UNIPAGO | UNISHIELD BY UNIPAGO

UNISHIELD

Guía de Ejecución

Manual operativo para inventariar la superficie expuesta, las credenciales, los consumidores de API y las herramientas externas del ecosistema. Está organizado para ejecución directa: seleccione la sección que corresponda, siga los pasos en orden y utilice los comandos indicados.

TLP:GREEN

EDICIÓN
Agosto 2026

RUTAS VERIFICADAS
27 de agosto de 2026

EXTENSIÓN
33 hojas

Contenido

Cinco secciones y sus procedimientos, con el esfuerzo estimado. Los enlaces saltan directo al bloque.

CÓMO LEER LOS MARCADORES

✅ Procedimiento verificado · sin costo
La verificación corresponde al procedimiento y a la fuente oficial indicada, no a la herramienta: no constituye evaluación de seguridad ni aprobación para uso corporativo, y las condiciones de un servicio de terceros pueden cambiar después de la fecha de verificación.

⚠️ Con salvedad
Funciona, pero hay algo que leer antes.

$ Requiere plan de pago
El nivel gratuito alcanza para probarlo una vez, no para repetirlo.

⚖️ Requiere coordinación previa
Con legal o gestión humana. Léala completa antes de ejecutar.

SECCIÓN I

Antes de empezar

Tres condiciones que aplican a todos los procedimientos de esta guía.

I.1 · Sobre qué sistemas

Todos los procedimientos de esta guía están diseñados para ejecutarse sobre activos que su institución posee o controla, con autorización del responsable de tecnología o seguridad de la información.

Ejecutar pruebas activas, escaneos o consultas de autorización contra sistemas de terceros sin autorización escrita constituye acceso no autorizado a sistemas de información y está tipificado en la **Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología**. La intención defensiva no altera esa calificación.

Un procedimiento requiere coordinación previa con las áreas legal o de gestión humana antes de ejecutarse. Está señalado con ⚖️ en el índice y en su encabezado.

I.2 · Sobre las herramientas

Las herramientas sin costo incluidas en esta guía permiten ejecutar verificaciones puntuales sin inversión previa. Para uso recurrente o incorporado a un proceso operativo, evalúe si su organización requiere una versión con soporte, administración centralizada y garantías de continuidad: las condiciones de uso de una herramienta gratuita pueden cambiar sin aviso.

Descargue o acceda a las herramientas únicamente desde los sitios oficiales indicados en esta guía. Evite enlaces patrocinados, repositorios espejo, instaladores de terceros, extensiones o versiones modificadas: son vectores habituales de distribución de software malicioso y captura de credenciales.

Antes de instalar, autorizar o proporcionar información a una herramienta externa, valide su procedencia y siga el proceso de evaluación y aprobación de seguridad de su organización.

La inclusión de una herramienta en esta guía no constituye su aprobación para uso corporativo.

I.3 · Sobre lo que estos procedimientos producen

⚠ **CUSTODIA DE LOS PRODUCTOS DE ESTE EJERCICIO**

Los archivos que generan estos procedimientos concentran, en un solo lugar, información que normalmente está dispersa y protegida. El inventario de credenciales lista las llaves activas de la organización con su fecha de último uso. El resultado del escaneo de repositorios contiene secretos en texto claro. El inventario de cuentas de servicio es un mapa de objetivos de ataque contra el directorio. Los reportes de tráfico saliente pueden identificar a personas.

Antes de ejecutar cualquier procedimiento, defina:

- Dónde se almacenan estos archivos, con cifrado en reposo.
- Quién tiene acceso, con criterio de mínimo privilegio.
- Cuánto tiempo se conservan.
- Cómo se destruyen al cerrar el ejercicio.

No los deje en la estación de trabajo del analista, no los envíe por correo sin cifrar y no los suba a repositorios ni a plataformas de colaboración.

Un inventario de exposición sin custodia es una herramienta de ataque documentada, ordenada y con dueño.

Descubrimiento no es vulnerabilidad

Cada nivel exige una respuesta distinta. Tratar toda observación como incidente agota al equipo; tratar todo incidente como observación pierde la ventana de respuesta.

NIVEL	QUÉ SIGNIFICA	EJEMPLO
Observación	Algo que no estaba inventariado	Un subdominio activo que nadie reconoce
Hallazgo	Una condición que requiere evaluación o regularización	Una credencial sin rotar en tres años; un servicio contratado fuera del proceso
Vulnerabilidad	Una debilidad comprobada y explotable	Una prueba de autorización que devuelve datos ajenos
Incidente	Evidencia de que ya ocurrió	Un secreto válido expuesto públicamente

LÉASE ANTES DE EJECUTAR

Para quién es esta guía

Esta guía asume conocimiento técnico intermedio: manejo de las consolas de AWS o Azure, línea de comandos básica, y conceptos de red como ASN y rangos IP. No es un curso introductorio; es un manual de ejecución para quien ya opera la infraestructura de su institución.

Cada procedimiento indica al inicio lo que necesita tener listo. Si un requisito no está a su alcance, esa parte corresponde a otra área; anótelo y sígalo con quien tenga el acceso.

Las rutas de menú y los nombres de pantalla corresponden a las interfaces vigentes al momento de la verificación. Los proveedores las renombran con frecuencia; si no encuentra una opción, consulte la documentación oficial enlazada en cada procedimiento.

Si solo puede hacer tres cosas este trimestre

En este orden. Las tres se hacen sin presupuesto y sin abrir un proyecto.

II.3 **Suscríbase a los reportes gratuitos**
Es el único paso que después trabaja solo.

III.2 **Extraiga el inventario de credenciales de nube**
Cinco minutos, y es el ejercicio de mayor rendimiento de la guía.

V.1 **Revise qué sale de su red**
El registro ya existe. Lea antes el bloque ⚖️ de la sección.

SECCIÓN II

¿Qué exponemos?

Las fuentes de esta sección son públicas y consultarlas no requiere autorización. Aun así, dentro del ecosistema aplica una regla de convivencia: estas rutas se usan sobre el dominio propio. Si al revisar el suyo encuentra un activo expuesto de otra institución miembro, no lo explore ni lo consulte: compártalo con UNISHIELD, que lo hace circular por el canal de intercambio del ecosistema sin atribuir el origen del hallazgo. La decisión y la acción sobre ese activo corresponden a la institución que lo posee.

II.1 · Certificados olvidados (Certificate Transparency)

✅ PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** un navegador. Ninguna cuenta para la vía principal.

Qué encuentra: subdominios de desarrollo, pruebas, staging y proyectos cerrados para los que alguna vez se emitió un certificado TLS. Todo certificado público queda registrado en los logs de Certificate Transparency, que son de solo agregado.

Vía principal: crt.sh

Sin cuenta, sin cuota y sin límite de consultas. Cubre exactamente este caso de uso.

