



Ciberresiliencia Empresarial: Más allá del Cumplimiento, la Sobrevivencia del Negocio

La transformación digital ha permitido a las empresas optimizar procesos, expandir sus mercados y ofrecer nuevos servicios. Sin embargo, este avance también ha incrementado la exposición a ciberataques cada vez más sofisticados y persistentes. En este contexto, **cumplir con la Ley Marco de Ciberseguridad es una base para comenzar, pero no es suficiente**; las empresas deben adoptar una estrategia integral de ciberresiliencia que proteja sus activos y además, asegure el mantenimiento de las operaciones ante cualquier incidente. La pregunta clave ya no es si una empresa será atacada, sino **cuán preparada está para resistir y recuperarse de un ataque cibernético**.

Según Rubrik: "Los atacantes intentaron afectar las copias de seguridad en el 93% de los ciberataques y tuvieron al menos un éxito parcial en el 73% de estos intentos".

¿Cuán preparada está su organización para resistir y recuperarse de un ataque cibernético?

En NLT Secure, entendemos que la seguridad no es un destino, sino un proceso continuo. Por ello, hemos desarrollado un modelo de protección integral que combina **prevención, detección, respuesta y recuperación**, permitiendo a las organizaciones disminuir riesgos, reducir el impacto de los incidentes y mantener su operatividad ante cualquier amenaza.

De la Ciberseguridad a la Ciberresiliencia: Un Cambio de Paradigma

Durante años, la ciberseguridad se ha basado en estrategias defensivas enfocadas en evitar ataques. Sin embargo, la evolución constante de las amenazas ha demostrado que ningún sistema es 100% invulnerable. **Un modelo basado únicamente en la prevención ya no es suficiente**. Es aquí donde la ciberresiliencia marca la diferencia: en lugar de solo intentar evitar ataques, las organizaciones deben prepararse para detectarlos a tiempo, responder de manera efectiva y recuperarse con rapidez para minimizar impactos.

"Hoy en día, las empresas no pueden depender de estrategias reactivas. En NLT Secure, creemos que la ciberresiliencia debe ser un pilar estratégico que garantice la continuidad operativa, incluso en medio de un ciberataque", señala **Lorenzo Espinoza, CEO de NLT Secure**.

Para lograrlo, las organizaciones deben transformar su visión de la ciberseguridad y adoptar un enfoque holístico basado en un **modelo integro de protección**.

Los 4 Pilares del Programa de Ciberresiliencia de NLT Secure

Nuestro programa de ciberresiliencia comienza con un **diagnóstico y evaluación inicial** lo que permite construir un plan personalizado y adaptado a las necesidades y recursos de cada cliente. Este programa es guiado por un **VCISO**,



quien acompaña el programa de ciberresiliencia garantizando su desarrollo y cumplimiento, brindando recomendaciones y reporte de seguimiento trimestral.

• **Prevención: Reducción de Riesgos y Protección Activa**

La mejor estrategia contra los ciberataques es impedir que sucedan. La prevención permite **reducir la superficie de ataque y fortalecer las defensas digitales antes de que una amenaza pueda materializarse**. Esto implica la implementación de buenas prácticas de seguridad, evaluaciones periódicas de riesgos y el cumplimiento de marcos normativos. Sin una estrategia de prevención clara, las organizaciones quedan expuestas a ataques que podrían haberse evitado con medidas proactivas.

• **Detección: Identificación Temprana de Amenazas**

Aún con las mejores medidas de prevención, algunas amenazas lograrán evadir los controles de seguridad. Es por eso que la **detección temprana es fundamental**. Un sistema efectivo de detección permite **identificar actividades sospechosas en tiempo**

real, analizar patrones de comportamiento e intervenir antes de que un ataque cause **daños significativos**. Un monitoreo continuo de seguridad, junto con inteligencia de amenazas y análisis proactivo, permite a las empresas anticiparse a incidentes y tomar decisiones informadas para neutralizar riesgos.

• **Respuesta: Acción Rápida y Contención de Incidentes**

Cuando ocurre un incidente de seguridad, la velocidad y la efectividad de la respuesta determinan el impacto real en la organización. La capacidad de respuesta debe enfocarse tanto en la contención inmediata como en la mitigación de daños y la restauración de operaciones. **Contar con un equipo especializado y protocolos bien definidos permite reducir el impacto de los ciberataques y evitar su propagación dentro de la infraestructura tecnológica**.

• **Recuperación: Garantizar la Continuidad del Negocio**

Un incidente de ciberseguridad puede afectar la infraestructura tecnológica, así como la reputación, la confianza de los clientes y la estabilidad operativa de la empresa. En NLT Secure, **brindamos un potente servicio de continuidad de negocio y recuperación ante desastres (BCDRaaS)**, el cual asegura la **rápida restauración de datos y sistemas críticos, minimizando así tiempos de inactividad y garantizando la estabilidad operativa ante cualquier interrupción**. **Nuestro servicio habilita la virtualización**

instantánea de sistemas, garantizando restauraciones rápidas, verificadas y confiables, con respaldos inmutables, almacenamiento distribuido geográficamente y detección de ransomware, asegurando una **protección integral y una recuperación efectiva** sin riesgos de pérdida de datos o tiempos de inactividad prolongados.

Más que Cumplimiento, una Estrategia para Garantizar el Futuro

Las empresas resilientes no solo cumplen con la normativa, sino que protegen su reputación, su operación y la confianza de sus clientes. La **ciberresiliencia no es un gasto adicional, sino una inversión en sostenibilidad y crecimiento**. En un mundo donde las amenazas son inevitables, lo que realmente marca la diferencia es la capacidad de resistir, responder y evolucionar ante cualquier crisis digital.

Es por ello que, en NLT Secure diseñamos estrategias adaptadas a cada empresa, asegurando que puedan resistir, responder y recuperarse de cualquier ciberamenaza, sin importar su tamaño o industria.

• **¿Está tu empresa preparada para un ciberataque?**

Contactanos:

- **Email:** hello@nitsecure.com
- **Web:** www.nitsecure.com
- **Teléfono:** +56 22 399 4300
- **WhatsApp:** +1 321 732 1664
- **NLT SECURE:** Construyendo un mundo digital más seguro para todos, juntos.

