UNIPAGO | UNISHIELD BY UNIPAGO

94 *días.*

RECONSTRUCCIÓN DE UN INCIDENTE

Nadie hizo nada mal. La parte *difícil de explicar.*

La reconstrucción de una intrusión que empezó con una decisión correcta tomada en 2021 y terminó noventa y cuatro días después, en una llamada que no hizo nadie de seguridad.

CASO FICTICIO · EJERCICIO DE APRENDIZAJE

VOL. 02 · OCTUBRE 2026

TLP:CLEAR

ANEXO OPERATIVO

Decir qué hay que hacer es fácil.
Por eso todo el mundo lo hace.

«Tenga visibilidad de sus activos» lleva dos décadas siendo el consejo correcto. Y si repetirlo funcionara, ya habría funcionado.

El problema no es el *qué*. Lo que falta siempre es la línea siguiente: en qué pantalla, con qué consulta, cuánto tarda, y qué hacer con lo que aparezca.

Esa línea casi nunca se escribe porque es específica, envejece, y exige haberlo hecho de verdad y no solo haberlo recomendado.

Por eso en UNISHIELD escribimos esa línea.

Guía de Ejecución. Cuatro inventarios, del II al V.

II ¿Qué exponemos?
Subdominios olvidados y recursos cloud sin declarar.

III ¿Quién tiene llaves?
Cuentas sin dueño y llaves que nunca se usaron.

IV ¿Quién nos habla?
Quién consume sus APIs y si entregan datos ajenos.

V ¿Qué consumimos?
Herramientas que entraron sin pasar por TI.

DESCARGAR LA GUÍA →

https://www.unishield.com.do/recurso/guia-de-ejecucion/

ANTES DE EMPEZAR

Este caso *no ocurrió*.

Meridiano Enterprise no existe. Ninguna empresa real nos ha reportado nada parecido, y este boletín no describe una brecha ocurrida en ninguna organización real.

Lo que sí es real es cada pieza. Todas las técnicas, vulnerabilidades y cifras que aparecen aquí provienen de incidentes documentados públicamente, con su fuente indicada. Lo que hicimos fue ensamblarlas en una secuencia plausible para una institución como la suya.

Doce controles sueltos se olvidan, ***pero una historia completa no***.

CÓMO LEER ESTE NÚMERO

El caso avanza en **seis actos**. Cada uno se lee de corrido sobre fondo oscuro y cierra con una banda clara: las cifras publicadas que sostienen lo que acaba de ocurrir en la historia.

El procedimiento vive aparte, en la **Guía de Ejecución**: al pie de cada acto está la remisión a su sección, y todo procedimiento de esta guía se ejecuta con herramientas gratuitas o con plan gratuito. Cierra con una lectura para el CISO y las fuentes de cada cifra.

94
DÍAS HASTA LA DETECCIÓN

60
DÍAS QUE GUARDABA EL REGISTRO DE ACCESOS

40
DÍAS SIN EVIDENCIA AL ABRIR LOS LOGS

APERTURA

Día 94

La llamada entró un martes por la mañana, y no la hizo nadie de seguridad. Fue una analista de conciliación de otra empresa. Estaba cuadrando consultas de autorizaciones del trimestre y le sobraban registros. No muchos. Los suficientes para que el número no cerrara y para que decidiera preguntar antes de ajustar la diferencia.

Siete días después de la llamada, alguien de Meridiano abrió los logs del API gateway para reconstruir qué había pasado y encontró el problema real del caso: la retención estaba configurada en sesenta días. De los treinta factores de costo que analiza IBM en su informe de 2026, el compromiso a través de un socio de negocio o de la cadena de suministro es el que más encarece una brecha: suma **227,250 dólares** por encima del promedio global. Es además el segundo vector de acceso inicial más común, y empata como el de ciclo más largo: 258 días para identificarlo y contenerlo, frente a los 247 de promedio general.

> *Los primeros cuarenta días de la intrusión no existían.*

No se habían borrado por sabotaje ni por descuido. Se habían borrado porque así estaba configurado, porque el almacenamiento cuesta y porque sesenta días le había parecido razonable a alguien, en algún momento, y nadie lo volvió a mirar.

