BRANDEFENSE COUNTRY REPORT · PERU 2026

Brandefense Informe del panorama de ciberamenazas de Perú 2026

Comercio de identidades, acceso de proveedores y decisiones para proteger la confianza pública

Odin by Brandefense
Periodo de investigación: 22 de noviembre de 2026
Versión 1.0 · Public Research Edition · TLP:CLEAR · 23 de noviembre de 2026. Periodo de investigación: 1 de enero–22 de noviembre de 2026

250
dominios candidatos seleccionados en diez grupos sectoriales combinados

9
casos de afirmaciones ilustrados mediante diez fichas de publicaciones

5
casos públicos con evidencia y unidades de incidente diferentes

58
entradas de ransomware sobre Perú, cada una una afirmación delictiva

CONTENIDO

Contenido

Translated with AI

Esta edición se ha traducido con IA a partir del texto original en inglés. En caso de diferencia, prevalece la edición en inglés.

01	Resumen ejecutivo	05
	Mapa del informe	09
02	El contexto digital y de amenazas de Perú	10
03	Exposición nacional: la selección de organizaciones	14
04	Actividad clandestina e interpretación de afirmaciones	22
05	Incidentes públicos y respuesta por sector	39
06	Mensajes no autorizados, afirmaciones de acceso y disponibilidad de servicios	46
07	Actores, ransomware y relaciones respaldadas	50
08	Economía del fraude: identidad, persuasión y pagos	60
09	Banca y protección del cliente	64
10	Respuesta regulatoria y decisiones de notificación	69
11	Perspectivas y supuestos condicionales de planificación	73
12	Plan de acción de 30/60/90 días	77
A	Apéndice A. Alcance, evidencia y confianza	84
B	Apéndice B. Registro de evidencia de publicaciones	87
C	Apéndice C. Fuentes	88
D	Apéndice D. Glosario en lenguaje sencillo	91
	Acerca de este informe	93

Directorio y ejecutivos	01 05 11 12
CISO y responsables de seguridad	03 04 06 07 12
Equipos SOC y de identidad	04 07 B
Fraude y protección del cliente	05 08 09
Asesoría legal y comunicaciones	05 06 10 12

Sobre esta edición

Traducido con IA. Esta edición se tradujo del original en inglés. En caso de discrepancia, prevalece la edición en inglés.

La evidencia sobre Perú reúne anuncios de datos de identidad, afirmaciones de extorsión y distintos reportes públicos de seguridad. Valide cada afirmación antes de contener cuentas, proteger a los clientes o recuperar servicios.

99 532

publicaciones etiquetadas como Perú; la asociación con el país no demuestra un incidente

58

entradas de ransomware del periodo solicitado; afirmaciones delictivas

14

casos: nueve afirmaciones del entorno clandestino y cinco reportes públicos

4

decisiones para directivos, con responsables y evidencia de cumplimiento

Contenido y rutas de lectura

Capítulo	Pregunta
1 Resumen ejecutivo	¿Qué decisiones deben tomarse primero?
2 Contexto	¿Qué condiciones de operación en Perú orientan la respuesta?
3 Exposición nacional	¿Qué se ha medido y qué información no está disponible?
4 Actividad clandestina	¿Qué demuestran las afirmaciones conservadas?
5 Sectores y casos públicos	¿Qué reportes públicos cambian una decisión concreta?
6 Disponibilidad e integridad de mensajes	¿Qué efecto sobre el servicio y qué participación están establecidos?
7 Actores y ransomware	¿Qué respalda cada etiqueta y relación?
8 Economía del fraude	¿Cómo separar los riesgos de identidad y de pagos?
9 Banca	¿Qué decisiones de protección y supervisión se desprenden?
10 Regulación	¿Qué obligaciones rigen y qué cambios llegarán después?
11 Perspectivas	¿Qué modificaría los supuestos de planificación?
12 Plan de acción	¿Quién actúa y cómo demuestra el cumplimiento?
Anexos A–D	Alcance, evidencia, fuentes y definiciones

CAPÍTULO 01

Resumen ejecutivo

01

ESTE CAPÍTULO RESPONDE

¿Qué hallazgos justifican decisiones inmediatas para las organizaciones peruanas?

