elastic

Aprovechando Elastic para potenciar el cumplimiento normativo de seguridad de datos

Resumen ejecutivo

A medida que el panorama de amenazas de ciberseguridad se vuelve cada vez más sofisticado (con ciberataques cada vez más frecuentes, dirigidos, sigilosos y técnicamente avanzados), la necesidad de una seguridad de los datos robusta y completa cobra mayor urgencia que nunca. Los requisitos legales y las posibles responsabilidades relacionadas con la ciberseguridad son cada vez más complejos y exigentes, lo que hace absolutamente necesario adoptar un enfoque de seguridad basado en el riesgo.

Para mantenerse al día con la lista cada vez mayor de requisitos regulatorios relacionados con la seguridad, evitar interrupciones comerciales potencialmente devastadoras y protegerse contra el riesgo de demandas costosas por violaciones de seguridad, las compañías deben adoptar un enfoque holístico y estratégico hacia la ciberseguridad. No hacerlo no solo expone a las empresas a serias consecuencias legales y financieras, sino también a daños operativos y de reputación irreparables.

Este informe técnico analiza cómo las organizaciones pueden utilizar Elastic para cumplir con sus obligaciones de seguridad y crear una defensa verdaderamente resistente contra las amenazas cibernéticas. La solución potente, flexible y escalable de Elastic ayuda a las empresas a satisfacer necesidades diversas y multifacéticas de cumplimiento normativo y ciberseguridad operativa, que incluyen las siguientes:

- Mayor visibilidad y capacidad de búsqueda de datos en las superficies de ataque
- Extracciones simplificadas de datos para solicitudes de cumplimiento normativo
- Detección y automatización optimizadas para mitigar amenazas
- Monitoreo y demostración de tu postura de seguridad
- Inteligencia de amenazas enriquecida

A continuación, proporcionamos una visión general de los conceptos fundamentales de seguridad que son comunes en todos los marcos de trabajo legales; revisamos las posibles consecuencias de no implementar estos conceptos con enfoque en los riesgos y la conformidad; e ilustramos cómo las organizaciones pueden usar la plataforma y las soluciones de Elastic para cumplir con las obligaciones de normativa y mitigar los riesgos de seguridad.

Ten en cuenta lo siguiente: *este documento técnico se proporciona solo con fines informativos y no pretende constituir asesoramiento legal. Consulta a un asesor legal para obtener asesoramiento legal.*

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Principios fundamentales de seguridad y obligaciones de cumplimiento relacionadas

El panorama moderno de cumplimiento de seguridad consiste en un mosaico de requisitos específicos de cada jurisdicción, industria y tipo de datos. Por lo tanto, las responsabilidades de las organizaciones varían según su ubicación, dónde operan, qué datos procesan y cómo, incluyendo la sensibilidad de esos datos y la naturaleza del negocio.

Por ejemplo, una institución financiera global podría estar sujeta simultáneamente a la Ley Gramm-Leach-Bliley (“GLBA”) federal de los EE. UU., el Reglamento de Ciberseguridad del Departamento de Servicios Financieros de Nueva York (“NYDFS2”), la Ley de Resiliencia de Operaciones Digitales de la UE (“DORA”) y la Directiva 2 de Seguridad de la Información y de las Redes de la UE (“Directiva NIS2”), entre otras leyes.

Por otro lado, una empresa minorista que cotiza en bolsa y tiene su sede en Estados Unidos podría estar sujeta a una serie de requisitos diferentes, como las normas de seguridad de datos PCI (“PCI-DSS”) para la seguridad de las tarjetas de pago, los requisitos de la ley Sarbanes-Oxley (“SOX”) para la seguridad de los sistemas de reporte financiero y las leyes estatales de notificación de infracciones de Estados Unidos. Sin olvidar, por supuesto, las leyes de privacidad y sus requisitos de seguridad de la información para la protección de la información personal.

Además de estos requisitos obligatorios, muchas empresas también mantienen certificaciones voluntarias de diversos marcos de trabajo de terceros, como ISO 27001, SOC 2, NIST CSF o UK Cyber Essentials.

A pesar de estas diferencias, los marcos de trabajo legales, regulatorios, autorreguladores y de la industria,así como las mejores prácticas generales de seguridad, convergen en gran medida en torno a un conjunto de principios esencialesde seguridad. A continuación, revisamos las partes clave de estos principios y proporcionamos ejemplos de cómo se ajustan con varios marcos de trabajo.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Inventario de datos, mapeo y clasificación

Las organizaciones no pueden desplegar controles de seguridad basados en el riesgo sin antes comprender qué datos tienen (un proceso conocido como inventario de datos), dónde se encuentran (data mapping) y la naturaleza sensible de esos datos (clasificación de datos).