1. Entre a `crt.sh`.
2. Busque su dominio con comodín para incluir subdominios:

CRT.SH · CONSULTA

```
%.sudominio.com.do
```

3. Añada `&output=json` a la URL del resultado si prefiere procesarlo con una herramienta en lugar de copiarlo de la tabla.

Segunda vía: CertSpotter (SSLMate)

Útil para automatizar. La API sin autenticar tiene un límite de tasa agresivo y no devuelve el historial completo, por lo que sirve como verificación complementaria, no como sustituto de crt.sh.

CERTSPOTTER API · URL

```
https://api.certspotter.com/v1/issuances?
domain=sudominio.com.do&include_subdomains=true&expand=dns_names
```

Qué hacer con el resultado. Copie los nombres a una hoja de cálculo, elimine duplicados y marque los que no reconozca. Si aparece, por ejemplo, `api-v1` cuando el servicio en operación es `v3`, ambos registros corresponden a activos fuera de inventario y deben documentarse como hallazgo.

Opción avanzada: Censys Platform $

Añade correlación con hosts y servicios, útil si ya trabaja con la plataforma. Dos condiciones antes de apoyarse en ella:

⚠ Cambio de sintaxis y de plataforma

Censys deprecará Legacy Search en septiembre de 2026. En la Plataforma hay que anteponer el dataset a cada consulta (`host.`, `cert.` o `web.`), de modo que el equivalente de `names:` es `cert.names:`.

El nivel gratuito se consume con las consultas, la paginación y los filtros laterales, de modo que se agota antes de terminar la revisión de un dominio con varios cientos de certificados. Las expresiones regulares están reservadas a los niveles de pago.

CENSYS PLATFORM · CONSULTA

```
cert.names: sudominio.com.do
```

FUENTE OFICIAL

crt.sh · crt.sh
CertSpotter · sslmate.com/certspotter
Censys Platform · docs.censys.com

Nota de verificación: deprecación de Legacy Search y cambio de sintaxis confirmados contra la documentación de Censys. Verifique la fecha efectiva antes de publicar.

QUÉ HACER CON EL HALLAZGO

No desactive ningún activo de inmediato. Un subdominio o un recurso "olvidado" puede seguir sirviendo a alguien que usted no tiene mapeado.

Aplique la secuencia siguiente. Primero, confirme si el activo recibe tráfico real; los reportes de Shadowserver y los logs de su balanceador o CDN se lo dicen. Segundo, si no ve tráfico, deshabilítelo de forma reversible en lugar de eliminarlo: detenga el servicio o bloquee el acceso, pero no borre todavía. Tercero, mantenga un período de observación proporcional al ciclo operativo del servicio, con un mínimo definido por su organización: para servicios de uso diario, una a dos semanas suele bastar; para procesos mensuales o trimestrales, el período debe cubrir al menos un ciclo completo. Solo entonces elimine.

II.2 · Su superficie expuesta a Internet (Shodan / Censys)

⚠ CON SALVEDAD

$ REQUIERE PLAN DE PAGO

- **Requiere:** cuenta de Shodan o Censys con sesión iniciada. Conocer su ASN o sus rangos IP.

Qué encuentra: servicios expuestos que no deberían estarlo: paneles de administración, bases de datos, RDP, APIs sin autenticación.

> ⚠ **Requisito previo a considerar**
>
> En la práctica, repetir esta revisión cada trimestre requiere un plan de pago. Los filtros de búsqueda de Shodan (`asn:`, `org:`, `net:`, `http.title:`) requieren una cuenta con sesión iniciada. La cuenta gratuita es limitada:
>
> - Devuelve solo la primera página o las dos primeras (aproximadamente entre 10 y 100 resultados, según la fuente).
> - Sin acceso a la API.
> - El filtro `vuln:` requiere un plan de pago.

PROCEDIMIENTO

1. Ubique su ASN o rangos IP. Si no los conoce, busque su institución por nombre en `bgp.he.net`. Si contrata conectividad y no tiene ASN propio, pida los rangos a su proveedor.
2. Inicie sesión en `shodan.io` y ejecute:

SHODAN · FILTROS

```
asn:AS12345
org:"Nombre de su institución"
ssl.cert.subject.CN:"sudominio.com.do"
asn:AS12345 port:3389
asn:AS12345 port:1433,3306,5432,27017
asn:AS12345 http.title:"login"
```

Alternativa sin costo: la API InternetDB de Shodan ✅

Devuelve los metadatos que Shodan tiene de una IP concreta —puertos abiertos, hostnames, etiquetas— sin cuenta y sin créditos. No permite buscar por ASN, de modo que sirve para recorrer una lista de IP que usted ya conoce, no para descubrir la superficie desde cero.

BASH · INTERNETDB

```
curl https://internetdb.shodan.io/203.0.113.10
```

Verifique la disponibilidad y el comportamiento actual del servicio antes de incorporarlo a una revisión periódica.

3. Use los filtros de la barra lateral (país, producto, puerto); estos filtros son los que revelan los servicios no previstos.

CÓMO CONFIRMAR QUE FUNCIONÓ

Su propio sitio web público debe aparecer en los resultados. Si no aparece, revise que el ASN o el rango sean los correctos antes de sacar conclusiones.

II.3 · Reportes gratuitos permanentes (Shadowserver)

✅ PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** una dirección de correo institucional y capacidad de demostrar control sobre sus rangos.

Es el único procedimiento de la guía que, una vez configurado, opera de forma automática y continua. Sin costo ni límite de uso.

Qué recibe: reportes diarios de activos comprometidos, expuestos y vulnerables dentro de su propia red, filtrados por su ASN, CIDR o dominio. Más de 100 tipos de reporte disponibles, en formato CSV, por correo o API.

PROCEDIMIENTO

1. Entre a `shadowserver.org/what-we-do/network-reporting/get-reports/`
2. Complete el formulario de solicitud con los datos de su organización y su espacio de red (ASN o CIDR).
3. Shadowserver evalúa la solicitud y verifica que usted controla esos rangos.
4. A partir de la aprobación, recibe los reportes diarios automáticamente.

Para administración posterior, como agregar rangos o cambiar destinatarios, escriba a `report_admin@shadowserver.org`.

FUENTE OFICIAL

`The Shadowserver Foundation · shadowserver.org/what-we-do/network-reporting/get-reports/`

Nota de verificación: confirmado sin costo, con URL oficial del formulario. La verificación de control de rangos es parte del proceso.

CÓMO CONFIRMAR QUE FUNCIONÓ

Recibirá un correo de confirmación de la suscripción. Después llega un correo por cada tipo de reporte suscrito, en los días en que haya datos para su red; ese correo no trae el archivo adjunto, sino una URL a la ubicación de descarga. Si no hay actividad detectada, no se envía reporte, y esa ausencia también constituye información de control.

