DELTA PROTECT®

# El presupuesto de ciberseguridad que tu empresa necesita

## Y cómo armarlo paso a paso

# Tabla de Contenidos

# 01. Introducción

El crecimiento acelerado de las amenazas digitales ha convertido a la ciberseguridad en una de las prioridades estratégicas más críticas para las organizaciones. Hoy en día, un ciberataque no solo compromete la continuidad operativa, también genera pérdidas financieras significativas y afecta la confianza de clientes y socios.

Ante este panorama, contar con un presupuesto de ciberseguridad bien estructurado deja de ser opcional: es la única manera de anticipar riesgos y proteger lo que más importa. En este material encontrarás un análisis del contexto actual, el impacto financiero de los ataques, las preguntas clave para definir tu presupuesto y una guía práctica para ponerlo en marcha de inmediato.

# 02. Panorama Actual: amenazas y tendencias

## Ninguna empresa es 100% segura

En el contexto digital actual, el gasto en ciberseguridad dejó de ser opcional. Los incidentes ya no son una posibilidad remota, sino una certeza estadística. La transformación digital, la hiperconectividad y la cadena de suministro extendida han aumentado la superficie de ataque en todas las industrias.

**1 de cada 3 empresas reportó haber sido víctima de inyección de código malicioso en el último año*.**

**Fuente: IBM, 2024*

## Costo promedio de un incidente

Los ciberataques no solo comprometen sistemas; comprometen resultados. El costo promedio por incidente en América Latina se estima en **$2.3 millones de dólares**, considerando desde interrupción de operaciones hasta pérdidas reputacionales y regulatorias.

Pero, ¿Qué significan para una (PYME) 2.3 millones de dólares? ¿**Por qué me atacarían a mí** que ni siquiera facturo ese monto al año? Hoy en día, el cibercrimen es masivo, automatizado y no discrimina. Con ayuda de IA, los atacantes logran desarrollar campañas masivas mientras personalizan perfiles de compañías. Industria, tamaño, regiones, rondas de inversión, tiempo en operación; elementos que les ayudan a segmentar ataques masivamente.

## Tendencias clave en el entorno actual

**El mercado de ciberseguridad está en expansión:**

En 2025, se proyecta que las empresas en LATAM asignen hasta un **15% del presupuesto total de TI a ciberseguridad** con un enfoque destacado en mayor inversión en software y servicios gestionados.

El crecimiento impulsado por la necesidad de cubrir múltiples frentes como: seguridad de endpoints, análisis de vulnerabilidades, gestión de identidad y servicios administrados, suele apalancarse de herramientas sofisticadas.

Sin embargo, en el mayor de los casos, estas se encuentran a un **50% o 60% de su potencial de uso**. Ahí es donde los servicios gestionados (MSSP) hacen su magia; con un enfoque de configuración, despliegue, monitoreo y soporte continuos, las herramientas, acompañadas del factor humano para el análisis profundo, retornan seguridad real.

**Recibe un diagnóstico personalizado →**

# 03. Impacto Financiero de los Ataques

*Un incidente no solo compromete la seguridad, compromete la viabilidad del negocio*

Cuando una empresa sufre un ciberataque, las consecuencias son **multidimensionales**: desde la respuesta inmediata hasta el impacto prolongado en ingresos, reputación y continuidad operativa.

El **costo promedio** de una brecha de seguridad a **nivel global en 2023** fue de **$4.45 millones de dólares**. En **sectores críticos como salud**, ese número puede **superar los $7.13 millones***.

## Principales rubros de impacto económico

Un solo incidente puede activar **una cadena de costos**, incluso si se decide "no pagar un rescate" en un Ransomware. Estos son los rubros más comunes:

### Respuesta y contención

Servicios forenses, consultoría externa, horas hombre de equipos internos.


### Interrupción del negocio

Downtime de sistemas críticos, pérdida de ingresos, incumplimientos contractuales.

### Pago de rescate o recuperación de activos

En ransomware, incluso si no se paga, hay que reconstruir entornos, aplicativos o hardware.

