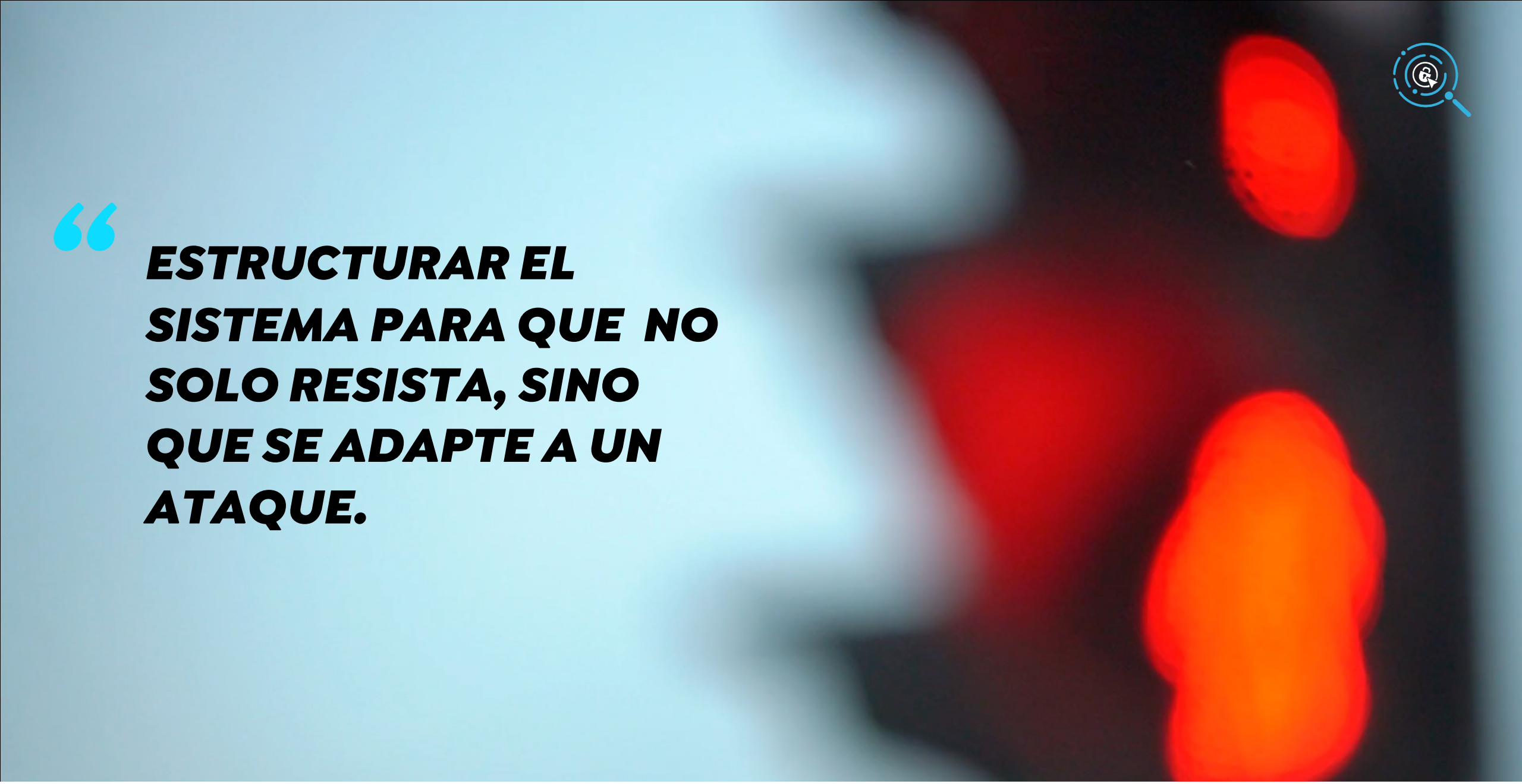
Acción: *interrumpido por factores estresantes internos y externos*

Resultado: *colapso del sistema*

ANTIFRÁGIL

EL SISTEMA RESILIENTE

- ***Anticipación:*** *Identificar posibles amenazas mediante evaluaciones de riesgos e inteligencia sobre amenazas;*
- ***Resistencia:*** *Mantener las operaciones críticas durante un ataque, a menudo utilizando arquitecturas de confianza cero para su contención;*
- ***Recuperación:*** *Restaurar sistemas y datos rápidamente, utilizando copias de seguridad y redundancia para minimizar la interrupción operativa;*
- ***Adaptación:*** *Aprender de los incidentes para mejorar las defensas, pasando de la mera protección a una seguridad integral y en constante evolución.*



“ESTRUCTURAR EL SISTEMA PARA QUE NO SOLO RESISTA, SINO QUE SE ADAPTE A UN ATAQUE.