4

decisiones para directivos vinculadas a evidencia y criterios de cumplimiento

Cuatro decisiones para directivos 07

El año en cifras 07

CAPÍTULO 01

Resumen ejecutivo

EN RESUMEN

La evidencia respalda validar cuentas, supervisar proveedores, proteger clientes y probar la continuidad. Ransompedia registra 58 entradas; las publicaciones clandestinas ofrecen identidades y acceso. Los reportes públicos distinguen uso indebido de cuentas de proveedores, acceso a información, transferencias cuestionadas y suplantación. Las publicaciones de noviembre no siempre describen datos recién obtenidos. Establezca una ruta de alertas, valide cuentas y registros propios, ensaye una alternativa para un servicio crítico y asigne responsables de notificación y comunicación.

Este informe combina evidencia propia de publicaciones conservadas y entradas de ransomware de Brandefense con información pública leída en sus fuentes. Separa publicaciones, anuncios, entradas, eventos públicos, denuncias y observaciones de dominios. Estas poblaciones no se suman para construir un total nacional de ataques. [S1][S2]

La fecha de corte solicitada es el 22 de noviembre. La recopilación se realizó mientras ese día seguía en curso; la evidencia refleja lo disponible al momento de comprobarla. Publicación, obtención, detección, recuperación del servicio y seguimiento regulatorio pueden tener fechas distintas.

1. El volumen de publicaciones no demuestra un total nacional de incidentes. La población etiquetada por país contiene 99 532 publicaciones. Nueve casos seleccionados examinan registros, documentos y presuntos accesos. Una conversación de enero identifica material anterior, sin demostrar de forma independiente cuándo se obtuvo ni la identidad del archivo. Valide relevancia y antigüedad antes de declarar un incidente nuevo. [S1]

2. La extorsión visible abarca varias etiquetas y puede repetir organizaciones. Ransompedia registra 58 entradas sobre Perú, frente a 26 de todo 2025. Se compara un año parcial con uno completo; no es una tasa de crecimiento. Qilin, The Gentlemen y Nova reúnen 28 de las 58 entradas. Cada entrada sigue siendo una afirmación delictiva. [S2]

3. Los reportes públicos justifican distintas decisiones de contención y protección. Los cinco casos públicos incluyen uso indebido de una cuenta de proveedor, acceso a información de clientes de una aseguradora y transferencias reportadas como no autorizadas. También incluyen una alerta de suplantación y un operativo. No son cinco intrusiones de red confirmadas. La respuesta debe seguir la función y la evidencia establecidas. [S17][S18] [S23][S20][S22]

4. La actividad reciente incluye afirmaciones, desmentidos e investigaciones sobre observaciones anteriores. La quincena final incluye anuncios de registros empresariales, datos educativos e historiales laborales, además de tres entradas de ransomware. Una publicación de un proveedor de noviembre analiza intentos de malware anteriores en varios países. Conserve la fecha y el tipo de evidencia de cada elemento. [S1][S2][S27][S32]

5. La exposición y las notificaciones necesitan denominadores y plazos propios. La selección contiene 250 dominios candidatos. Se anunció una credencial para la venta para 68 candidatos al comprobarlos; esto no establece acceso utilizable. Las obligaciones sobre datos personales, servicios digitales y actividad financiera tienen

desencadenan-
tes y destinatarios distintos. Asigne responsables de validación y notificación antes de un incidente. [S3][S5][S6][S7]