PARA QUE LA SOLICITUD AVANCE RÁPIDO

- Solicite por ASN antes que por CIDR: es la forma preferida y evita revisiones manuales.
- Que el correo del solicitante figure en los registros whois del ASN acelera la verificación.
- Use un alias de correo institucional, no la dirección individual de un analista.

II.4 · Recursos cloud no declarados

PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** acceso de lectura a la consola de su proveedor (AWS o Azure).

AWS

Cuentas olvidadas. Busque cuentas de proyectos cerrados en:

`consola › AWS Organizations › AWS accounts`

Reglas abiertas a todo Internet. La vía gratuita y ya calculada es la verificación *Security Groups – Unrestricted Access*:

`Trusted Advisor › Security › Security Groups - Unrestricted Access`

Recursos creados fuera de proceso. Seleccione todas las regiones y filtre por recursos sin etiquetas. Lo creado por proceso formal suele llevar etiquetas; lo creado de forma manual, no.

`Resource Groups & Tag Editor › Tag Editor › todas las regiones › recursos sin etiquetas`

> **FUENTE OFICIAL**
>
> AWS Trusted Advisor · docs.aws.amazon.com/awssupport/latest/user/security-checks.html
> AWS Organizations · docs.aws.amazon.com/organizations

Azure

Suscripciones olvidadas.

`portal › Cost Management + Billing › Subscriptions`

Reglas abiertas y puertos de administración expuestos. Las recomendaciones básicas de postura son gratuitas; algunas capacidades avanzadas de Defender for Cloud tienen costo.

`Microsoft Defender for Cloud › Recommendations › filtro Networking`

Recursos sin etiquetar.

`All resources › Add filter › Tags › sin valor`

> **CÓMO CONFIRMAR QUE FUNCIONÓ**
>
> Contraste el conteo de recursos que devuelve la consola con lo que su equipo cree tener. Toda diferencia corresponde, por definición, a recursos sin gestión asignada.

II.5 · Cambio de proceso (aplica a todos)

PROCEDIMIENTO VERIFICADO · SIN COSTO

> Al desmontar un servicio, elimine **primero el registro DNS y después el recurso**. El intervalo inverso, un registro que apunta a un recurso que ya no existe, permite a un tercero reclamar el destino (*subdomain takeover*) y alojar contenido bajo su dominio.

SECCIÓN III

¿Quién tiene llaves?

III.1 · Cuentas de servicio en el directorio (on-premise)

✅ PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** el módulo de Active Directory de PowerShell (RSAT) y permiso de lectura sobre el directorio.

Qué encuentra: cuentas habilitadas con contraseña que nunca expira y sin actividad reciente registrada. El estado de MFA no forma parte del resultado: Active Directory on-premise no expone ese atributo, y ese dato se consulta en Entra o en la solución de autenticación que lo aporte.

Vía gráfica

Centro de administración de Active Directory (`dsac.msc`) con búsqueda global por atributos, o una consulta guardada:

`dsac.msc › Global Search` `dsa.msc › Saved Queries`

Vía PowerShell (método recomendado para este caso)

POWERSHELL

```
Get-ADUser -Filter {PasswordNeverExpires -eq $true -and Enabled -eq $true} `
  -Properties PasswordLastSet, LastLogonDate, Department |
  Select-Object Name, SamAccountName, Department, PasswordLastSet, LastLogonDate |
  Sort-Object PasswordLastSet |
  Export-Csv cuentas-servicio.csv -NoTypeInformation -Encoding UTF8
```

Ordene por `PasswordLastSet` . **Todo valor superior a dos años debe priorizarse para revisión;** se considera hallazgo cuando la antigüedad no esté respaldada por una excepción vigente, un propietario identificado y controles compensatorios. Si `LastLogonDate` está vacío, la cuenta no registra uso y permanece habilitada.

⚠️ **LastLogonDate va por detrás de la actividad real**

El campo deriva de `lastLogonTimestamp` . Con los ajustes por defecto va entre nueve y catorce días por detrás de la fecha actual, por diseño: es un umbral aleatorizado destinado a limitar el tráfico de replicación, no un indicador en tiempo real.

Una cuenta usada ayer puede aparecer sin actividad reciente. Trátelo como indicador de inactividad prolongada, nunca como confirmación de desuso, y descuente esa latencia del período de observación antes de desactivar nada. Para seguimiento real, consulte el registro de eventos de seguridad de los controladores de dominio.

Acotar a cuentas de servicio

El filtro anterior localiza cuentas con contraseña perpetua, que no es lo mismo que cuentas de servicio. Para acotar a las que tienen un servicio Kerberos registrado, añada `ServicePrincipalName -like "*"` como discriminante complementario, no como sustituto.

POWERSHELL · DISCRIMINANTE COMPLEMENTARIO

```
Get-ADUser -Filter {PasswordNeverExpires -eq $true -and Enabled -eq $true `
  -and ServicePrincipalName -like "*"} -Properties ServicePrincipalName
```

No toda cuenta de servicio tiene SPN: las que ejecutan tareas programadas o servicios locales pueden no tenerlo. Quedan además fuera del alcance de este comando las cuentas de servicio administradas de grupo (`Get-ADServiceAccount`) y las cuentas de equipo.

Verifique el alcance de `ServicePrincipalName` contra la documentación de su nivel funcional de directorio antes de publicar.

Nota técnica. `PasswordNeverExpires` no es un atributo real de Active Directory. Es una propiedad calculada del atributo `UserAccountControl` . Esto explica por qué algunas herramientas no lo muestran directamente.

FUENTE OFICIAL

Microsoft Learn · Get-ADUser · learn.microsoft.com/powershell/module/activedirectory/get-aduser

Nota de verificación: filtro confirmado contra múltiples fuentes concordantes. El comando funciona con el módulo Active Directory de PowerShell (RSAT) instalado.

CÓMO CONFIRMAR QUE FUNCIONÓ

Abra un par de las cuentas señaladas y confirme en sus propiedades que efectivamente tienen la contraseña sin expiración y sin actividad reciente. Con ello se valida que el filtro se aplicó correctamente.

QUÉ HACER CON EL HALLAZGO

El criterio rector es la reversibilidad: la desactivación de una credencial se revierte en segundos, la eliminación no se revierte. Por esa razón el procedimiento nunca inicia con la eliminación.

El procedimiento seguro, confirmado por la documentación de AWS, comprende cuatro etapas. **Desactive** la llave o la cuenta, que es una acción reversible al instante. **Observe** durante un período proporcional al ciclo operativo del servicio, con un mínimo definido por su organización: una a dos semanas para uso diario, al menos un ciclo completo para procesos mensuales o trimestrales. En AWS, vigile CloudTrail en busca de errores de acceso denegado que indiquen dependencias de esa credencial. **Si algo se rompe**, reactive de inmediato; la interrupción identifica al consumidor que dependía de ella. **Si nada se rompe** en el período de gracia, entonces sí elimine de forma permanente.

