DATA ERASURE · DATA GOVERNANCE · COMPLIANCE · PRIVACY

WHITEPAPER · 2025

SOBREVIVIR Y PROSPERAR EN LA ERA DE LA PRIVACIDAD

Gobernanza de Datos con Overty

Overty®

overtytech.com · Data Erasure & Governance

CONTENIDO

Gobernanza de Datos con Overty

$4.44M
COSTO PROMEDIO
de una brecha de datos IBM 2025

240+
DÍAS
tiempo de detección y contención

100%
CERTIFICADO
borrado auditado independientemente

01

Introducción

¿Por qué importa el borrado de datos?

Vivimos en un mundo donde la gestión del dato es estratégica. Las organizaciones generan, recopilan y procesan cantidades masivas de información: desde identificadores personales, registros financieros y comunicaciones electrónicas, hasta datos sensibles de clientes y empleados. Sin embargo, no toda esta información tiene un valor permanente para el negocio ni un propósito legal que justifique su conservación indefinida.

Cuando datos que ya no deberían existir continúan almacenados, no solo se desperdician recursos tecnológicos, sino que se incrementa el riesgo de exposición no deseada. Esta acumulación de información innecesaria hace que cada brecha o acceso no autorizado pueda tener un impacto más amplio y costoso para la organización.

El riesgo es cuantificable y creciente

El **IBM Cost of a Data Breach Report 2025** reporta que el costo promedio global de una brecha de datos es de **USD $4.44 millones** por incidente. Este costo incluye:

— Gastos de respuesta inmediata

— Investigaciones forenses

— Multas regulatorias

— Pérdida de ingresos y clientes

— Daño reputacional

> ■ **Dato clave**
>
> Los tiempos de detección y contención de brechas a menudo exceden los 240 días, multiplicando el daño total del incidente.
> Cuanto más dato tiene una empresa, mayor es su superficie de ataque.

Más allá de la seguridad: privacidad y confianza

Eliminar datos que ya no son necesarios es una **medida de respeto hacia la privacidad de las personas**. Una base de datos saturada de información obsoleta puede ser explotada para robo de identidad, fraude o phishing dirigido, e incrementa la probabilidad de exposición de datos personales sensibles.

Eliminar datos innecesarios **reduce la "huella de datos"** de la organización, habilitando una postura de privacidad más sólida, confiable y defendible ante reguladores.

Conclusión de sección: El borrado seguro de datos reduce en forma real y medible el riesgo de brechas costosas, optimiza la infraestructura y refuerza la confianza de clientes, socios y auditores.

02

Estado actual

Herramientas sin gobernanza

En muchas organizaciones existe una **contradicción crítica**: tienen licencias de software para borrar datos, pero **no tienen un enfoque estructurado de gestión del borrado** como parte de su gobernanza de datos. Este desfase entre tecnología y proceso tiene consecuencias importantes.

¿Qué está sucediendo realmente?

Mientras que las herramientas de borrado pueden eliminar información de forma individual, no resuelven por sí mismas los retos organizacionales:

- **No hay procesos formales documentados** que establezcan cómo y cuándo borrar cada tipo de dato.
- **No existen políticas de retención aprobadas** con reglas claras basadas en riesgos y regulaciones.
- **No hay integración con procesos clave** como backups, leasing de equipos o offboarding de personal.
- **No existe una matriz de retención** que asigne plazos según tipo de información y marco regulatorio.
- **No se captura trazabilidad centralizada** ni evidencia auditable que respalde decisiones de eliminación.

Consecuencias del gap estructural

El borrado ocurre de forma reactiva, sin criterios formales.
No existe evidencia documentada para auditorías o reguladores.
Se incumplen principios de minimización y calidad del dato.
El riesgo crece silenciosamente cada día.

03

Marco regulatorio

El imperativo de cumplimiento

El panorama regulatorio global exige no solo proteger los datos, sino también gestionar su ciclo de vida completo —incluyendo su eliminación oportuna y verificable. Las organizaciones sin procesos formales de borrado se exponen a sanciones crecientes.

GDPR (Europa)

Exige el "derecho al olvido" y la minimización del dato. Retener información sin propósito legítimo constituye incumplimiento del principio de limitación del almacenamiento.

ISO/IEC 27001

Requiere controles formales sobre el ciclo de vida del activo informático y la eliminación segura de medios y equipos. Control 8.10 del Anexo A.

PCI-DSS

Obliga a conservar datos de tarjetahabientes solo cuando sea estrictamente necesario y eliminarlos de forma segura y verificable. Requerimientos 3.1 y 3.2.

HIPAA (EE.UU.)

Establece requisitos específicos para la disposición de información de salud protegida, tanto en formato físico como digital.

LFPDPPP (México)

Contempla el derecho de cancelación y obliga a suprimir datos cuando se cumpla la finalidad para la que fueron recabados.

La diferencia crítica

No basta con cumplir — hay que DEMOSTRAR el cumplimiento.
Sin evidencia documentada de eliminación, no hay cumplimiento real.
Los reguladores exigen trazabilidad, no solo buenas intenciones.