Estos procesos también son fundamentales en caso de que se produzca una violación de datos, ya que permiten a las empresas saber mejor si los datos afectados ocasionarán obligaciones legales, reglamentarias o contractuales de notificación de la violación. Por estas razones, el inventario, el mapeo y la clasificación de datos son requisitos explícitos o condiciones previas necesarias para cumplir con varios marcos de trabajo. Por ejemplo:

- La *Regla de Salvaguardas de la FTC* (16 CFR artículo 314), que implementa requisitos para ciertas instituciones financieras sujetas a la GLBA, exige que las instituciones financieras alcanzadas identifiquen y evalúen la sensibilidad de la información de los clientes como parte de su proceso de evaluación de riesgos.
- La *Norma de Seguridad de la HIPAA* (45 CFR artículo 164.308) obliga de manera similar a las entidades alcanzadas a inventariar y proteger la información médica protegida electrónica (“ePHI”).
- Bajo el artículo 30 del Reglamento General de Protección de Datos de la UE (“GDPR”), las organizaciones deben mantener un registro de las actividades de procesamiento, lo que efectivamente requiere un inventario de datos y un mapeo para demostrar el cumplimiento.
- Las obligaciones de notificación de incumplimiento de cada estado de EE. UU. generalmente surgen solo si se ven comprometidos ciertos tipos de datos personales sensibles relacionados con los residentes de ese estado. En consecuencia, en un caso de filtración de datos, las empresas deben ser capaces de determinar qué categorías de datos se incluyen en un set de datos comprometido.
- Los marcos de trabajo como NIST SP 800-53 y los Controles de CIS enfatizan la clasificación de datos para garantizar que las protecciones estén alineadas con la sensibilidad de los datos. Al establecer un esquema claro de inventario y clasificación, las empresas pueden implementar controles de acceso con mayor confianza, monitorizar los flujos de datos confidenciales, cumplir con las obligaciones reglamentarias y reducir el riesgo de divulgación no autorizada.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Controles de acceso basados en roles

Los controles de acceso basados en roles ("RBAC") son medidas diseñadas para garantizar que las personas tengan acceso solo a los sistemas y datos que necesitan para cumplir con sus responsabilidades (un concepto también conocido como "privilegio mínimo"). La aplicación sistemática de los RBAC reduce el riesgo de acceso sin autorización por parte de personas malintencionadas y puede ayudar a limitar el alcance de una intrusión. Muchos marcos de trabajo legales e industriales requieren explícitamente o recomiendan encarecidamente el RBAC:

- Bajo el RGPD de la UE, solo las personas con autorización correspondiente con necesidad de conocer pueden acceder a los datos personales. Incluso, la regulación define el acceso sin autorización como un caso de filtración de datos.
- Los estándares de Massachusetts para la protección de la información personal, 201 CMR 17.04, requieren que las empresas que hacen negocios en Massachusetts implementen medidas de control de acceso seguro que restrinjan el acceso a registros y archivos que contienen información personal sensible a quienes necesitan dicha información para realizar sus funciones laborales.
- La Regla de Seguridad de HIPAA exige que el acceso a ePHI se limite a quienes tengan una necesidad legítima de saber.
- El artículo 9(4) de la DORA de la UE requiere que las instituciones financieras alcanzadas implementen políticas que limiten el acceso físico o lógico a los activos únicamente a lo que sea necesario para funciones y actividades legítimas y aprobadas.
- Los estándares de la industria como NIST SP 800-53, ISO/IEC 27001 y CIS Controls (p. ej., CIS Control 6) también enfatizan RBAC como una práctica fundamental de administración de acceso.

 | © 2026 Elasticsearch B.V. Todos los derechos reservados.

Logging y monitoreo

Los logs de eventos de seguridad son uno de los recursos más importantes con los que cuentan las empresas para detectar incidentes de seguridad. Los logs que reflejan información como fechas y horas de acceso, acciones realizadas y el usuario que realizó esas acciones son esenciales para verificar si el acceso al sistema fue autorizado e investigar posibles actividades sin autorización. Monitorear los logs en tiempo real o casi en tiempo real también es clave para detectar y abordar las amenazas de manera oportuna.