Una advertencia sobre las fechas de último uso: algunas credenciales legítimas se usan de forma esporádica, por procesos que corren una vez al mes o al trimestre. No trate un "sin uso en 90 días" como sentencia automática; el período de gracia con monitoreo existe precisamente para detectar esos casos antes de provocar una interrupción.

III.2 · Llaves de la nube

PROCEDIMIENTO VERIFICADO · SIN COSTO CON COSTO (PARCIAL)

- **Requiere:** acceso a IAM en AWS, o a App registrations en Entra, con permiso de lectura.

AWS · reporte de credenciales (gratuito) ✅

Es el procedimiento de mayor rendimiento de la sección y requiere aproximadamente cinco minutos.

Vía GUI

`consola › IAM › Credential report › Download Report`

Vía CLI (dos comandos; el primero, por sí solo, no devuelve nada)

```bash
aws iam generate-credential-report
aws iam get-credential-report --query 'Content' --output text | base64 -d > cred.csv
```

En macOS, el segundo termina en `base64 -D`.

Cómo leerlo. Ordene por `access_key_1_last_used_date`. Las filas con `N/A` son llaves activas que nunca se usaron; empiece por ahí.

⚠ Limitación oficial documentada

El reporte solo incluye las dos primeras access keys por usuario y no incluye credenciales de servicio específicas (CodeCommit, Bedrock, CloudWatch Logs). Para obtener visibilidad completa debe utilizarse `ListServiceSpecificCredentials` y `ListAccessKeys`.

FUENTE OFICIAL

docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html

AWS · analizador de acceso no utilizado 💲

Identifica automáticamente roles, llaves y contraseñas sin usar, con período de rastreo configurable (de 1 a 365 días).

`IAM › Access Analyzer › Analyzer settings › Create analyzer › Unused access`

💲 **Tiene costo**

A diferencia del credential report, IAM Access Analyzer cobra por rol y usuario analizado por mes. Preséntelo como opción de mayor madurez, no como el paso base.

FUENTE OFICIAL

docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-create-unused.html

Azure / Entra · secretos de aplicaciones ⚠️

Vía GUI (revisión individual, aplicación por aplicación). Abra cada una, revise sus certificados y secretos, y busque los que no tengan caducidad:

`entra.microsoft.com › Applications › App registrations › All applications › Certificates & secrets › Expires`

Vía script oficial de Microsoft (evita la revisión individual). Microsoft publica un script de PowerShell listo para exportar todas las app registrations con secretos y certificados por expirar a un CSV.

✅ **Método recomendado para Azure.** Microsoft mantiene el script oficialmente, lo que elimina la necesidad de la revisión manual aplicación por aplicación.

FUENTE OFICIAL

learn.microsoft.com/entra/identity/enterprise-apps/scripts/powershell-export-apps-with-expiring-secrets

CÓMO CONFIRMAR QUE FUNCIONÓ

Cada llave marcada como sin uso debe poder cruzarse con CloudTrail (AWS) para confirmar que no registra actividad reciente. Si CloudTrail tampoco registra actividad, el hallazgo queda confirmado.

III.3 · Consentimientos OAuth

PROCEDIMIENTO VERIFICADO · SIN COSTO

▸ **Requiere:** rol de Cloud Application Administrator o superior en Entra.

Por qué es el canal más crítico: un consentimiento puede mantener acceso programático persistente con independencia de cambios de contraseña o reinicios de MFA, mientras el consentimiento y las credenciales o tokens asociados permanezcan válidos. Ese acceso no requiere contraseña y puede no aparecer como inicio de sesión anómalo.

Revisar lo ya concedido

1. Vaya a la lista completa de aplicaciones empresariales:

   `entra.microsoft.com › Applications › Enterprise applications › All applications`

2. Aplique el filtro `Application type = All Applications`. Es indispensable: con el valor por defecto, las aplicaciones de terceros no se listan.

3. Revise la pestaña **Permissions** de cada app, y la pestaña **Users and groups** para ver quién la autorizó.

Vía scriptable (Microsoft Graph PowerShell)

Resuelve en un comando lo que la ruta manual hace en cien clics, con el mismo criterio que la guía aplica a la nube en III.2.

POWERSHELL · MICROSOFT GRAPH

```
Connect-MgGraph -Scopes "Application.Read.All","Directory.Read.All"

Get-MgOauth2PermissionGrant -All |
  Select-Object ClientId, ResourceId, ConsentType, PrincipalId, Scope |
  Export-Csv consentimientos.csv -NoTypeInformation -Encoding UTF8

Get-MgServicePrincipal -All |
  Select-Object DisplayName, AppId, PublisherName, AccountEnabled |
  Export-Csv service-principals.csv -NoTypeInformation -Encoding UTF8
```

⚠️ **Cambio de ajustes por defecto de julio de 2025 (MC1097272)**

Microsoft actualizó los ajustes por defecto para bloquear protocolos de autenticación heredados y exigir consentimiento administrativo para el acceso de aplicaciones de terceros a archivos y sitios. El despliegue comenzó a mediados de julio de 2025 y se completó en agosto de 2025.

Las organizaciones que ya habían bloqueado el consentimiento de usuario, aplicado los ajustes recomendados o configurado políticas propias no se ven afectadas por este cambio.

El cambio actúa sobre consentimientos futuros. En consecuencia, no altera lo ya concedido, y la revisión histórica del paso 1 sigue siendo indispensable.

Priorice: permisos de aplicación (no delegados) sobre correo, archivos o sitios; editor no verificado con permisos amplios; consentimiento de alguien ya desvinculado; y aplicaciones sin actividad en 90 días con permisos vigentes.

Auditoría de eventos de consentimiento. Exportable a CSV:

```
Monitoring & health › Audit logs › Activity = Consent to application
```

El control preventivo (dos ajustes que van juntos)

1. `Enterprise applications › Consent and permissions › User consent settings` y elija *Allow user consent for apps from verified publishers, for selected permissions*.
2. En la misma sección, en **Admin consent settings**, active el flujo de solicitud de consentimiento administrativo.

> Sin el segundo ajuste, el primero genera fricción operativa y suele revertirse; ambos deben aplicarse en conjunto.

Google Workspace:

```
Admin console › Security › Access and data control › API controls ›
Manage Third-Party App Access
```

FUENTE OFICIAL

`learn.microsoft.com/entra/identity/enterprise-apps/manage-consent-requests`
`learn.microsoft.com/entra/identity/enterprise-apps/configure-user-consent`

Nota de verificación: rutas confirmadas. El cambio de ajustes por defecto de julio de 2025 corresponde al aviso MC1097272 del centro de mensajes de Microsoft. La ruta de clasificación de permisos (Low/Medium/High) está en la misma sección Consent and permissions.