**Fuente: IBM Cost of a Data Breach Report 2023*

## Multas regulatorias

En sectores regulados (finanzas, salud, telecomunicaciones), una brecha implica sanciones millonarias que pueden comprometer la continuidad operativa del negocio.

## Costos legales

Asesoría, demandas, notificaciones obligatorias a usuarios o autoridades. Alguna vez investigué cuánto cuesta la hora de un Abogado Especialista en derecho penal informático en Ciudad de México... mejor ni mencionarlo.

## Pérdida reputacional

Clientes que se van, leads que no convierten, inversionistas que pierden confianza, proveedores preocupados.

El daño **no solo es técnico, sino financiero y prolongado**. El presupuesto en ciberseguridad es, en esencia, una **medida de control financiero preventivo**.

| FINANCIERA | RETAIL | LOGÍSTICA |
|---|---|---|
| Pérdida por fraude<br>+<br>sanción CNBV<br>+<br>churn de clientes<br>=<br>**$1.5M – $3M** | Ataque a POS con ransomware<br>=<br>**4 días sin vender**<br>+<br>pérdida de confianza | Parálisis de trazabilidad<br>=<br>**incumplimiento de entregas**<br>+<br>penalizaciones |

| TRANSPORTE | TELECOM | SaaS |
|---|---|---|
| Cancelación de rutas por brecha en mantenimiento<br>=<br>**millones en reembolsos** | Fuga de datos<br>=<br>**sanción de IFT**<br>+<br>cambio masivo de contraseñas a clientes | Robo de credenciales de clientes<br>=<br>**cancelaciones**<br>+<br>daño a marca |

*El tiempo promedio para detectar una brecha es de 207 días, y en contenerla, otros 73 días más. Durante ese tiempo, los atacantes pueden moverse libremente dentro de la red.*

# 04. Claves estratégicas para presupuestar

***Las preguntas correctas para construir la aproximación correcta***

Diseñar un presupuesto de ciberseguridad no comienza con herramientas, sino con estrategia y postura. La inversión debe responder a riesgos reales, capacidades internas, y objetivos de negocio. Estas son las claves estratégicas que deben guiar tu aproximación:

1

## Ciber Resiliencia: más allá de la prevención

El objetivo no es solamente evitar ataques, sino garantizar que la empresa **pueda resistir, responder y recuperarse** sin comprometer su operación.

*Pregunta clave: ¿Nuestra empresa podría continuar operando si mañana se encripta todo nuestro sistema principal?*

Invertir en resiliencia significa **proteger operaciones, ingresos y reputación**, no solo activos tecnológicos.

2

## Amenazas clave para nuestro negocio

No todos los riesgos son iguales. Cada industria, modelo de negocio y entorno operativo enfrenta amenazas distintas. El presupuesto debe priorizar las que **pueden impactar más gravemente la continuidad operativa o la confianza del cliente.**

*Pregunta clave: ¿Cuáles son las 3 amenazas que más afectarían nuestro negocio si se materializan? ¿Cuáles son nuestros activos de mayor valor? ¿Cómo se comunican las áreas de mi empresa entres sí mismas y con terceros?*

Estos puntos y preguntas son **claves** para priorizar tu inversión, en **dinero** y en **tiempo**.

## 3 Esfuerzo organizacional transversal

La ciberseguridad no es un proyecto del área de TI, es un **esfuerzo organizacional completo**. Desde recursos humanos hasta compras, cada área tiene un rol en la protección del negocio.

*Pregunta clave: ¿Qué tan alineados están nuestros líderes en temas de riesgo digital? ¿Hay visión común?*

Asignar presupuesto sin acompañamiento del resto de la organización **limita el impacto real de la inversión**.

## 4 Postura integrada: herramientas + cultura

Un buen presupuesto debe cubrir tanto los **controles tecnológicos** como los **factores humanos y organizacionales**. Tener un firewall sin capacitación es como tener una alarma sin personas que la escuchen.