04

Los riesgos reales

De no gobernar el ciclo de vida del dato

Cada archivo olvidado, cada respaldo histórico sin depuración, cada equipo reasignado sin control formal, es una posible fuente de exposición. No gobernar el borrado no es una omisión menor: **es un riesgo estructural**.

4.1 Privacidad vulnerada

■ **Aumenta la superficie de ataque**

Más datos almacenados significan más vectores potenciales de acceso. Los atacantes no distinguen entre datos "activos" y datos "olvidados".

■ **Incrementa la exposición en brechas**

Cuando ocurre un incidente, el impacto depende directamente del volumen y sensibilidad de la información comprometida. Retener datos sin propósito amplifica el daño.

■ **Puede generar sanciones regulatorias**

Las leyes de protección de datos obligan a conservar información únicamente el tiempo necesario. Mantener datos sin justificación puede interpretarse como incumplimiento.

4.2 Costos financieros reales

El costo promedio de una brecha alcanza **USD $4.44 millones**. Con deficiente gobernanza del dato, el impacto se amplifica por mayor volumen comprometido, alcance regulatorio adicional, complejidad forense y más notificaciones obligatorias.

■ Servicios forenses y legales

■ Pérdida de confianza de clientes

■ Cancelación de contratos

■ Aumento en primas de ciberseguro

■ Daño reputacional de largo plazo

> ■ **El riesgo silencioso**
>
> El riesgo más silencioso es NO ELIMINAR datos cuando corresponde.
> La acumulación indiscriminada de información no es fortaleza digital.
> Es vulnerabilidad acumulada — visible para los atacantes.

05

La solución Overty

Gobernanza, automatización y trazabilidad

La mayoría de las organizaciones ya tiene herramientas de borrado. Lo que no tienen es **gobernanza**. Overty propone un cambio de paradigma: del borrado reactivo al **borrado gobernado, automatizado y auditable**.

No se trata solo de eliminar datos. Se trata de convertir la eliminación en un proceso corporativo formal, alineado a regulación, riesgo y estrategia empresarial.

¿Qué hace diferente a Overty?

✔ Política corporativa de retención y eliminación

Diseño e implementación de lineamientos formales alineados a regulación y mejores prácticas internacionales.

✔ Matriz de retención por tipo de dato

Definición clara de qué se conserva, cuánto tiempo y bajo qué fundamento legal o regulatorio.

✔ Integración con procesos críticos de negocio

Backup, leasing, renovación tecnológica, migraciones y offboarding dejan de ser puntos ciegos.

✔ Trazabilidad centralizada y reportes auditables

Evidencia consolidada, verificable y lista para auditorías internas o regulatorias.

✔ Evidencia certificada de eliminación

Soporte documental alineado a NIST 800-88, DoD 5220.22-M, ISO 27001, PCI-DSS y GDPR.

> **La propuesta de valor**
>
> Overty no solo ejecuta el borrado.
> Lo convierte en un control corporativo defendible.
> Gobernanza estructurada + automatización + trazabilidad
> alineada a marcos regulatorios internacionales.

06

Cumplimiento regulatorio

Overty como habilitador de evidencia

La diferencia entre cumplir y demostrar cumplimiento es crítica. La falta de evidencia documentada puede generar observaciones, hallazgos o sanciones bajo los marcos regulatorios más exigentes.

ISO/IEC 27001

Exige controles formales sobre el ciclo de vida del activo. Overty genera evidencia alineada al Anexo A, Control 8.10.

PCI-DSS

Requiere eliminación segura y verificable de datos sensibles. Overty cumple los requerimientos 3.1 y 3.2.

CNBV y Banxico

Demandan gestión integral de riesgos tecnológicos y evidencia de implementación de controles.

GDPR / LFPDPPP

El borrado certificado de Overty soporta el derecho al olvido y el principio de minimización en ambos marcos.

Sin proceso, no hay control. Sin evidencia, no hay cumplimiento. Overty cierra el gap entre la herramienta técnica y el proceso corporativo, integrando gobernanza, automatización y trazabilidad en un solo marco operativo.

07

Conclusión

La privacidad como ventaja competitiva

El dato ya no es únicamente un activo tecnológico o financiero. Es un activo reputacional, regulatorio y estratégico. Las organizaciones son responsables de gestionar el ciclo de vida completo de su información, incluyendo su eliminación oportuna y verificable.

En un entorno donde las regulaciones son cada vez más estrictas, las brechas más frecuentes y costosas, y los clientes exigen mayor transparencia, la privacidad se convierte en un elemento de **confianza empresarial** —no solo de cumplimiento.

Las organizaciones que gobiernan el ciclo de vida del dato:

✔ Reducen su exposición a riesgos legales y financieros

✔ Disminuyen el impacto potencial de incidentes de seguridad

✔ Fortalecen su postura ante auditorías y reguladores

✔ Generan credibilidad frente a clientes e inversionistas

✔ Convierten la privacidad en ventaja competitiva sostenible

■ El resultado

Overty permite pasar de un borrado operativo e informal
a un modelo estructurado, automatizado y auditable,
alineado con marcos regulatorios y mejores prácticas internacionales.

En un mercado donde la confianza es un activo escaso,
la gobernanza del dato se convierte en ventaja competitiva.

Overty Corporation LLC · overtytech.com

Data Erasure · Data Governance · Compliance · Privacy