CÓMO CONFIRMAR QUE FUNCIONÓ

Tras aplicar el control preventivo, pida a un usuario de prueba que intente consentir una aplicación de terceros no verificada. Debe recibir la pantalla de solicitud de aprobación, no la de consentimiento directo.

QUÉ HACER CON EL HALLAZGO

Revocar el consentimiento impide emitir tokens nuevos, pero no invalida los access tokens ya emitidos, que siguen siendo válidos hasta expirar —típicamente una hora, y más si hay evaluación de acceso continuo. Para cortar el acceso de inmediato hay que deshabilitar el inicio de sesión del service principal y revocar los refresh tokens. Es una diferencia material en respuesta a incidentes.

La revocación presenta además dos particularidades que deben considerarse para completar la remediación.

La primera: **revocar el permiso no impide que el usuario vuelva a consentir la misma aplicación**. Por eso la revocación siempre va acompañada del control preventivo de la Sección III.3; sin él, la aplicación vuelve a autorizarse en días. La segunda: **el consentimiento sobrevive al borrado de la cuenta del usuario que lo otorgó**. Si desvinculó a alguien y no revocó lo que había consentido, ese acceso permanece activo y debe revocarse desde la aplicación (el service principal), no desde el usuario.

El orden recomendado: para un acceso claramente malicioso, deshabilite el inicio de sesión del service principal de inmediato, lo que corta todo sin borrar nada. Para una aplicación legítima pero sobre-permisionada, revoque los permisos específicos que sobran. Antes de eliminar por completo un service principal, confirme que ninguna automatización ni paquete de acceso dependa de él, igual que con cualquier otra credencial.

III.4 · Secretos en repositorios

✅ PROCEDIMIENTO VERIFICADO · SIN COSTO

💲 CON COSTO (PARCIAL)

- **Requiere:** acceso de administración a su plataforma de código, o permiso para clonar los repositorios localmente.

Detección integrada de la plataforma

PLATAFORMA	RUTA	LICENCIA
GitHub	`Repo/Org › Settings › Code security › Secret protection`	✅ Gratis en repos públicos · 💲 requiere GHAS en privados
Azure DevOps	`Project settings › Repos › habilitar Advanced Security`	💲 Requiere GitHub Advanced Security for Azure DevOps
GitLab	`Secure › Security configuration › Secret Detection`	✅ Escaneo básico en tier gratuito · dashboards en tier de pago

Alternativa gratuita para cualquier plataforma (incluye escaneo de historial)

⚠️ **Seguridad de la descarga**

Utilice exclusivamente el repositorio oficial indicado. No descargue instaladores desde resultados patrocinados, repositorios espejo o sitios de terceros.

```bash
gitleaks git . --report-path fugas.json
trufflehog git file://./repositorio --only-verified
```

> Ejecute estas herramientas únicamente sobre repositorios de su propia organización, incluidos los privados y los archivados. Si detecta un secreto de su institución expuesto en un repositorio ajeno, no lo explore: rótelo de inmediato —la rotación le corresponde a usted, y es lo único que corta el acceso— y compártalo con UNISHIELD para que el ecosistema tenga el dato.

`gitleaks git` recorre todo el historial de commits por defecto, lo cual es el alcance requerido, dado que un secreto eliminado en un commit posterior permanece recuperable. El subcomando `detect` quedó deprecado en la versión 8.19.0: sigue funcionando, pero está oculto del menú de ayuda.

Dos criterios de ejecución: empiece por los repositorios internos, con probabilidad notablemente mayor de contener secretos que los públicos, y rote, no borre: borrar el archivo no invalida la credencial.

> **FUENTE OFICIAL**
>
> docs.github.com/code-security/secret-scanning
> learn.microsoft.com/azure/devops/repos/security/github-advanced-security-secret-scanning
> docs.gitlab.com/user/application_security/secret_detection
> github.com/gitleaks/gitleaks · github.com/trufflesecurity/trufflehog

CÓMO CONFIRMAR QUE FUNCIONÓ

El escaneo debe reportar cero secretos en un repositorio que usted sepa limpio, y detectar un secreto insertado deliberadamente como prueba. Con ello se confirma que la herramienta está mirando el historial y no solo el estado actual.

> **QUÉ HACER CON EL HALLAZGO**
>
> Un secreto expuesto se remedia rotando, nunca borrando. Borrar el archivo, el commit o el mensaje no invalida la credencial; únicamente la oculta a quien debe rotarla. Buena parte de los secretos filtrados sigue siendo válida años después de su supuesta eliminación.
>
> El orden correcto es rotar primero y limpiar después. **Rote** la credencial en el sistema que la emitió, de modo que la versión filtrada deje de funcionar. **Verifique** que los servicios legítimos siguen operando con la credencial nueva. **Después**, y solo como higiene, limpie el historial del repositorio. El orden inverso, limpiar primero, abre un intervalo en el que la credencial ya no figura en el código pero mantiene el acceso vigente.

SECCIÓN IV

¿Quién nos habla?

Consumidores de API

IV.1 · Inventario de consumidores por credencial

PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** acceso al panel de su API gateway y a sus logs (CloudWatch, o Analytics de APIM).

Error de método a evitar: agrupar por IP. Las IP cambian, se comparten y se ocultan tras NAT y CDN. Agrupe por credencial: API key, `client_id` o common name del certificado.

AWS API Gateway

Consumidores y su uso. Cada key debería estar asociada a un usage plan con throttling y cuota.

```
consola › API Gateway › Usage Plans · API Keys
```

Métricas por consumidor. Muestra volumen y throttles por cliente.

```
CloudWatch › Metrics › AWS/ApiGateway › By ApiKey
```

Logs detallados. Habilite CloudWatch Logs por stage para ver cada llamada con su contexto de API key.

> ⚠️ **Salvedad oficial importante**
>
> AWS documenta explícitamente que los usage plans y las API keys no son un mecanismo de autorización, y que el throttling y la cuota se aplican *best-effort*, no como límite duro. Sirven para identificar y medir consumidores, no para autenticar. La autenticación va por IAM, Lambda authorizers o Cognito.

> FUENTE OFICIAL
>
> `docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html`

Azure API Management

Consumidores. Cada suscripción tiene su par de claves.

```
portal › API Management › Subscriptions · Users
```

Analítica por consumidor. En la sección **Analytics**, filtrable por suscripción, producto y API.

> FUENTE OFICIAL
>
> `learn.microsoft.com/azure/api-management/api-management-subscriptions`

Las seis preguntas (para cualquier plataforma)

1. Cuántas credenciales distintas están activas.
2. Si cada una tiene dueño con nombre.
3. Cuándo rotó por última vez.
4. Si se usó desde más de un ASN o país.
5. Si hay tráfico en endpoints deprecados (es un zombie confirmado).
6. Qué endpoints devuelven más volumen por petición.