CONSTRUYENDO RESILIENCIA

LOS PILARES ESENCIALES

TECNOLOGÍA

HERAMIENTAS Y ARQUITECTURA

INFRAESTRUCTURA DE DEFENSA Y RECUPERABILIDAD

PROCESOS

GOBERNANZA Y OPERACIONES

CONSISTENCIA, REPETIBILIDAD Y PREPARACIÓN

PERSONAS

CULTURA Y COMPORTAMIENTO

EL LAZO DE LOS PILARES

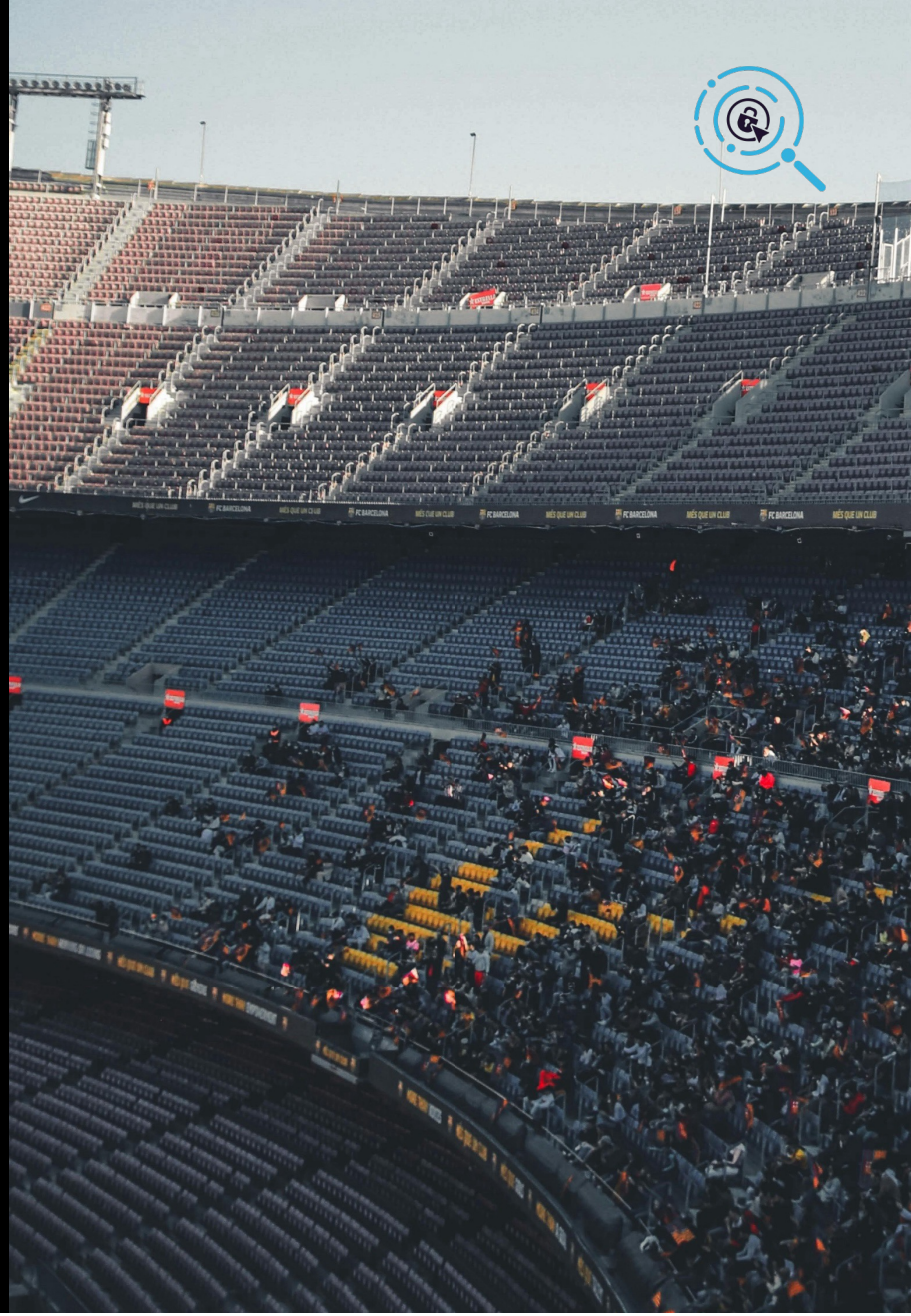
TECNOLOGÍA_

MÁS ALLÁ DE LAS SOLUCIONES

- > ***Arquitectura Zero Trust***
- > ***Gestión de Identidad y Accesos***
- > ***Protección de Endpoint y Redes***
- > ***Detección y Monitoreo***
- > ***Protección de Datos***
- > ***Recuperación y Disponibilidad***
- > ***Gestión de Vulnerabilidades***

- > ***Selección de tecnologías***
- > ***Implementación***
- > ***Configuraciones***
- > ***Adecuación continua***
- > ***Quality Assessments***

¿CUÁNTOS RECURSOS DE LAS SOLUCIONES NO SON UTILIZADOS ACTUALMENTE?



PROCESOS_

MÁS ALLÁ DE LOS PAPELES

- Gestión de riesgos
- Respuesta a incidentes
- Plan de Continuidad de Negocio
- Gestión de cambios y configuración
- Gestión de riesgos de terceros
- Cumplimiento y auditoría
- Integración de inteligencia y amenazas

- Conocimiento técnico del equipo
- Conocimiento de los procesos
- Garantía de ejecución
- Continuidad de los procesos
- Gobernanza y políticas
- Actuar bajo presión

¿CÓMO REACCIONA TU EQUIPO ANTE UNA SITUACIÓN DE EMERGENCIA?

PERSONAS_

MÁS ALLÁ DE ENTRENAMIENTOS

- > Concienciación y formación en seguridad
- > Roles y responsabilidades claros
- > Compromiso ejecutivo y de la directiva
- > Cultura de seguridad
- > Gestión de amenazas internas
- > Desarrollo de talentos y capacidades

