



GUÍA DE CONTINUIDAD OPERATIVA

Ransomware y pérdida de datos: la guía de continuidad operativa para empresas colombianas

Checklist práctico para evaluar y blindar la infraestructura de su organización

EL PROBLEMA

El riesgo ya no es lejano: es cotidiano

En los últimos años, los ataques de ransomware y las fallas de infraestructura han dejado de ser un riesgo lejano para convertirse en una amenaza cotidiana para empresas y entidades públicas en Colombia y la región.

Un solo incidente puede detener la operación de una organización durante días —o incluso semanas— mientras se intenta recuperar la información. Las pérdidas no son solo económicas: también afectan la reputación, la confianza de los clientes y, en el caso de entidades públicas, la continuidad de servicios esenciales.

Los datos son contundentes: una proporción significativa de las empresas que sufren un ataque de ransomware nunca logra recuperar la totalidad de su información, y el tiempo promedio de inactividad tras un incidente se mide en días, no en horas.

La pregunta ya no es si su empresa sufrirá un incidente de seguridad o una falla crítica, sino si estará realmente preparada para recuperarse cuando ocurra.

Esta guía está diseñada para ayudarle a evaluar el nivel real de protección de su infraestructura y entender cómo el backup en la nube puede marcar la diferencia entre una interrupción menor y una crisis operativa.

EL PUNTO DE PARTIDA

Por qué el backup tradicional ya no es suficiente

Durante años, hacer una copia de seguridad significaba guardar los datos en un disco externo, un servidor secundario en la misma oficina, o una cinta que alguien debía cambiar manualmente. Este enfoque tenía sentido cuando las amenazas eran distintas — pero hoy presenta limitaciones serias:

Un solo punto de falla

Si el ransomware llega a la red local, con frecuencia también cifra o daña las copias de respaldo almacenadas en el mismo entorno.

Sin cifrado adecuado

Muchas copias tradicionales no cuentan con cifrado robusto en tránsito ni en reposo, dejando los datos expuestos.

Recuperación lenta y manual

Restaurar desde cintas o discos físicos puede tomar días, tiempo que la mayoría de las organizaciones no puede permitirse perder.

Falta de pruebas periódicas

Es común generar backups que nunca se verifican, hasta que llega el momento de necesitarlos — y fallan.

La continuidad operativa moderna exige un estándar distinto, definido por dos métricas clave:

RTO — Recovery Time Objective

Cuánto tiempo tarda su organización en volver a operar tras un incidente.

RPO — Recovery Point Objective

Cuánta información puede permitirse perder entre la última copia y el momento del incidente.

Si su organización no tiene claridad sobre estos dos números, es una señal de que su estrategia de backup necesita revisión.

CON ACRONIS CLOUD BACKUP

Qué es el backup en la nube

El backup en la nube consiste en replicar automáticamente la información crítica de su organización hacia un entorno externo, seguro y geográficamente independiente de su infraestructura local. A diferencia del backup tradicional, una solución como **Acronis Cloud Backup** ofrece:

Replicación automática y continua

Sin depender de que alguien ejecute el proceso manualmente.

Cifrado de extremo a extremo

Tanto en tránsito como en reposo, protegiendo los datos incluso si son interceptados.

Aislamiento ante ransomware

Mediante copias inmutables que no pueden ser cifradas ni eliminadas por un atacante que ya esté dentro de la red.

Recuperación ante desastres (Disaster Recovery)

Permite restaurar sistemas completos en la nube en caso de que la infraestructura local quede inutilizable.

Flujo simplificado del proceso

Servidor /
infraestructura local



Replicación cifrada y
automática



Almacenamiento en la
nube (aislado)



Recuperación rápida
ante incidente

Este modelo traslada la responsabilidad de la protección desde un proceso manual y vulnerable hacia una arquitectura diseñada específicamente para resistir los escenarios de falla más comunes hoy: ransomware, error humano, falla de hardware y desastres físicos.