CÓMO CONFIRMAR QUE FUNCIONÓ

El número de credenciales activas que arroje el panel debe coincidir con las integraciones que usted puede nombrar. Si hay más credenciales que integraciones conocidas, la diferencia constituye el punto ciego del inventario.

QUÉ HACER CON EL HALLAZGO

Para cada credencial de consumidor que quede sin dueño identificable, aplique el mismo principio de reversibilidad de la Sección III. No la borre; **desactívela y espere**. En un API gateway esto se hace deshabilitando la key o la suscripción, lo cual es reversible. Si al cabo del período de observación —al menos un ciclo operativo completo del consumidor— nadie reclama la interrupción, elimínela. Si alguien reclama, ya identificó al dueño que faltaba, y ahora puede documentarlo.

Para las integraciones entre instituciones del ecosistema, el alcance excede lo técnico: cada credencial compartida debería tener, del otro lado, un contacto con nombre y un acuerdo que permita rotarla sin depender del calendario de la contraparte. Si hoy no puede rotar una credencial sin abrir un ticket y esperar semanas, esa credencial es, en la práctica, permanente y debe tratarse como riesgo abierto.

IV.2 · Prueba de autorización rota (BOLA)

PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** dos credenciales de su propio sistema con ámbitos de acceso distintos, preferiblemente en ambiente de pruebas o preproducción.

Por qué los escáneres tradicionales pueden no detectarlo: la petición es válida, la autenticación correcta y la respuesta un `200` legítimo. Identificar BOLA requiere comparar el comportamiento de una misma operación bajo identidades o ámbitos de autorización diferentes; exige pruebas específicas de autorización, manuales o automatizadas. Es el riesgo número 1 del OWASP API Security Top 10 desde 2019 (la edición 2023 sigue vigente en 2026).

Procedimiento manual · sobre sus propios sistemas

Las dos cuentas son credenciales de su propio sistema con ámbitos de acceso distintos: los registros que la cuenta A puede ver no son los que puede ver la cuenta B. Lo que se verifica es si su API comprueba el ámbito, no solo la identidad de quien pregunta.

1. Con la cuenta A, cree o identifique un recurso y anote su identificador.
2. Con la cuenta B, autenticada legítimamente, solicite ese mismo identificador.
3. Si devuelve los datos de A, el endpoint es vulnerable.

Repita donde viaje el identificador: ruta, query string, cuerpo y cabeceras.

Herramienta de apoyo (gratuita): la extensión **Autorize** de Burp Suite automatiza esta prueba repitiendo cada petición con las credenciales de un segundo usuario y marcando dónde el acceso no fue bloqueado.

> ⚠️ **Seguridad de la descarga**
>
> Utilice exclusivamente el repositorio oficial indicado. No descargue instaladores desde resultados patrocinados, repositorios espejo o sitios de terceros.

> Autorize repite peticiones de forma automatizada. Úsela exclusivamente contra entornos propios, preferiblemente en ambiente de pruebas o preproducción, y con el alcance documentado por escrito antes de iniciar. No la apunte a endpoints de terceros bajo ninguna circunstancia.

FUENTE OFICIAL

`OWASP API Security Top 10 2023 · owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization`
`Autorize · github.com/PortSwigger/autorize`

Nota de verificación: confirmado que la edición 2023 del OWASP API Top 10 es la vigente a mediados de 2026 y que BOLA (API1:2023) mantiene el primer lugar.

CÓMO CONFIRMAR QUE FUNCIONÓ

Una prueba correcta produce ambos resultados: la cuenta B recibe sus propios datos con normalidad, y no recibe los de la cuenta A. Un **403** indica que el control de autorización funcionó; un **404** es preferible, porque el 403 confirma la existencia del objeto y permite enumerar identificadores válidos aunque no se acceda a ellos. Si obtiene una negativa en ambos casos, revise que la cuenta B esté bien autenticada antes de declarar el endpoint seguro.

La verificación que ninguna institución puede hacer sola

El procedimiento anterior comprueba que sus endpoints no entreguen a una credencial los registros que corresponden a otra, dentro de su propio sistema. Es la prueba que usted puede correr esta semana.

Existe una pregunta más amplia: si sus endpoints distinguen entre una organización y otra cuando varias comparten plataforma. Responderla exige credenciales legítimas de dos entidades distintas consultando el mismo identificador, y eso ninguna institución puede hacerlo por su cuenta.

> ⚠️ **No lo intente**
>
> Consultar el endpoint de otra entidad con sus credenciales, o pedirle a un contacto que consulte el suyo sin acuerdo formal, constituye acceso no autorizado a sistemas de información bajo la **Ley 53-07**. La intención defensiva no cambia esa calificación, y un hallazgo obtenido así no es utilizable.

Lo que sí corresponde hacer

1. **Complete el procedimiento interno.** La mayoría de los fallos de autorización aparecen ahí, y la remediación es la misma.
2. **Si su análisis sugiere que el riesgo también existe entre organizaciones**, documéntelo y compártalo con UNISHIELD, sin ejecutar ninguna prueba adicional.
3. **Cualquier verificación que involucre a dos entidades requiere acuerdo escrito previo** entre ambas partes, con alcance, ventana de tiempo, identificadores y manejo del resultado definidos antes de la primera petición.

> **SI YA DETECTÓ ALGO POR ACCIDENTE**
>
> No lo confirme con una segunda petición. Una consulta de verificación contra el endpoint ajeno es exactamente la conducta tipificada, y además contamina la evidencia. Documente lo que vio, no repita la petición y compártalo con UNISHIELD el mismo día. El manejo del incidente sigue siendo de su institución; UNISHIELD recibe el dato y lo lleva al foro de intercambio.

SECCIÓN V

¿Qué consumimos?

Shadow IT · shadow IA

V.1 · Qué sale de la red

PROCEDIMIENTO VERIFICADO · SIN COSTO

COORDINACIÓN PREVIA

▸ **Requiere:** acceso a los informes del firewall o proxy perimetral.

Qué encuentra: los servicios externos que el personal está usando, y cuánta información está saliendo hacia ellos.

Es el registro que su institución ya está generando. No requiere activar nada.

Si su firewall tiene control de aplicaciones o filtrado de URL, la ruta es la categoría, no el dominio: la mayoría de los fabricantes ya clasifica «IA generativa» y «SaaS no gestionado» como categorías propias, y eso evita depender de una lista de dominios que envejece.

ANTES DE EXTRAER ESTOS REGISTROS

El análisis del tráfico saliente puede identificar a personas. Antes de ejecutarlo:

- Verifique que exista política de uso aceptable vigente que informe al personal del monitoreo del tráfico de red, comunicada y aceptada.
- Coordine con el área de gestión humana y con el responsable de protección de datos si el análisis va a descender a nivel de usuario individual.
- Defina y documente el período de retención de los reportes que genere.

