



FORTINET[®]
COLOMBIA



Juan Carlos Puentes
Country Manager Fortinet Colombia
ANDI - 11 Shared Services Center Forum



FORTINET



**MÁS
PAÍS**

11.º SHARED SERVICES CENTER FORUM 2026
DE LA EFICIENCIA AL VALOR EMPRESARIAL

Ciberresiliencia en Centros de Servicios Compartidos

De la eficiencia operacional
a la continuidad del negocio.



Operaciones
más eficientes



Servicios
más seguros



Mayor confianza
del negocio



Organizaciones
más resilientes

SECURE NETWORKS EVERYWHERE

GLOBAL
SERVICES
GREATER
POSSIBILITIES

FINANCE
HUMAN RESOURCES
PROCUREMENT
IT SERVICES
CUSTOMER EXPERIENCE
DATA & ANALYTICS
AND MORE

PEOPLE
PROCESSES
TECHNOLOGY
A STRONGER
TOMORROW



El CSC se convirtió en un punto crítico del negocio

Los Centros de Servicios Compartidos habilitan múltiples funciones y compañías, conectando personas, procesos y datos en diferentes países. Un incidente ya no afecta "un área", puede impactar simultáneamente todo el negocio.



UN CSC.
MÚLTIPLES
CONEXIONES.
MAYOR IMPACTO.

Múltiples compañías

Varios países

Procesos interconectados

Cientes internos y externos

BOGOTÁ
NUEVA YORK
MADRID
CIUDAD DE MÉXICO
SÃO PAULO
SINGAPUR



El impacto de un incidente en un CSC puede ser:



Operativo
Interrupción de procesos críticos



Financiero
Pérdidas y penalidades



Reputacional
Pérdida de confianza de clientes y aliados



Regulatorio
Incumplimiento normativo



Estratégico
Frenar iniciativas de crecimiento

La paradoja de los Centros de Servicios Compartidos

La centralización genera gran valor, pero también concentra dependencias que pueden poner en riesgo la continuidad del negocio.

PERSONAS
PROCESOS
TECNOLOGÍA
UN SOLO PROPÓSITO:
CONTINUIDAD



El verdadero reto no es solo ser más eficientes,
sino ser más resilientes.

¿Qué puede detener **un CSC hoy?**

Cinco escenarios reales que pueden interrumpir la operación, afectar múltiples compañías y comprometer la continuidad del negocio.

SECURE
NETWORKS
EVERYWHERE

PERSONAS
PROCESOS
TECNOLOGÍA
UN SOLO PROPÓSITO:
RESILIENCIA

01



Ransomware

Cifrado de sistemas y paralización de procesos críticos (finanzas, nómina, operaciones).



02



Compromiso de identidad

Acceso no autorizado que permite fraude, robo de información y movimiento lateral en múltiples áreas.



03



Interrupción de nube y SaaS

Indisponibilidad de aplicaciones esenciales para el negocio (ERP, colaboración, RR. HH., servicio al cliente, etc.).



04



Ataque a terceros y supply chain

Compromiso de proveedores, BPOs o socios que impacta directamente la operación del CSC.



05



IA y fuga de información

Uso no controlado de GenAI, exposición de datos sensibles y riesgos asociados a nuevas formas de ataque.



El impacto va más allá de un área:



Múltiples compañías



Varios países



Procesos críticos



Clientes internos y externos



Pérdidas financieras y reputacionales

Ciberseguridad $\neq$ Ciberresiliencia

Diferentes preguntas. Enfoques complementarios. Un mismo objetivo: un negocio más fuerte y preparado para lo que venga.



Ciberseguridad

“¿Cómo **prevenimos** el ataque?”