Sin embargo, la gestión de logs puede ser un desafío para las organizaciones con sistemas complejos y diversos que pueden generar grandes volúmenes de logs todos los días. Estas organizaciones deben confiar en soluciones técnicas para agregar logs de manera efectiva y monitorearlos para detectar actividad anómala. Los marcos de trabajo legales e industriales enfatizan la importancia del logging y el monitoreo:

- El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS) exige a todas las compañías que almacenan, transmiten o procesan datos de tarjetas de pago registrar y monitorizar todos los accesos a los componentes del sistema y a los datos del titular de las tarjetas.
- La Norma de Seguridad de HIPAA exige que los controles de auditoría registren y examinen la actividad en sistemas que contienen ePHI.
- La sección 404 del SOX requiere que la gerencia y los auditores evalúen e informen sobre la eficacia de los controles internos de las empresas públicas en los reportes financieros. Dichos auditores evalúan esos controles en comparación con marcos de trabajo como COBIT, que requieren logs de auditoría de la actividad del usuario, acceso a los sistemas financieros y cambios en los datos financieros.
- El componente “Detectar” del CSF NIST especifica que las empresas deben registrar eventos de seguridad y mantener un monitoreo de seguridad continuo, lo cual también es indispensable para el informe oportuno de incidentes notificables bajo, por ejemplo, el artículo 32 del GDPR de la UE, el artículo 23 del NIS2 de la UE, o el artículo 19 de DORA de la UE.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Detección de intrusiones y respuesta

Es un hecho desafortunado que en el panorama de amenazas actual, cada organización es un potencial objetivo para ataques cibernéticos. Las organizaciones deben mantener sistemas de detección de intrusiones y procesos para responder a incidentes de seguridad en el caso inevitable de que se produzca un intento de intrusión. Estos sistemas son fundamentales para que las empresas puedan identificar rápidamente un ataque y responder a él antes de que se convierta en un incidente grave. Sin embargo, los sistemas de detección de intrusiones y los procesos de respuesta a incidentes rara vez son eficaces desde el primer momento; más bien, las empresas deben establecer una base de referencia de actividad y adaptar los criterios de alertas a los atributos únicos de la empresa. Esta personalización aumenta la precisión de las alertas y ayuda a garantizar que los incidentes se clasifiquen y se aborden adecuadamente en función de su gravedad. La detección de intrusiones y la respuesta a ellas es fundamental en muchos marcos de trabajo legales e industriales:

- Las leyes federales, estatales e internacionales de notificación de violaciones de datos exigen que las violaciones de datos se notifiquen en plazos específicos. Si bien suelen pensar que el GDPR impone el plazo más corto para el informe (dentro de las 72 horas posteriores a la determinación de que se ha producido una violación de datos reportable), vale la pena señalar que DORA requiere que los incidentes principales relacionados con la tecnología de la información y la comunicación (“TIC”) se informen dentro de las cuatro horas posteriores al descubrimiento.

- El artículo 500.16 del Reglamento de Ciberseguridad del NYDFS requiere que las entidades reguladas tengan planes de respuesta a incidentes para responder rápidamente y recuperarse de los incidentes de ciberseguridad.

- DORA también exige que las instituciones financieras reguladas desarrollen planes detallados de respuesta a incidentes.

- El CSF del NIST especifica que las compañías mantengan controles detallados de “Detectar” y “Responder” para detectar y responder a incidentes de seguridad.

 | © 2026 Elasticsearch B.V. Todos los derechos reservados.

El costo del incumplimiento

No implementar controles de seguridad efectivos y compatibles puede exponer a las empresas, su liderazgo y sus juntas directivas a riesgos legales, financieros y de reputación serios. Desde un punto de vista práctico, las organizaciones con herramientas o procesos de monitorización ineficaces corren el riesgo de acceso sin autorización prolongado, lo que puede permitir a un atacante realizar un reconocimiento sobre una compañía e imitar más fielmente la actividad autorizada, todo ello mientras filtra datos o prepara el terreno para un ataque de ransomware. El logging incompleto también puede hacer que sea imposible determinar si se autorizó una actividad sospechosa o inesperada, lo que puede llevar a una notificación excesiva e insuficiente.

En caso de una brecha de datos o incidente de ciberseguridad, un mapeo e inventario insuficientes de datos puede dificultar la identificación de datos afectados. Esto puede provocar retrasos en la notificación a las partes afectadas y a los reguladores. Estos retrasos, a su vez, aumentan los posibles daños sufridos por las víctimas, violan los plazos regulatorios de informe y agravan la carga inmediata de la recuperación y el resarcimiento con reclamos adicionales por daños, sanciones regulatorias y costos adicionales de aplicación y litigios. Para los proveedores de empresa a empresa, también puede dificultar la identificación de qué clientes empresariales se vieron afectados por un incidente.