Analice por destino y por categoría, no por persona. El objetivo declarado de este canal es descubrir herramientas, no perfilar usuarios.

PROCEDIMIENTO

1. Extraiga, para los últimos noventa días: destino (FQDN o SNI), categoría, origen interno, número de sesiones y bytes salientes. Incluya las sesiones denegadas: un bloqueo repetido es una necesidad no atendida, y esa conversación también le corresponde a TI.
2. Ordene por orígenes internos distintos, no por número de sesiones. Diez mil conexiones de un equipo son una anécdota; cuarenta equipos distintos son adopción.
3. Ordene después por bytes salientes. Ese segundo orden responde la pregunta que de verdad importa: no qué herramientas se usan, sino cuánta información está saliendo hacia ellas.
4. Contraste con la lista semilla del Anexo para validar la clasificación del fabricante o cubrir lo que no venga categorizado.

DÓNDE ESTÁ ESE INFORME

Cada fabricante publica este informe con un nombre distinto. Busque el que cruce **destino, categoría, origen interno y volumen de tráfico saliente** en una sola vista, normalmente bajo los informes de aplicaciones, de navegación web o de tráfico por categoría. Si su plataforma no lo trae armado, la exportación cruda de sesiones con esos cinco campos y una hoja de cálculo bastan.

Confirme la ruta contra la documentación del fabricante y la versión de firmware que tenga en producción; cambian entre versiones.

NOTA DE MÉTODO

Cuente clientes distintos, no consultas: el número de orígenes internos distintos mide adopción, y es lo que decide si hay algo que gobernar.

CÓMO CONFIRMAR QUE FUNCIONÓ

Puede responder, con datos y no de memoria, cuántos equipos distintos de su red hablaron con un servicio externo no gestionado durante el último mes, y cuántos megabytes salieron hacia el que más recibió. Si aparece el destino pero no el volumen, el informe elegido no es el correcto.

Los puntos ciegos de este canal

Si los navegadores resuelven por DNS sobre HTTPS, el destino puede no aparecer en sus registros internos de resolución. Bloquee los endpoints conocidos de DoH y fuerce el uso de los resolutores internos por política de navegador.

Con la adopción creciente de Encrypted Client Hello, el SNI se degrada como fuente de visibilidad. La categorización por destino IP y por reputación mantiene utilidad, pero este canal perderá granularidad.

Si no dispone de un firewall con control de aplicaciones, el registro de consultas del DNS interno ofrece una vista parcial: verá qué se resolvió, pero no cuánto salió. **Sin estos controles, el inventario que produzca este procedimiento estará incompleto y no sabrá en qué medida.**

V.2 · Consentimientos OAuth

Es el mismo control de la Sección III.3, visto desde el ángulo de qué herramientas externas entraron. No se duplica aquí. Ver Sección III.3.

V.3 · Política de extensiones de navegador

PROCEDIMIENTO VERIFICADO · SIN COSTO

- **Requiere:** administración de directivas de grupo, Intune o la consola del navegador.

Este bloque es una recomendación de política, no un inventario. Inventariar cientos de extensiones no es sostenible; el control efectivo consiste en definir quién autoriza la instalación.

Los motores basados en Chromium (Chrome, Edge) comparten la misma API de gestión, y Firefox tiene equivalentes. Las políticas se despliegan por directiva de grupo (GPO), Intune/MDM, o la consola de administración del navegador.

Cuatro estrategias de control

No son una progresión de madurez: son complementarias, y una organización puede sostener la lista permitida, el flujo de aprobación y la protección por sitio al mismo tiempo.

Estrategia 1 · Bloquear todo salvo lo aprobado (default-deny)

`ExtensionInstallBlocklist` = `*` bloquea todas las extensiones, incluidas las ya instaladas, que se deshabilitan en el siguiente arranque. Luego `ExtensionInstallAllowlist` = IDs de las extensiones aprobadas.

Estrategia 2 · Flujo de solicitud

Habilite la solicitud de extensiones por parte del usuario con aprobación de TI. Sin este flujo, la estrategia de lista permitida genera resistencia y tiende a revertirse.

Estrategia 3 · Bloqueo por permiso

Si el default-deny no es viable, use `ExtensionSettings` con `blocked_permissions` para prohibir extensiones que pidan permisos peligrosos.

Estrategia 4 · Protección por sitio (de mayor impacto y menor uso)

`runtime_blocked_hosts` impide que cualquier extensión lea o modifique los sitios que usted especifique:

JSON · EXTENSIONSETTINGS

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.suinstitucion.com.do"]
  }
}
```

La protección por sitio como punto de partida recomendado: mantiene las extensiones operativas en el resto de la navegación y les impide leer o modificar los sistemas institucionales críticos. Protege los sistemas críticos sin prohibir herramientas de uso legítimo y sin desplazar la actividad hacia equipos personales, fuera del alcance de la institución.

Orden de evaluación de las políticas: Forcelist > Allowlist > Blocklist. Una extensión forzada prevalece siempre; una permitida se instala incluso con bloqueo general mediante `*`.

FUENTE OFICIAL

Chrome · support.google.com/chrome/a/answer/7532015 · chromeenterprise.google/policies
Edge · learn.microsoft.com/deployedge/microsoft-edge-manage-extensions-ref-guide
Guía de Google · "Managing Extensions in Your Enterprise"

Nota de verificación: las cuatro estrategias confirmadas contra documentación oficial de Google y Microsoft. `runtime_blocked_hosts` acepta hasta 100 entradas y soporta comodines de eTLD.

CÓMO CONFIRMAR QUE FUNCIONÓ

Con la política aplicada, abra uno de los sitios protegidos y revise la consola de la extensión: no debe poder leer ni modificar la página. Intente además instalar una extensión fuera de la lista permitida; debe quedar bloqueada.

V.4 · Tarjeta corporativa

PROCEDIMIENTO VERIFICADO · SIN COSTO

Requiere: el reporte de cargos de Compras y Finanzas. Ningún acceso técnico.

Qué se está buscando

Este canal no audita el gasto: audita el proceso. Un cargo recurrente a un servicio tecnológico que no pasó por evaluación de seguridad ni por el proceso formal de compras es un hallazgo de gobierno, no una conducta individual.

Solicite el dato a Compras y a Finanzas en ese orden de detalle:

1. **Descriptor de comercio, monto y recurrencia.** Responde qué se está pagando.
2. **Centro de costo.** Responde dónde vive la necesidad que llevó a contratarlo.
3. **Titular de la tarjeta.** Solo cuando haga falta para completar la regularización del servicio.

Los dos primeros niveles suelen bastar para dimensionar la adopción y para abrir la conversación con el área correspondiente. El tercero identifica a una persona y conviene reservarlo para cuando exista algo concreto que regularizar, porque el objetivo del ejercicio es incorporar el servicio al inventario y a la evaluación de seguridad, no señalar a quien lo contrató.

Un servicio descubierto por esta vía suele resolverse mejor migrándolo a una cuenta corporativa gestionada que cancelándolo: la cancelación empuja el uso hacia canales donde la institución ya no tiene visibilidad.

No requiere herramienta técnica. Pida a Finanzas 12 meses de cargos y reembolsos, filtre la columna de descriptor de comercio y cruce con centro de costo y titular. Busque descriptores como estos:

```
DESCRIPTORES DE COMERCIO

OPENAI · ANTHROPIC · PERPLEXITY · CURSOR · NOTION · GRAMMARLY
OTTER · FIREFLIES · CANVA · MAKE · ZAPIER
AWS · DIGITALOCEAN · VERCEL · NETLIFY
```

Posiblemente encontrará suscripciones nunca evaluadas, cargos de personas ya desvinculadas, y suscripciones de nivel personal (sin acuerdo de procesamiento de datos, con datos usados para entrenamiento).

No requiere fuente externa; corresponde a un procedimiento administrativo.

PLANTILLAS

Para llenar

Inventario de credenciales de API

CREDENCIAL (ID PARCIAL)	DUEÑO INTERNO	CONTRAPARTE EXTERNA	ÚLTIMO USO	SEVERIDAD	RESPONSABLE	FECHA OBJETIVO	EVIDENCIA DE CIERRE

Triaje de herramientas descubiertas

HERRAMIENTA	CANAL DE DESCUBRIMIENTO	ORÍGENES DISTINTOS	CUENTA PERSONAL / EMPRESARIAL	SEVERIDAD	RESPONSABLE	FECHA OBJETIVO	EVIDENCIA DE CIERRE

Evidencia de cierre: el artefacto que permite dar el punto por cerrado en comité —captura de la credencial deshabilitada, ticket de rotación, acta de la excepción aprobada. **Revisión:** máximo 6 meses.

PLANTILLAS

Referencia de severidad

Orientativa, para llenar la columna de severidad de las dos plantillas sin abrir una discusión en cada fila. Ajústela al criterio de clasificación que ya tenga su institución.

HALLAZGO	SEVERIDAD	ACCIÓN
Secreto válido en repositorio	CRÍTICA	Rotación inmediata
API expuesta sin dueño	ALTA	Asignar responsable y revisar exposición
Consentimiento OAuth sobreprivilegiado	ALTA	Revocar o reducir permisos
Extensión con acceso a sistemas críticos	ALTA	Restringir o remover
Credencial activa sin uso	MEDIA-ALTA	Deshabilitar de forma controlada
Servicio externo no autorizado	SEGÚN LOS DATOS QUE TRATE	Evaluar y regularizar

Autorización interna del ejercicio

Reglas de enfrentamiento. Requerida antes de ejecutar III.4 y IV.2. Una página, firmada, archivada con el resultado del ejercicio.

Sistemas incluidos (nombre, entorno, URL o rango)

Ventana de tiempo autorizada (fecha y hora de inicio y cierre)

Herramientas autorizadas (nombre y versión)

Participantes (nombre, área, rol en el ejercicio)

Manejo de resultados (dónde se almacenan, quién accede, cuándo se destruyen)

Exclusiones expresas (sistemas o entornos fuera de alcance)

Responsable de tecnología · firma y fecha

Responsable del ejercicio · firma y fecha

ANEXO

Lista semilla de dominios

Respaldo para validar la clasificación del firewall en la Sección V.1, o para cubrir lo que su plataforma no venga categorizando. Agrupada por categoría; los comentarios (`# ...`) marcan cada grupo.

DOMINIOS-SEMILLA.TXT

```
# Asistentes
openai.com  chatgpt.com  claude.ai  anthropic.com  gemini.google.com
perplexity.ai  deepseek.com  mistral.ai  copilot.microsoft.com  poe.com

# APIs y plataformas de modelos
api.openai.com  api.anthropic.com  openrouter.ai  together.ai
groq.com  replicate.com  fal.ai  huggingface.co  ollama.com

# Desarrollo y automatización
cursor.com  replit.com  v0.dev  lovable.dev  windsurf.com
bolt.new  n8n.io  langflow.org  make.com  zapier.com

# Reuniones y transcripción
otter.ai  fireflies.ai  fathom.video  tldv.io  granola.ai
tactiq.io  read.ai  supernormal.com  krisp.ai

# Contenido y productividad
jasper.ai  copy.ai  grammarly.com  midjourney.com
runwayml.com  elevenlabs.io  gamma.app  notion.so  canva.com
```

CIERRE

Encontró algo. ¿Ahora qué?

Reporte cualquier hallazgo relevante para el ecosistema: un activo heredado expuesto, una credencial comprometida, una falla de autorización en una integración, un indicador que no reconozca.

CORREO

ciberseguridad@mail.unishield.com.do

HUELLA PGP

NUESTROS COMPROMISOS CON QUIEN REPORTA

Manejo no punitivo

Un reporte no es una confesión. UNISHIELD no evalúa, califica ni escala el nivel de madurez de la institución que reporta, ni ante el regulador ni ante los demás miembros. Un ecosistema donde reportar es costoso es un ecosistema donde nadie reporta.

Sin atribución por defecto

Todo hallazgo que se comparta con los demás miembros circula anonimizado. La institución de origen se identifica solo si ella misma lo autoriza por escrito.

Circulación sin atribución, no intervención

Si el hallazgo involucra a otra entidad del ecosistema, UNISHIELD lo hace circular por el canal de intercambio sin revelar el origen del reporte. UNISHIELD no interviene en sistemas de terceros, no coordina la divulgación ni remedia por cuenta de nadie: la acción corresponde a cada institución sobre sus propios activos.

> **ESCRÍBANOS TAMBIÉN CUANDO NO ENCUENTRE NADA**
>
> El dato agregado de cuántas instituciones revisaron sus activos heredados este trimestre es, hoy, información que no existe. Construirla es parte de lo que hace un ISAC sectorial.

Control documental

CÓDIGO	UNISHIELD-GE-2026-01
VERSIÓN	2.0
FECHA DE EMISIÓN	Agosto de 2026
CLASIFICACIÓN	TLP:GREEN
ELABORADO POR	Centro de Inteligencia de Amenazas Cibernéticas · UNIPAGO
PRÓXIMA REVISIÓN	Febrero de 2027, o antes si cambia una ruta verificada

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	CAMBIO
1.0	Agosto 2026	Primera edición.
2.0	Agosto 2026	Sección I nueva. II.1 reordenada a crt.sh. V.1 pasa del DNS al firewall. Correcciones en III.1, III.3, III.4 y IV.2. Taxonomía de hallazgos, referencia de severidad y autorización interna del ejercicio.