Cuatro decisiones para directivos

1. **Establezca la ruta de alertas y valide la evidencia propia.** Confirme que las alertas pertinentes sobre cuentas y datos lleguen a un equipo identificado. Valide titularidad, estado, privilegios y medidas previas antes de decidir la contención (§3–4, §12).
2. **Pruebe los privilegios de proveedores y el servicio mínimo seguro.** Demuestre quién puede suspender una cuenta de proveedor, emitir una corrección confiable y mantener una tarea crítica cuando el servicio normal no está disponible (§5–6, §12).
3. **Mantenga la protección de clientes y pagos durante la recuperación técnica.** Verifique de forma independiente los cambios de beneficiario y de recuperación de cuentas. Ofrezca a los clientes una vía legítima para comprobar solicitudes sospechosas (§8–9).
4. **Separe las decisiones de notificación y conserve los momentos de conocimiento.** Determine el alcance en datos personales, servicios digitales y actividad financiera. Distinga las normas vigentes de las propuestas en consulta y las disposiciones con vigencia posterior (§10).

El año en cifras

99 532

Publicaciones etiquetadas como Perú en el periodo solicitado, por fecha de publicación

QUÉ NO MIDE

Ataques dirigidos confirmados, ofertas únicas o incidentes nacionales

58

Entradas de ransomware sobre Perú en el periodo solicitado

QUÉ NO MIDE

Cifrado comprobado, organizaciones únicas o pérdidas

26

Entradas sobre Perú en todo 2025

QUÉ NO MIDE

Una base del mismo periodo

28 de 58

Entradas con las etiquetas Qilin, The Gentlemen y Nova

QUÉ NO MIDE

Operadores, tasas de éxito o pagos realizados

3

Entradas fechadas entre el 8 y el 22 de noviembre

QUÉ NO MIDE

Tres intrusiones nuevas confirmadas de forma independiente

9 / 10

Casos clandestinos ilustrados / fichas de publicaciones anonimizadas

QUÉ NO MIDE

Nueve intrusiones confirmadas o diez eventos independientes

5	250	15
Casos públicos, incluidas alertas y un operativo	Dominios candidatos seleccionados intencionalmente	Observaciones de registros de tarjetas en las publicaciones revisadas
QUÉ NO MIDE	QUÉ NO MIDE	QUÉ NO MIDE
Cinco intrusiones de red confirmadas	Personas jurídicas independientes, una clasificación por ingresos o prevalencia nacional	Validez, titularidad o uso verificados; exposición nacional de tarjetas o pérdidas por fraude

Fuentes: evidencia de publicaciones conservadas [S1], Ransompedia [S2] y alcance de observación de la selección [S3]. La cifra de tarjetas corresponde a una población limitada de publicaciones, no a una estimación de exposición nacional.

CONCLUSIONES CLAVE

01

Valide la afirmación concreta sobre una cuenta, datos o un servicio antes de declarar impacto.

02

Entradas, reportes públicos y casos de publicaciones son poblaciones distintas.

03

Asigne responsables de acceso de proveedores, protección de clientes, continuidad y notificación de manera conjunta.

Mapa del informe

Doce capítulos y cinco rutas de lectura. Cada capítulo comienza con una pregunta de decisión y termina con tres conclusiones prácticas.

Directorio y ejecutivos	Financiar la validación y la recuperación de servicios	01 05 11 12
CISO y responsables de seguridad	Priorizar evidencia propia y dependencias	03 04 06 07 12
Equipos SOC y de identidad	Comprobar afirmaciones de acceso y contexto de dispositivos	04 07 B
Fraude y protección del cliente	Verificar solicitudes y reducir daños posteriores	05 08 09
Asesoría legal y comunicaciones	Conservar cronología, alcance y decisiones de notificación	05 06 10 12

Las etiquetas de evidencia son **observación**, **afirmación del actor**, **reporte oficial** e **inferencia analítica**. Un anuncio observado sigue siendo una afirmación sobre su contenido. Un reporte oficial puede confirmar un evento y dejar sin resolver al actor, la vía de acceso o la población afectada.