Esta es la historia de lo que ocurrió antes de esa llamada. Empieza cinco años atrás, y empieza bien.



ACTO I

El portal que *funcionó*

> **Recordatorio.** Meridiano Enterprise es una empresa ficticia. El caso no ocurrió; cada técnica y cada cifra que lo componen sí están documentadas.

En 2021, Meridiano puso en línea un portal para que sus clientes consultaran autorizaciones. Lo llamaron portal-auth.meridiano.com.do. Resolvió un problema real: eliminó llamadas telefónicas, redujo reclamos y los clientes lo adoptaron rápido. Dos años después el equipo levantó la v2, migró a los clientes en tandas y en octubre de 2023 dio la migración por cerrada. El acta decía «migración completada». Y era verdad.

La v1 siguió corriendo.

No fue negligencia. El ingeniero que firmó ese cierre ya tenía otros dos proyectos encima, y en el acta la palabra *completada* significaba lo que significa en todas partes: que el último usuario se había movido. Apagar el servidor anterior era una tarea de otra semana, de otro sprint, de una lista que nunca se vació.

Así que la v1 quedó ahí. Sin monitoreo, porque nadie monitorea lo que ya no se usa. Sin parches, porque no estaba en la lista de sistemas a parchar. Sin dueño, porque oficialmente ya no existía.

Tres años después seguía respondiendo peticiones.

LO QUE DICEN LOS DATOS AKAMAI

Akamai midió que **solo el 23% tiene inventario completo y sabe qué APIs exponen datos sensibles, frente al 40% de 2022**: la visibilidad cae mientras la superficie crece. Una API dada de baja pero todavía encendida es la peor de ese conjunto. Nadie la vigila, y arrastra fallas sin corregir porque, en los papeles, ya no está.

En la Guía de Ejecución · Cómo consultar los registros de transparencia de certificados y contrastar el resultado contra su inventario documentado. → **Sección II**



ACTO II

Nadie eligió a *Meridiano*

En algún momento de mayo, un proceso automatizado encontró portal-auth-v1.

Conviene detenerse en cómo. No hubo una decisión de atacar a Meridiano. Nadie estudió a la institución, nadie evaluó qué datos tenía, nadie calculó cuánto podría pagar. Un agente enumeró rangos de Internet, identificó servicios expuestos, cruzó versiones contra vulnerabilidades conocidas y probó las que encajaban.

La v1 corría un componente con una falla publicada dieciocho meses antes. El parche existía desde entonces.

Nunca se aplicó, porque el sistema no estaba en la lista de sistemas a parchar.

18
MESES QUE EL PARCHE LLEVABA DISPONIBLE

0
DECISIONES HUMANAS DE ATACAR A MERIDIANO

LO QUE DICEN LOS DATOS UNIT 42 · WALLARM

El **30 de julio de 2026**, Unit 42 documentó una campaña ofensiva orquestada con asistencia de IA: el actor **intentó explotar más de cuatrocientos sesenta objetivos combinando operación autónoma y manual**. En operaciones manuales paralelas, Unit 42 confirmó exfiltración en tres organizaciones vía NetScaler y ejecución de comandos en once instancias de Marimo. Las fallas eran de 2026: lo que decidió el resultado fue la velocidad, no la sofisticación.

Hoy no hace falta que alguien lo elija como objetivo: basta con que tenga algo encendido y olvidado. Y casi siempre es una API, la puerta por la que un sistema le pide datos a otro. **106 de las 245 incorporaciones al catálogo KEV de CISA durante 2025 fueron relacionadas con APIs**, la mayor superficie explotada del conjunto (Wallarm).

En la Guía de Ejecución · Cómo ubicar su ASN, verse desde fuera con Shodan y Censys, y activar los reportes gratuitos permanentes de Shadowserver. → **Sección II**



ACTO III

Nadie estaba seguro de *qué se rompería*

Dentro de la v1, en un archivo de configuración, había una llave de API en texto plano. No era del portal: era la de la clínica que en 2021 sirvió de piloto, copiada ahí para las pruebas y nunca retirada. La clínica seguía usando esa misma llave en su propio sistema, en producción, cada día.