El incumplimiento de los requisitos de seguridad afirmativa, como aquellos impuestos por las leyes de privacidad para proteger la información personal, puede conllevar sanciones considerables, multas y otras responsabilidades legales. Todas las empresas también enfrentan el riesgo de negligencia, incumplimiento de contrato u otras demandas judiciales (a menudo en acciones colectivas) de demandantes cuya información se filtró en un incidente. En particular, la Ley de Privacidad del Consumidor de California (CCPA) establece un derecho privado de acción para los demandantes cuyos datos confidenciales se filtraron como resultado de que una compañía no mantuviera medidas de seguridad razonables. Las sanciones y los daños contemplados en regulaciones como HIPAA, CCPA o el RGPD de la UE pueden alcanzar rápidamente los siete dígitos.

Más allá de las sanciones directas por incumplimiento, el daño a la reputación causado por una seguridad deficiente también puede ser grave. Las compañías que sufren una violación de seguridad o no cumplen con las normas de seguridad pueden perder la confianza de los clientes, enfrentar una reacción negativa del público, experimentar una interrupción comercial significativa y sufrir impactos a largo plazo en el valor de su marca. Las compañías que cotizan en bolsa también corren el riesgo de que el precio de sus acciones se vea afectado a raíz de fallos de seguridad ampliamente publicitados. Los riesgos incluyen la pérdida de clientes y posibles demandas de compensación por no proteger adecuadamente los datos de los clientes, lo que lleva a la pérdida de negocios e ingresos. A la luz de estas importantes consecuencias, las compañías deberían tomar la seguridad en serio invirtiendo adecuadamente en obligaciones de cumplimiento normativo y mitigando los riesgos de seguridad.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Aprovecha Elastic para el cumplimiento normativo

La plataforma Elasticsearch es la base para las dos soluciones preparadas para el uso de Elastic: Elastic Observability y Elastic Security. Las organizaciones pueden utilizar la plataforma abierta y flexible de Elastic para cumplir con sus obligaciones de cumplimiento normativo y abordar los riesgos principales de ciberseguridad en distintos canales. Lo más importante es que las soluciones de Elastic son inherentemente ágiles y escalables; pueden desplegar y recopilar datos de una amplia variedad de sistemas y plataformas, y sus capacidades de búsqueda pueden aprovecharse para innumerables casos de uso. A continuación se presentan solo algunos ejemplos de cómo Elastic puede utilizarse para respaldar los principios fundamentales de un programa de seguridad:

Mapeo y clasificación de datos

Elastic puede respaldar las medidas de mapeo de datos indexando datos estructurados y no estructurados entre los entornos, y proporcionando a las organizaciones una visibilidad centralizada sobre los tipos y las ubicaciones de sus datos. Mediante el uso de etiquetas personalizadas, metadato y machine learning, Elastic puede ayudar a identificar patrones en los datos (por ejemplo, datos personales, registros financieros, registros del sistema), lo que facilita la clasificación de los datos en función de su sensibilidad o de las obligaciones normativas. Aunque Elastic no es un motor dedicado a la clasificación de datos, sus poderosas capacidades de búsqueda y análisis pueden integrarse en programas más amplios de gobernanza de datos para ayudar a rastrear e inventariar datos en sistemas en la nube y locales.

Control de acceso basado en roles (RBAC)

Aunque Elastic no es una herramienta RBAC, la plataforma puede realizar la ingesta de logs de todos los sistemas de una organización para ayudar a identificar deficiencias en la gestión de permisos. Las organizaciones pueden analizar los patrones de acceso para identificar los sistemas a los que los grupos de usuarios pueden o no necesitar acceder y utilizar esa información para asignar privilegios de acceso. Elastic también ayuda a nuestros clientes a ingestar políticas de acceso de grupo de varios sistemas, permitiendo a las compañías generar informes a partir de esos datos para demostrar la aplicación de los derechos de acceso en auditorías o investigaciones de cumplimiento normativo. Además, Elastic incluye características RBAC integradas en sus interfaces Elastic Security y Kibana. Los administradores pueden definir roles que limitan el acceso de usuario a índices, dashboards o acciones específicas (como ver o editar), con el fin de aplicar el principio de acceso de privilegio mínimo.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

Logging y monitoreo

Una de las fortalezas principales de Elastic, y uno de los casos de uso más comunes, es la agregación, el almacenamiento y el análisis de logs a escala. Usando Elastic Agent, las empresas pueden realizar la ingesta de logs desde endpoints, servidores, servicios cloud y aplicaciones. Estos logs se indexan en Elasticsearch, permitiendo el análisis y la visualización en tiempo real en Kibana. Elastic admite la retención de logs a largo plazo, alertas y detección de anomalías, lo que lo convierte en una solución ideal para la agregación de logs y el monitoreo de seguridad, así como en una herramienta efectiva para el reporte de cumplimiento. La suite de observabilidad también proporciona monitoreo de rendimiento de aplicaciones (APM), métricas y monitoreo del tiempo de actividad para una visibilidad holística de la infraestructura.