CAPÍTULO 02

El contexto digital y de amenazas de Perú

02

ESTE CAPÍTULO RESPONDE

¿Qué condiciones de operación cambian la respuesta a la evidencia del informe?

84,2%

penetración de internet en el panorama de octubre de 2026

2.1 Una población conectada depende de varios servicios de identidad 11

2.2 Separe la institución, el servicio y su proveedor 11

2.3 El contexto político no determina la atribución 12

2.4 Los pares regionales aportan contexto, no una clasificación de seguridad 12

2.5 La responsabilidad de notificar forma parte de la preparación operativa 12

CAPÍTULO 02

El contexto digital y de amenazas de Perú

EN RESUMEN

Perú combina un uso extendido de servicios digitales con distintas responsabilidades de seguridad. La información de identidad, el acceso a servicios públicos y las operaciones financieras aparecen en poblaciones de evidencia diferentes. Una interrupción web, una venta ilegal de datos y un uso indebido de cuentas confirmado exigen decisiones distintas. Las comparaciones regionales describen visibilidad; el marco legal separa incidentes de datos personales y servicios digitales. Identifique el servicio, el proveedor de identidad, el custodio de datos y el responsable de notificación antes de contener.

2.1 Una población conectada depende de varios servicios de identidad

El panorama de octubre de 2026 de DataReportal señala 29,5 millones de usuarios de internet y 84,2% de penetración. También indica 39,6 millones de conexiones móviles y 32,7 millones de identidades de usuarios en redes sociales. Las conexiones y las identidades sociales no equivalen a personas únicas. El editor advierte sobre la comparabilidad entre ediciones. [S4]

Para los defensores, estas cifras son contexto. No miden ciberdelincuencia, cuentas afectadas ni el alcance de un anuncio concreto. No se puede dividir una oferta de base de datos etiquetada por país entre los usuarios de internet para estimar el porcentaje de población afectada.

La dependencia práctica está entre la persona, los servicios que la reconocen y los canales para recuperar el acceso. Un registro de identidad divulgado podría servir en una suplantación posterior sin dar acceso a la institución original. Es un modelo analítico de riesgo, no un hallazgo de que los registros examinados causaron un fraude concreto.

Por eso, las organizaciones deberían identificar tanto la recuperación como la autenticación normal. Determine qué personal puede cambiar un teléfono, aprobar un beneficiario nuevo, recuperar una cuenta privilegiada o emitir una credencial de reemplazo. Compruebe cómo se verifican y registran esas acciones de forma independiente.

2.2 Separe la institución, el servicio y su proveedor

El registro de incidentes distingue los sistemas internos de una institución, una cuenta de proveedor, un canal público de comunicación y el servicio dirigido al cliente. La evidencia sobre uno no demuestra acceso a los demás.

Una cuenta de administrador de un servicio público anunciada exige validación por los responsables del servicio y de identidad. Un documento que menciona a un prestador de salud requiere comprobar titularidad y procedencia. Una alerta empresarial sobre un video falso de inversión exige protección del cliente y respuesta de marca. Su asociación con Perú no crea una cadena de intrusión común.

Esta distinción importa al coordinar proveedores. Una organización puede ser responsable del mensaje público y depender de otro para identidad, alojamiento o distribución. El ejercicio de recuperación debería establecer quién puede suspender una cuenta del proveedor y quién puede autorizar una reapertura segura.

2.3 El contexto político no determina la atribución

Este informe no toma posición sobre las elecciones generales, las sucesiones presidenciales, el Congreso, los partidos, los candidatos, las protestas ni las decisiones del Gobierno. Tampoco toma posición sobre las relaciones de Perú con Chile o Bolivia. Esos asuntos no establecen la identidad ni la motivación de un atacante.

Una referencia política en una publicación es el encuadre de su autor. La etiqueta de idioma no demuestra nacionalidad. Una caída durante un evento público no demuestra interferencia deliberada; una afirmación delictiva no demuestra un efecto sobre una elección.