Identificar y reducir la superficie de ataque



Bloquear amenazas conocidas y desconocidas



Proteger personas, dispositivos y datos



Aplicar controles, políticas y cumplimiento

ENFOQUE EN
EVITAR QUE OCURRA

AMENAZAS

ATAQUES

VULNERABILIDADES

INCERTIDUMBRE

CONTINUIDAD

CONFIANZA

OPERACIÓN

CRECIMIENTO

UN
NEGOCIO
MÁS FUERTE



Ciberresiliencia

“¿Cómo **seguimos operando** cuando la prevención no es suficiente?”



Detectar y responder rápidamente



Mantener servicios críticos en operación



Recuperar y adaptarse



Aprender y mejorar continuamente



Fortalecer la confianza de clientes, aliados y reguladores

ENFOQUE EN
SEGUIR OPERANDO SIEMPRE



La ciberseguridad reduce la probabilidad.
La ciberresiliencia garantiza la continuidad.



Misma visión.
Mayor valor para el negocio.

De proteger tecnología a proteger servicios críticos

La ciberresiliencia en un CSC va más allá de la infraestructura.
Se trata de asegurar la continuidad de los servicios que impulsan el negocio.

SECURE
NETWORKS
EVERYWHERE



Cuando protegemos los servicios críticos del CSC, protegemos la operación, la experiencia de los clientes y el crecimiento del negocio.



Procesos de negocio que dependen del CSC



Nómina y Gestión de Talento



Cuentas por Pagar y Cuentas por Cobrar



Compras y Abastecimiento



Servicio al Cliente y Operaciones



Finanzas y Planeación



TI y Servicios Tecnológicos



Data & Analytics e Inteligencia de Negocio

El ciclo de Ciberresiliencia

De la estrategia a la recuperación, un ciclo continuo para mantener los servicios críticos en operación.

SECURE
NETWORKS
EVERYWHERE

ORGANIZACIONES
MÁS RESILIENTES
PARA UN MUNDO
MÁS COMPLEJO.



La ciberresiliencia no es un proyecto,
es **una capacidad continua del negocio.**

PERSONAS. PROCESOS. TECNOLOGÍA.
RESULTADOS REALES.

Cuando ocurre el incidente: **velocidad + coordinación**

De la detección a la recuperación, con un equipo, un plan y la tecnología adecuada para mantener el negocio en operación.

EQUIPOS
CONECTADOS
DECISIONES
MÁS RÁPIDAS
NEGOCIOS
MÁS RESILIENTES.

SECURE
NETWORKS
EVERYWHERE

DE LOS
INCIDENTES
A LAS
OPORTUNIDADES
DE SER MÁS
FUERTES.



Habilitado por:



Personas

Equipos multidisciplinarios, roles y responsabilidades claras.



Procesos

Planes de respuesta probados, gobernanza y comunicación efectiva.



Tecnología

Visibilidad integral, automatización y orquestación de respuestas.



Resultado:



Menor tiempo de impacto en el negocio.



Mayor continuidad de los servicios críticos.



Organizaciones más resilientes.

IA: acelerador del CSC... y nueva superficie de riesgo

La inteligencia artificial puede impulsar la eficiencia, la innovación y la experiencia en los servicios compartidos. Pero también amplía la superficie de riesgo si no se gestiona adecuadamente.

SECURE
NETWORKS
EVERYWHERE

LA IA POTENCIA
TU NEGOCIO.
CUANDO LA USAS
DE FORMA SEGURA
Y RESPONSABLE.

IA para la productividad

Un CSC más eficiente, inteligente y centrado en las personas.



Automatiza tareas repetitivas

Acelera procesos como clasificación de solicitudes, resúmenes, reportes y gestión documental.



Mejora la experiencia de empleados y clientes

Asistentes virtuales que responden más rápido y con mayor precisión.



Genera insights para mejores decisiones

Análisis de datos en lenguaje natural y detección de tendencias.



Impulsa la innovación

Nuevos servicios, mayor valor y foco en actividades de alto impacto.



Aumenta la eficiencia y la escala

Más capacidad con los mismos recursos.



Más tiempo para lo que realmente importa: las personas y el crecimiento del negocio.