Muchas regulaciones, como la M-21-31 para las agencias del gobierno federal de los Estados Unidos, requieren que las organizaciones almacenen logs durante un período de tiempo determinado. La estructura de organización de datos en niveles de Elastic permite que los datos se almacenen de manera rentable en función de la frecuencia y rapidez con la que se deben usar y acceder a ellos. El modo de índice logsdb de Elasticsearch **reduce la huella de almacenamiento de losdatos de log hasta en un 65 %**, lo que aumenta la visibilidad y el cumplimiento mientras que mantiene todos los datos inmediatamente accesibles para su análisis.

Por citar solo un ejemplo, la Universidad de York migra su sistema de SIEM a Elastic Security para optimizar las capacidades de ciberseguridad, optimizar la eficiencia operativa y reducir costos. Mediante el despliegue de aproximadamente 9000 Elastic Agents en servidores, computadoras de escritorio y portátiles, y la recopilación de logs de toda la infraestructura de nube híbrida de la universidad, que incluye Google Cloud, AWS, Azure y servidores local, la universidad ingesta 500 gigabytes de datos al día, con 35 terabytes de logs en almacenamiento. También se conecta con herramientas de seguridad como los firewalls de Palo Alto Networks, Cloudflare y Duo, lo que garantiza una monitorización integral en diversas plataformas. Esta configuración permite búsquedas rápidas en grandes cantidades de datos, reduciendo los tiempos de consulta de horas a segundos.

Detección de intrusiones y respuesta

Elastic Security incluye capacidades de detección y respuesta en los endpoints (EDR) e integra fuentes de inteligencia sobre amenazas para facilitar la detección de intrusiones. Permite a los equipos de seguridad monitorizar amenazas conocidas y desconocidas empleando análisis de comportamiento, mapeo de ataques y reglas de detección personalizadas. Gracias al logging centralizado, los analistas pueden correlacionar rápidamente eventos entre sistemas, investigar alertas en contexto y orquestar flujos de trabajo de respuesta. Elastic también admite respuestas automatizadas mediante integraciones con plataformas de orquestación, automatización y respuesta de seguridad (SOAR) de terceros, lo que la convierte en una herramienta poderosa para mejorar la preparación para la respuesta a incidentes y la búsqueda de amenazas. Estas capacidades avanzadas reducen la probabilidad de una brecha y aceleran el tiempo de respuesta en caso de una intrusión exitosa, lo que a su vez mitiga las posibles responsabilidades legales asociadas a un incidente.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.

AHEAD, un proveedor líder de transformación y plataforma digital, mejoró en gran medida sus capacidades de detección y respuesta de intrusiones al integrar Elastic Security en sus servicios de seguridad administrados. AHEAD ahora hace la ingesta de datos de seguridad del cliente en Elastic, que se ejecuta en Elastic Cloud, donde los datos se enriquecen, agregan y conectan a fuentes de inteligencia de amenazas. Elastic también es la fuente de datos para el sistema SOAR de la organización. Los analistas de seguridad de AHEAD también pueden aprovechar las alarmas impulsadas por IA que resaltan la información relevante dentro de los eventos de seguridad, reduciendo el tiempo necesario para examinar manualmente grandes cantidades de datos y ayudando a reducir la carga de falsos positivos.

Conclusión

A medida que el panorama de amenazas de ciberseguridad sigue planteando desafíos sofisticados para las organizaciones, cumplir con los crecientes requisitos regulatorios relacionados con la seguridad y la privacidad de datos y reducir riesgos también se vuelve más complejo. El no hacerlo no solo expone a las empresas a consecuencias legales y financieras serias, sino también a daños operativos y de reputación. Elastic puede ayudar a los CIOs y CISOs a mejorar el cumplimiento de sus organizaciones con estos diversos requisitos legales, especialmente en áreas como mapeo y clasificación de datos, RBAC, logging y monitorización, y detección y respuesta a intrusiones.

 © 2026 Elasticsearch B.V. Todos los derechos reservados.