La respuesta debería aplicar el mismo estándar de evidencia a todas las afiliaciones políticas. Conserve el registro del servicio, indique lo confirmado, describa lo no resuelto y asigne la siguiente comprobación. Omita insultos y llamados al reclutamiento al describir material de actores.

2.4 Los pares regionales aportan contexto, no una clasificación de seguridad

La comparación utiliza Chile, Colombia, Ecuador y Bolivia. Chile y Ecuador aportan contexto regional del Pacífico; Colombia añade una comparación andina de servicios digitales de mayor tamaño; Bolivia aporta una población visible menor de un país vecino. La selección no implica un bloque político ni economías equivalentes.

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

Los recuentos de entradas del capítulo 7 son descriptivos. Los países difieren en población, composición sectorial, prácticas de divulgación y fuentes visibles para el servicio. Ningún recuento observado establece una probabilidad de ataque ni clasifica la capacidad defensiva nacional.

El mismo límite se aplica a las publicaciones. Un vendedor internacional puede anunciar el mismo servicio para muchos países. Sin evidencia de incidentes que lo respalde, un cambio de volumen asociado a un país no demuestra un cambio equivalente en intrusiones exitosas.

2.5 La responsabilidad de notificar forma parte de la preparación operativa

El reglamento del Marco de Confianza Digital entró en vigencia durante el periodo del estudio. La notificación de datos personales y la supervisión financiera tienen alcances y desencadenantes distintos. El capítulo 10 distingue las obligaciones y sus fechas de vigencia. [S5][S6][S7]

Utilice un registro compartido para los hechos, pero documente por separado cada decisión de notificación. Conocimiento, detección, publicación y recuperación pueden ocurrir en fechas diferentes. Un incidente puede requerir asistencia técnica, evaluación de privacidad, comunicación al cliente y denuncia policial sin convertirse en varias intrusiones.

Para el directorio, importa si la organización puede decidir antes del plazo aplicable. Para el responsable del servicio, importa si puede mantener un servicio mínimo seguro durante la investigación. Para el analista, importa si cada conclusión conserva su etiqueta de evidencia al llegar al resumen.

CONCLUSIONES CLAVE

01

Conexiones, cuentas, registros y personas tienen denominadores diferentes.

02

El acceso de proveedores y los mensajes públicos necesitan responsables propios de respuesta.

03

El contexto político y la comparación regional no establecen atribución ni clasificaciones de riesgo nacional.

CAPÍTULO 03

Exposición nacional: la selección de organizaciones

ESTE CAPÍTULO RESPONDE

¿Qué observaciones están disponibles y cuáles requieren validar activos propios?

250

dominios candidatos seleccionados en diez grupos sectoriales combinados

3.1 Ficha de la población 15
3.2 Resultados de exposición disponibles 16
3.3 Conserve qué afirmación se comprobó al validar credenciales 18
3.4 Cada control de correo y web necesita su propio denominador 18
3.5 Una alerta preventiva de software no es un recuento de incidentes 20
3.6 Límites de integración e interpretación 21

CAPÍTULO 03

Exposición nacional: la selección de organizaciones

EN RESUMEN

La selección contiene 250 dominios candidatos elegidos intencionalmente. No es una muestra de prevalencia nacional ni una clasificación por ingresos. Deben validarse titularidad, servicios relacionados e independencia jurídica. Se anunció una credencial para 68 de los 250 candidatos; el acceso actual requiere validación. Trate las observaciones no disponibles como desconocidas y use alertas validadas y registros locales para decidir si corresponde contener.