IA como nueva superficie de riesgo

Nuevos vectores, nuevas amenazas, mayor exposición.



Shadow AI

Uso no autorizado de herramientas de IA por parte de empleados, sin control ni visibilidad.



Datos sensibles en GenAI

Información corporativa, financiera o de clientes compartida en modelos públicos.



Identities no humanas y agentes

Agentes de IA y automatizaciones con accesos y permisos que pueden ser mal gestionados.



Ataques a través de prompts

Manipulación de instrucciones para obtener información sensible, evadir controles o generar contenido malicioso.



Aplicaciones y ecosistemas de IA

Integración con terceros y plugins que amplían la exposición de datos y sistemas.



La innovación sin control también aumenta el riesgo.

MISMAS
OPORTUNIDADES.
NUEVOS DESAFÍOS.

PERSONAS
MÁS CAPACIDAD
MÁS VALOR
UN CSC
MÁS INTELIGENTE

NUEVAS
AMENAZAS
MAYOR
EXPOSICIÓN
MAYOR
RESPONSABILIDAD

Uso seguro y responsable de GenAI



Políticas y gobernanza claras

Qué se puede usar, con qué datos y bajo qué condiciones.



Conciencia y cultura

Formación y buenas prácticas para todos los usuarios.



Controles y monitoreo

Visibilidad del uso, protección de datos y gestión de accesos.



Innovación con confianza

Aprovechar el potencial de la IA con un enfoque de seguridad y cumplimiento.

Arquitectura de ciberresiliencia para CSC/GBS

Personas, datos, aplicaciones y servicios siempre protegidos,
para que el negocio nunca se detenga.

PERSONAS
SERVICIOS
OPERACIONES
CONFIANZA

SERVICIOS COMPARTIDOS SIEMPRE EN OPERACIÓN
MÁS EFICIENCIA. MÁS RESILIENCIA. MÁS VALOR.



Acceso seguro

Las personas correctas,
con el acceso correcto,
desde cualquier lugar.



Protección de datos y aplicaciones

Lo que más importa,
siempre protegido.



Seguridad en la nube y SaaS

Operación segura
en entornos híbridos
y multi-nube.



Detección y respuesta

Visibilidad total para
actuar antes, durante
y después de un incidente.



Recuperación y mejora continua

Volver a operar más rápido
y más fuertes.

CSC / GBS

PERSONAS QUE HACEN
QUE EL NEGOCIO AVANCE

HOY
SERVICIOS
MÁS SEGUROS
PARA UN
MAÑANA
MÁS FUERTE

RESULTADOS
PARA EL NEGOCIO



Continuidad
de los servicios críticos



Mayor confianza
de clientes y aliados



Menores riesgos
y costos



Más eficiencia
y productividad



Crecimiento sostenible

La pregunta para el CEO
no es "¿podemos ser atacados?"

¿Puede nuestro Centro de Servicios
Compartidos continuar operando
cuando ocurra?

La resiliencia no se trata de si ocurrirá un incidente,
sino de qué tan preparados estamos para seguir generando valor.

MÁS
RESILIENCIA.
MÁS
CONTINUIDAD.
MÁS
OPORTUNIDADES.

01



Identificar los servicios críticos

Conocer qué procesos del
Centro de Servicios Compartidos
son esenciales para el negocio,
quiénes dependen de ellos y cuáles
serían los impactos si se ven
afectados.



02



Medir la resiliencia

Evaluar nuestro nivel de
preparación, identificar brechas
y establecer métricas claras
de continuidad y recuperación
para tomar mejores decisiones
y priorizar inversiones.



03



Probar la respuesta y recuperación

Realizar ejercicios y simulacros
que validen nuestros planes,
fortalezcan la coordinación
entre equipos y aseguren
que podemos volver a operar
en el menor tiempo posible.



Mayor continuidad
del negocio



Confianza de clientes,
empleados y aliados



Menor impacto
financiero y reputacional



Una organización
más fuerte y preparada

FORTINET®