Alguien la mencionó, en su momento. La conversación duró poco: nadie sabía con certeza qué dependía todavía de esa credencial, revocarla podía romper algo que nadie tenía mapeado, y el portal v1, insistía el argumento, ya no existía. Se dejó para después.

Todos hemos estado en esa reunión.

La llave seguía siendo válida en producción cinco años más tarde.

LO QUE DICEN LOS DATOS GITGUARDIAN · PALO ALTO · ENTRO

Al reevaluar el conjunto en enero de 2026, **el 64% de los secretos confirmados como válidos en 2022 seguía siendo válido**. Cuatro años sin revocar: borrar el archivo donde estaba no desactiva la llave. Durante 2025 se detectaron **28.65 millones de secretos embebidos nuevos** en commits públicos de GitHub, un 34% más que el año anterior, y los **repositorios internos tienen seis veces más probabilidad** de contenerlos que los públicos.

109:1	97%	62%
Credenciales de máquina por cada credencial humana. De cada 109, 79 corresponden a agentes de IA. Hace un año la razón era 82:1.	De las identidades no humanas tiene más permisos de los que su función exige (Entro).	De las identidades no humanas en AWS no tuvo actividad en los últimos 90 días (Entro).

En la Guía de Ejecución · Cómo levantar el inventario de llaves activas, cuentas de servicio y secretos en repositorios, y en qué orden priorizar la rotación. → **Sección III**



ACTO IV

IV El API hizo exactamente *lo que le pidieron*

Con la llave válida, el acceso pasó al API de producción. La consulta de autorizaciones recibe un número de autorización y devuelve su estado, la organización que la solicitó, el detalle de lo autorizado y los datos PII del titular. Verifica que la llave sea válida, y nada más.

No verifica a cuál organización pertenece el registro consultado.

Durante ocho semanas, alguien enumeró identificadores. Sin prisa: unos miles por día, dentro del volumen habitual de la integración, en horario laboral. No se disparó una sola alerta, y no fue casualidad: la detección vigilaba credenciales fallidas y picos de tráfico, y no hubo ni lo uno ni lo otro. Cada consulta llegaba autenticada y recibía la respuesta normal del sistema: 200 OK, aquí están los datos.

Solo que entregó datos que no debía entregar, a quien no debía entregarlos.

DIAGRAMA 1 · LA CADENA DEL INCIDENTE · ACTOS I A IV



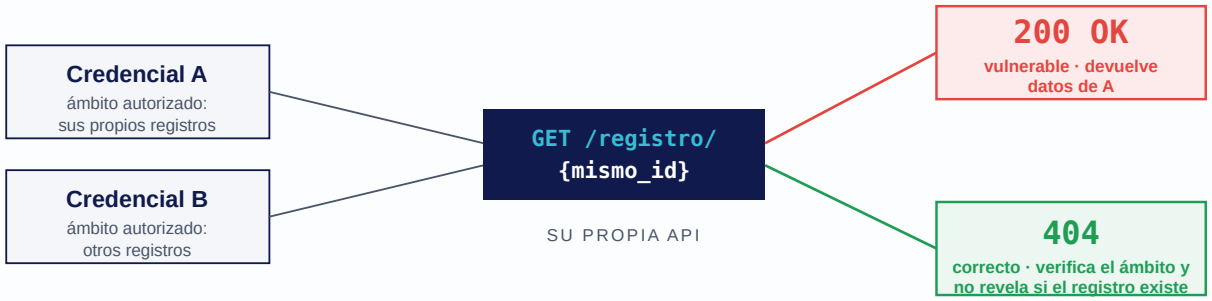
LO QUE DICEN LOS DATOS

Esto se llama **BOLA** (*Broken Object Level Authorization*), o autorización rota a nivel de registro, uno de los principales riesgos del OWASP API Security Top 10.

Los escáneres tradicionales rara vez lo detectan, porque la consulta es válida, el usuario está autenticado y la respuesta es legítima. Lo único anómalo es el dato que salió.