*Pregunta clave: ¿Estamos integrando tecnología, procesos y cultura, o solo comprando software aislado?*

La seguridad efectiva es aquella que se **vive en la operación diaria**, no solo la que se instala. Definir e incentivar una cultura interna de seguridad nos permitirá vivir los procesos, aprovechar las herramientas y transmitir nuestra postura de seguridad a proveedores críticos.

*El presupuesto de ciberseguridad no se define con una hoja de Excel.*

*Se construye a partir de preguntas estratégicas, evaluación de riesgos y entendimiento del negocio.*

# 05. Guía rápida para definir tu presupuesto

El presupuesto de ciberseguridad debe construirse con base en los requerimientos reales del negocio, no solo en amenazas generales. Esta guía te permite avanzar paso a paso en la definición de un presupuesto eficaz, realista y estratégico.

## Checklist práctico para alinear prioridades, capacidades y decisiones

### 1. Prioriza por requerimientos

Antes de pensar en herramientas, piensa en lo que **estás obligado o comprometido a cumplir para seguir operando o para concretar nuevas ventas**:

- ☐ Regulaciones locales: CNBV, INAI, IFT, entre otras
- ☐ Requisitos contractuales con clientes (por ejemplo: ISO 27001, NDA, cláusulas de seguridad)
- ☐ Proyectos especiales que requieren certificaciones como requisito para participar

### 2. Identifica tu nivel de madurez actual

Evalúa con objetividad qué tan preparado estás:

- ☐ ¿Tienes visibilidad sobre tus activos críticos? (información, aplicaciones, dispositivos)
- ☐ ¿Qué controles básicos ya están implementados? ¿Funcionan bien?
- ☐ ¿Qué malas prácticas existen en tu operación (cuentas compartidas, contraseñas débiles, accesos sin MFA)?

*Una autoevaluación sencilla con base en controles como CIS v8 o NIST CSF puede ayudarte a detectar brechas inmediatas.*

### 3. Organiza tu inversión por bloques y necesidades

Distribuye el presupuesto con enfoque estratégico:

- ☐ **Requerimientos**: lo que debes cumplir (paso 1)
- ☐ **Impacto de negocio**: lo que protege la operación y evita pérdidas
- ☐ **Postura integral empresarial**: lo que construye resiliencia a largo plazo (cultura, procesos, tecnología integrada)

*Esta organización ayuda a asignar tiempo y dinero con base en prioridades de negocio.*

### 4. Define si necesitas un socio estratégico

No todo se puede (ni se debe) hacer internamente:

- ☐ Evalúa tu **conocimiento técnico disponible**: hasta dónde podrías llegar con tu personal
- ☐ Considera el **costo de oportunidad** de hacerlo tú vs. un proveedor experto. ¿Cuánto tiempo vas a asociar? ¿Qué cosas estás dejando de hacer por dedicarte al proyecto?
- ☐ Asegúrate de entender los **costos ocultos** de: evaluación inicial, licencias, implementación, configuración, soporte y mantenimiento. Todo alineado al fin último (ISO27001, definir una cultura integral, implementar un SOC, etc.)

*Un socio puede ayudarte a ejecutar más rápido, cumplir regulaciones y mantener la operación segura con menor carga interna.*

### 5. Levanta la mano con alta dirección

Involucrar a los líderes es fundamental para obtener seguimiento, apoyo e impacto organizacional. Hazlo desde una lógica de negocio:

- ☐ ¿Por qué necesitamos esta inversión?
- ☐ ¿Qué beneficios trae y qué riesgos evita?
- ☐ ¿Cómo lo vamos a implementar y quién será responsable?

*No solicites presupuesto para tecnología: comunica impacto, continuidad, reputación y cumplimiento.*

### 6. Valida el plan de trabajo (con o sin tu socio estratégico)

Tu presupuesto debe aterrizar en un plan claro:

- [ ] Cronograma de actividades
- [ ] Resultados esperados por iniciativa y etapa
- [ ] Escalabilidad en la estrategia: ¿cómo evoluciona la estrategia en el largo plazo?
- [ ] Inversiones extra que podrían surgir: Antimalware (Sentinel One), Mobile Device Management (Jump Cloud), Pruebas de Penetración (Delta Protect), SIEM (SecOps), Data Loss Prevention (Nigthfall), ISO27001 (Delta Protect)
- [ ] Key players internos clave en cada etapa: responsables principales, líderes de áreas, etc.