LO QUE GANA SU ORGANIZACIÓN

Beneficios clave

1

Continuidad operativa garantizada

Su organización puede seguir funcionando incluso si la infraestructura local sufre un incidente grave, gracias a la posibilidad de recuperar sistemas completos desde la nube.

2

Protección real contra ransomware

El versionado y la inmutabilidad de las copias impiden que un atacante cifre o borre los backups, algo que sí ocurre con frecuencia en esquemas tradicionales.

3

Cumplimiento normativo

Contar con copias cifradas, verificables y con trazabilidad facilita el cumplimiento de exigencias regulatorias, particularmente para entidades públicas.

4

Reducción de costos operativos

Elimina la necesidad de mantener infraestructura física adicional, hardware de respaldo y procesos manuales de administración.

Recuperación en minutos, no en días. Ante un incidente, la diferencia entre restaurar en minutos u horas —en lugar de días— puede significar la diferencia entre una interrupción menor y una crisis operativa completa.

CHECKLIST

¿Su empresa está protegida?

Responda sí o no a cada pregunta:

- ☐ ¿Sus backups se prueban periódicamente, y no solo se generan?
- ☐ ¿Cuenta con copias almacenadas fuera de su red local, aisladas de un posible ataque de ransomware?
- ☐ ¿Sabe con precisión cuánto tiempo tardaría en recuperar sus sistemas críticos (RTO)?
- ☐ ¿Tiene claridad sobre cuánta información podría perder entre incidentes (RPO)?
- ☐ ¿Su proveedor de backup cifra los datos tanto en tránsito como en reposo?
- ☐ ¿Sus copias de seguridad son inmutables, es decir, no pueden ser modificadas ni eliminadas por un atacante?
- ☐ ¿Cuenta con un plan documentado de recuperación ante desastres?
- ☐ ¿Su equipo de TI recibe alertas automáticas si un proceso de backup falla?
- ☐ ¿Ha realizado un simulacro real de recuperación en el último año?
- ☐ ¿Su estrategia de backup cumple con los requisitos normativos aplicables a su sector?

Resultado: Si respondió "No" a dos o más preguntas, su organización tiene brechas reales en su estrategia de continuidad operativa que deberían atenderse cuanto antes.

EXPERIENCIA QUE RESPALDA ESTA GUÍA

27 años protegiendo infraestructura crítica

Durante más de 27 años, Avance Consultores IT ha diseñado e implementado soluciones de infraestructura tecnológica crítica para organizaciones que no pueden darse el lujo de fallar, incluyendo entidades como la **Policía Nacional** y el **Ministerio de Defensa Nacional**, brindando servicios de consultoría especializada e infraestructura de alta disponibilidad.

Esta experiencia en entornos donde la continuidad operativa es innegociable es la misma que aplicamos al diseñar estrategias de backup en la nube para empresas privadas y entidades públicas en Colombia.

27+

AÑOS DE TRAYECTORIA

250+

PROYECTOS EJECUTADOS

1.000+

CLIENTES ATENDIDOS

SOBRE AVANCE CONSULTORES IT

Avance Consultores IT es aliado tecnológico de empresas y entidades públicas en Colombia desde hace más de 27 años. Somos partner autorizado de Microsoft Office 365 y especialistas en:

Consultoría IT e infraestructura

Virtualización VMware / Hyper-V

Redes corporativas y seguridad

Licenciamiento Windows Server

Backup Acronis

Data Centers

Mantenimiento tecnológico

¿LISTO PARA EVALUAR SU INFRAESTRUCTURA?

Solicite su diagnóstico gratuito de infraestructura

Si su checklist arrojó más de una alerta, el siguiente paso es sencillo: una evaluación gratuita con nuestro equipo de expertos, quienes analizarán su infraestructura actual y le indicarán exactamente dónde están las brechas y cómo cerrarlas.

WHATSAPP / CELULAR

316 430 9801

PBX

601 516 6847

CORREO

Info@avaconit.com



Más de 27 años siendo el aliado tecnológico de empresas y
entidades públicas en Colombia.



PBX: 601 516 6847 · Celular/WhatsApp: 316 430 9801 · Info@avaconit.com
Bogotá, Colombia