Además, escala rápido: una sola falla puede extraer miles de registros en minutos. No expone un expediente, **expone el conjunto completo**. En plataformas compartidas, la pregunta no es si su sistema verifica al usuario, sino si **verifica la empresa**. Esa validación más profunda requiere credenciales de dos entidades y un acuerdo escrito entre ambas. Empiece por lo que puede hacer por su cuenta.

DIAGRAMA 2 · LA PRUEBA DE AUTORIZACIÓN UN MISMO IDENTIFICADOR, DOS CREDENCIALES CON ACCESOS DISTINTOS



Ambas credenciales están autenticadas y ambas peticiones son válidas. La diferencia está en el ámbito: los registros que A puede ver no son los que B puede ver. Si B recibe datos en lugar de una negativa, su API verifica quién pregunta pero no si esa credencial tenía derecho a ese registro. Y no se disparará ninguna alerta, porque cada petición es legítima. La respuesta correcta es una negativa, y mejor un 404 que un 403: el 403 confirma que el registro existe, y eso basta para enumerar identificadores válidos aunque no se llegue a leerlos.

SOLO SOBRE SISTEMAS AUTORIZADOS

Esta prueba se ejecuta únicamente sobre sistemas que su institución posee o controla, con autorización de su responsable de tecnología. Ejecutarla contra sistemas de terceros constituye acceso no autorizado, tipificado en la **Ley 53-07**.

Según Akamai, **el 87% de las organizaciones sufrió un incidente de API en el último año**, con un costo promedio de 700 mil dólares por incidente. Para un equipo técnico el número útil es otro: cuántas de sus consultas se han probado con credenciales de dos usuarios distintos.

En la Guía de Ejecución · Cómo inventariar consumidores por credencial y cómo probar autorización rota sobre sus propios sistemas. **→ Sección IV**



ACTO V

Dos clics que *nadie revisó*

Semanas después, y sin ninguna conexión con lo anterior, pasaron dos cosas en Meridiano. Un analista de operaciones instaló una extensión de navegador que resumía documentos: pedía permiso para leer el contenido de todas las páginas visitadas, y él lo concedió, porque para eso servía.

Y una asistente de dirección conectó un asistente de productividad a su correo. Un clic en *Aceptar*. La aplicación pidió acceso de lectura al buzón y lo obtuvo.

Cuando por fin se convocó la reunión de emergencia para discutir la anomalía, un transcriptor capturó la conversación completa. No apareció en la lista de participantes.

Ninguno de los dos clics disparó una alerta de seguridad.

LO QUE DICEN LOS DATOS OX SECURITY · INVICTUS IR · LAYERX

Una extensión opera **dentro de la sesión confiable del usuario**: ningún proceso anómalo, solo datos saliendo por una conexión que parece normal. OX Security halló dos extensiones que suplantaban una herramienta legítima: más de **900,000 instalaciones** sacando conversaciones de IA de usuarios.

Cuando un usuario autoriza una aplicación externa a entrar en su correo, le entrega **una llave que quizás no caduque**: sigue abriendo aunque él cambie su contraseña o le reinicien el segundo factor. Con tokens OAuth robados a una integración de terceros, **UNC6395** alcanzó más de 700 organizaciones. Y un dato incómodo: el **68% de los inicios de sesión corporativos no pasa por el sistema de identidad de la empresa** (LayerX).

En la Guía de Ejecución · Cómo descubrir la adopción real en el tráfico saliente del firewall, revisar consentimientos OAuth, aplicar las cuatro estrategias de control de extensiones y auditar la tarjeta corporativa. → **Sección V**



ACTO VI

VI Noventa y cuatro días *fue suerte*

Volvamos a la llamada del martes. Meridiano no detectó nada. Lo supo porque alguien más, en otra empresa, decidió preguntar en lugar de ajustar una diferencia menor en una conciliación. Si esa analista hubiera cerrado el número, que es lo que se hace mil veces al año con diferencias pequeñas, el acceso habría seguido abierto.