*Un presupuesto sin plan es una lista de deseos; con plan, es una estrategia concreta.*

### 7. Ejecuta, revisa y comunica

Presupuestar no termina con la aprobación. Asegura el seguimiento:

- [ ] Da seguimiento al proyecto (implementaciones, actividades y entregables)
- [ ] Ajusta por necesidades nuevas o errores detectados
- [ ] Comunica avances y cambios de postura a toda la organización
- [ ] Ajusta procesos y reglas para proveedores y terceros

*Un presupuesto efectivo debe vivirse, no archivarse. Hazlo parte de la cultura empresarial.*

**¿Necesitas un socio estratégico? →**

# 06. Key Insights

## No hay una fórmula universal: el presupuesto debe ser a la medida

Cada organización tiene riesgos, madurez, contexto y objetivos distintos.

Intentar aplicar un "modelo estándar" de presupuesto puede llevar a **gastos innecesarios, herramientas innecesarias e impacto pasajero.**

*La ciberseguridad no se compra en paquetes genéricos: se diseña como un traje a medida.*

## La cultura organizacional es el paso 0

Antes de hablar de firewalls o herramientas, es indispensable construir una base cultural donde **la seguridad sea parte de la operación diaria**.

- Líderes comprometidos
- Equipos sensibilizados
- Procesos seguros por diseño

*Un equipo que entiende el porqué, ejecuta mejor el cómo.*

## Ciber Resiliencia

En el mundo actual, **ser atacado es casi inevitable**. La diferencia está en **cómo previenes, respondes y te recuperas**.

- ¿Qué medidas básicas tienes? Backups, MFA, Política de contraseñas, etc.
- ¿Tu equipo sabría qué hacer si mañana hay un incidente?
- ¿Cuál es tu proceso de recuperación?

*Invertir en resiliencia es invertir en continuidad, reputación y supervivencia.*

## Invertir estratégicamente hoy, para proteger el negocio mañana

La asignación estratégica de presupuesto a Ciberseguridad ayuda a:

- **Evitar pérdidas millonarias**
- **Proteger relaciones comerciales**
- **Asegurar cumplimiento normativo**
- **Escalar sin miedo**

*No se trata solo de proteger datos, sino de proteger el negocio completo.*

# Conclusiones

Definir un presupuesto de ciberseguridad no es simplemente asignar recursos, sino reconocer que la protección digital es un componente estratégico para la continuidad y el crecimiento del negocio. Cada organización enfrenta riesgos diferentes según su industria, tamaño y nivel de madurez, por lo que no existen fórmulas universales.

Un presupuesto bien planteado debe ser entendido como un **traje a la medida**: capaz de adaptarse a las necesidades específicas de la empresa, de priorizar lo esencial sin sobredimensionar gastos y de evolucionar conforme cambian las amenazas y los objetivos corporativos. La clave está en verlo no como un gasto adicional, sino como una inversión planificada que asegura resiliencia, confianza y sostenibilidad en el tiempo.

DELTA PROTECT®

Delta Protect es una empresa mexicana de ciberseguridad que protege a negocios en México y LATAM mediante servicios como pentesting, cumplimiento normativo, certificaciones, evaluaciones de riesgo y monitoreo SOC. Hemos apoyado a más de 300 empresas en 8 países —incluyendo Bitso, Liverpool y BlackRock— a fortalecer su seguridad y generar confianza. Nuestra misión es hacer la ciberseguridad simple, escalable y efectiva, construyendo un futuro digital más seguro para todos.

Comienza a proteger tu empresa hoy →

Delta Protect @delta.protect @DeltaProtect www.deltaprotect.com