3.1 Ficha de la población

Elemento	Definición
Población seleccionada	250 dominios candidatos en 10 grupos sectoriales combinados
Selección	Relevancia para servicios públicos y cobertura sectorial; sin clasificación por ingresos
Celdas previstas	25 candidatos por grupo; las observaciones publicadas requieren un denominador utilizable
Unidad	Dominio candidato, que puede representar un servicio relacionado o una organización multinacional
Independencia	La titularidad jurídica y la independencia entre entidades siguen sin validarse
Observación de exposición	Las ofertas vigentes y las asociaciones acumuladas de dominios necesitan su propia fecha
Representatividad	Los resultados no estiman prevalencia nacional ni probabilidad sectorial de incidentes
Calificaciones	Solo puede publicarse una cifra principal nacional de Atlas validada

Los sectores abarcan administración central y regional, finanzas y seguros, universidades e investigación, energía y agua, minería y materiales, transporte y logística, servicios de consumo, salud, y comunicaciones, agricultura e industria. Las categorías operativas menores se agrupan. La distribución de candidatos no es un resultado de seguridad medido.

3.2 Resultados de exposición disponibles

En la comprobación del 22 de noviembre, 68 de los 250 dominios candidatos seleccionados tenían una credencial anunciada para la venta. Es una oferta anunciada, no acceso actual verificado. Los dominios requieren validar titularidad e independencia antes de llegar a conclusiones por organización. [S3]

Cifra principal nacional de Atlas para la cartera seleccionada



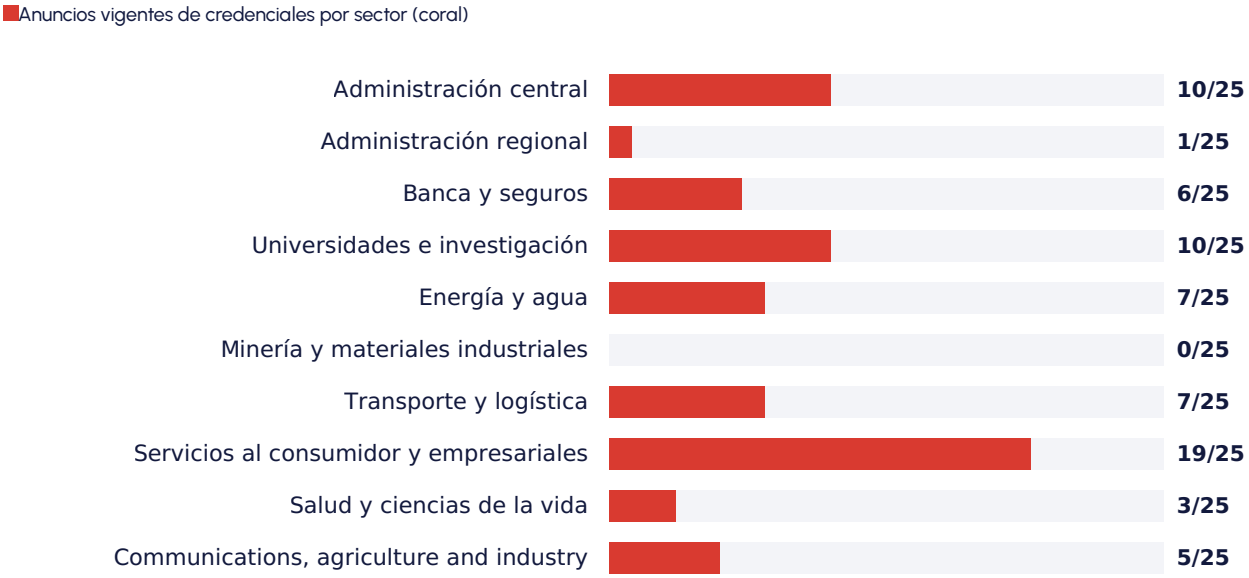
49/100 resume esta cartera seleccionada, no la probabilidad nacional de ataque ni la incidencia. Fuente: Odin by Brandefense, 250 dominios candidatos seleccionados, 22 de noviembre de 2026 [S3]. Las asociaciones pueden solaparse e incluir observaciones anteriores.