Noventa y cuatro días no es un mal resultado. Es un resultado afortunado.

La media global multisectorial para identificar y contener una brecha es de 247 días, y este año subió un 2.5%.

LO QUE DICEN LOS DATOS IBM · PONEMON

El *Cost of a Data Breach Report 2026* de IBM deja dos datos que describen este caso mejor que cualquier otro. El primero es cuánto se tarda en saber. El segundo es quién lo dice: **una parte sustancial de las brechas no las detecta la organización afectada**, sino un tercero que avisa. Meridiano se enteró exactamente así.

247
Días de media global multisectorial para detectar y contener una brecha.

$4.99 M
Costo promedio global de una brecha, récord de la serie.

> Si un adversario llevara tres meses dentro de mi entorno, **¿qué evidencia tendría hoy para demostrarlo o descartarlo?** Si guarda menos registro del tiempo que un intruso suele pasar dentro, ya no se trata de detectar. Se trata de excavar.
>
> Nuestra recomendación, calibrada por riesgo y no como mínimo universal: **180 días en línea y doce meses en archivo** para gateway, identidad, DNS y firewall. El número exacto depende de su regulación, la criticidad del dato y su apetito de riesgo. Una alerta por volumen de registros distintos consultados podría haberlo detectado en días, no el día 94. La retención es lo que después permite reconstruirlo.

Meridiano Enterprise no cayó frente a un adversario sofisticado. Tres decisiones abrieron la puerta, una borró la evidencia y una dejó abierta la siguiente.

Dar por cerrada una migración cuando el último usuario se movió.

No revocar una credencial por temor a romper algo que nadie tenía mapeado.

Construir un API que verifica autenticación, igual que todas las demás.

Retener logs sesenta días, porque el almacenamiento cuesta y sesenta parecía suficiente.

Conceder acceso de lectura a una aplicación útil, con un clic.

Cada una defendible. Ninguna revisada nunca más.

> **El riesgo grave rara vez viene de la negligencia. Viene de la *acumulación de decisiones razonables* que nadie volvió a mirar.**

Por eso la respuesta no es un control nuevo. Es una fecha de revisión.

De dónde *sale cada cifra*

FUENTES POR PÁGINA

Pág. 04 y 11	**IBM / Ponemon, *Cost of a Data Breach Report 2026*** (29 jul 2026): 227,250 dólares, 258 días, 247 días y su alza del 2.5%, 4.99 millones.
Pág. 05	**Akamai, *2026 API Security Impact Study*** (28 abr 2026): 23% frente al 40% de 2022.
Pág. 06	**Palo Alto Networks Unit 42, Chinese-Speaking Threat Actor Harnesses AI Models for Autonomous Cyberattacks** (30 jul 2026): más de 460 objetivos, 3 NetScaler, 11 Marimo. **Wallarm, *2026 API ThreatStats Report*** (17 feb 2026): 106 de 245 incorporaciones al KEV.
Pág. 07	**GitGuardian, *State of Secrets Sprawl 2026*** (mar 2026): 64%, 28.65 millones, +34%, seis veces. **Palo Alto Networks, *2026 Identity Security Landscape*** (may 2026): 109:1, 79 agentes de IA, 82:1. **Entro Security, 2025 State of Non-Human Identities and Secrets:** 97%. **Entro Labs, The NHI & Secrets Risk Report H1 2025:** 62%.
Pág. 09	**OWASP, *API Security Top 10*** edición 2023 (API1:2023, BOLA). **Akamai, *2026 API Security Impact Study*** : 87% y 700 mil dólares. **Ley 53-07** sobre Crímenes y Delitos de Alta Tecnología.
Pág. 10	**OX Security** (ene 2026): 900,000 instalaciones. **Invictus IR, *The Consent Epidemic*** (feb 2026): UNC6395, más de 700 organizaciones. **LayerX** : 68%.

HERRAMIENTAS MENCIONADAS

Gratuitas, de código abierto o con plan gratuito. Algunas funciones, como el filtro por red de Shodan, requieren membresía. Su uso paso a paso está documentado en la Guía de Ejecución, sección por sección.