- > Responsabilidad
- > Compromiso de todos
- > Rol individual en la seguridad
- > Interés por seguridad


EN SU EMPRESA, ¿LAS PERSONAS SON EL ESLABÓN MÁS DÉBIL O EL MÁS FUERTE?

EL SISTEMA RESILIENTE ANTIFRÁGIL

- Los sistemas antifrágiles **se benefician** al enfrentar incidentes cibernéticos;
- Los sistemas antifrágiles **transitan** de un estado de interrupción a uno de recuperación y, finalmente, a uno de mejora;
- **El desorden** en los sistemas antifrágiles siempre resulta beneficioso;
- Los sistemas antifrágiles responden positivamente a las amenazas, aprovechando sus **oportunidades de aprendizaje**;

> ***Los sistemas antifrágiles son inmunes a las amenazas.***

- *Diagnóstico de Ciberseguridad*
- *Outsourcing*
- *Análisis de Superficie de Ataque*
- *Ethical Hacking/Pentest*
- *Gestión Continua de Vulnerabilidades*
- *Simulación de Phishing*
- *Programa de Concientización*
- *Seguridad de Cadena de Sumnistro*
- *Hardening de Soluciones*
- *Revisión/Desarrollo de Políticas de Seguridad*

NUESTRO COMPROMISO CON TU SEGURIDAD_

NUESTRO COMPROMISO CON TU SEGURIDAD_

- **20% de descuento** en las consultorías para los participantes (*one shot* o 1 año en servicios continuos);
- Un **Análisis de Superficie de Ataque gratis** a las 5 personas que respondan estas preguntas.

SEGURIDADAMÉRICA.com ciberseconsultorías

“¿PREGUNTAS?

Fabio Brodbeck

+55 (48) 99122-6644

serv@seguridadamerica.com

fabio@ostec.com.br

SEGURIDAD AMÉRICA.com
cibersec consultorias

SEGURIDAD AMÉRICA.com

ciberseconsultorias

Contenido público