La cifra principal nacional de Atlas para esta cartera seleccionada es 49/100. Resume la exposición de la cartera; no es una probabilidad nacional de ataque ni una tasa de incidencia. No se publica ninguna calificación sectorial ni por organización. [S3]

Observación de la cartera	Conteo	Interpretación
Dominios con asociaciones de equipos	231	No verifica titularidad de equipos de la organización
Asociaciones de equipos	747 185	Al menos esta cantidad de asociaciones acumuladas; puede haber solapamiento
Dominios con asociaciones de equipos etiquetadas como de empleados	208	Etiqueta de función de la fuente, no empleo validado
Asociaciones de equipos etiquetadas como de empleados	83 414	Asociaciones solapadas, no personal único
Dominios con asociaciones de registros de credenciales	233	La pertinencia histórica y actual requiere validación
Asociaciones de registros de credencia-les	4 429 470	No son cuentas ni personas únicas
Asociaciones de documentos	887	No establece que cada documento sea confidencial
Asociaciones de posibles dominios simi-lares	13 105	No son phishing ni abuso de marca veri-ficados

Las cifras son asociaciones de dominios, no equipos, cuentas, documentos ni personas únicas. Los conteos pueden solaparse entre registros y dominios relacionados. No constituyen una población de incidentes exclusivamente de 2026. La instantánea se reunió el 22 de noviembre; algunos periodos de asociación terminan el 18 de noviembre. Los posibles dominios similares cubren del 19 de octubre al 18 de noviembre. [S3]

Los conteos sectoriales de señales requieren validación y no constituyen calificaciones sectoriales de riesgo



Dominios candidatos con credenciales anunciadas / candidatos seleccionados. No se verifica acceso actual ni se publica una calificación sectorial de riesgo. Fuente: Odin by Brandefense, 250 dominios candidatos seleccionados, 22 de noviembre de 2026 [S3]. Las asociaciones pueden solaparse e incluir observaciones anteriores.

Grupo sectorial seleccionado	Candidatos	Credencial anunciada para la venta	Dominios con asociaciones de equipos	Asociaciones de registros de credenciales
Administración central	25	10	25	143 467
Administración regional	25	1	25	13 489
Banca y seguros	25	6	24	87 730
Universidades e investigación	25	10	25	3 815 424
Energía y agua	25	7	22	39 841
Minería y materiales industriales	25	0	20	54 536
Transporte y logística	25	7	24	35 352
Servicios al consumidor y empresariales	25	19	24	68 087
Salud y ciencias de la vida	25	3	19	32 363
Comunicaciones, agricultura e industria	25	5	23	139 181

Cada celda sectorial contiene 25 candidatos. Los conteos descargables de ofertas describen dominios candidatos con credenciales anunciadas, no organizaciones en venta ni acceso vigente verificado. Las etiquetas de empleo proceden de la fuente y no acreditan una relación laboral. Los grupos dividen dominios seleccionados, no entidades jurídicas validadas independientemente. Sus conteos de señales no establecen prevalencia sectorial ni una clasificación comparativa de riesgo. [S3]

Estas poblaciones responderían preguntas diferentes. Una oferta vigente indica que se anuncia un acceso. Una asociación histórica puede corresponder a una cuenta antigua o ya atendida. Una asociación de dispositivo no demuestra empleo, titularidad ni acceso a sistemas internos de la organización.

Cuando llegue una alerta pertinente, valide primero el activo y la cuenta. Confirme que el servicio pertenece a la organización, determine si la cuenta corresponde a personal, proveedor, estudiante o cliente, y revise su estado. Evite convertir una asociación de dominio en un incidente de empleado comprobado.

3.3 Conserve qué afirmación se comprobó al validar credenciales

Un registro útil separa cuatro preguntas: si el material corresponde a un servicio propio, si la cuenta sigue activa, si hubo uso no autorizado y si las medidas previas ya lo atendieron. Responder una no responde las demás.

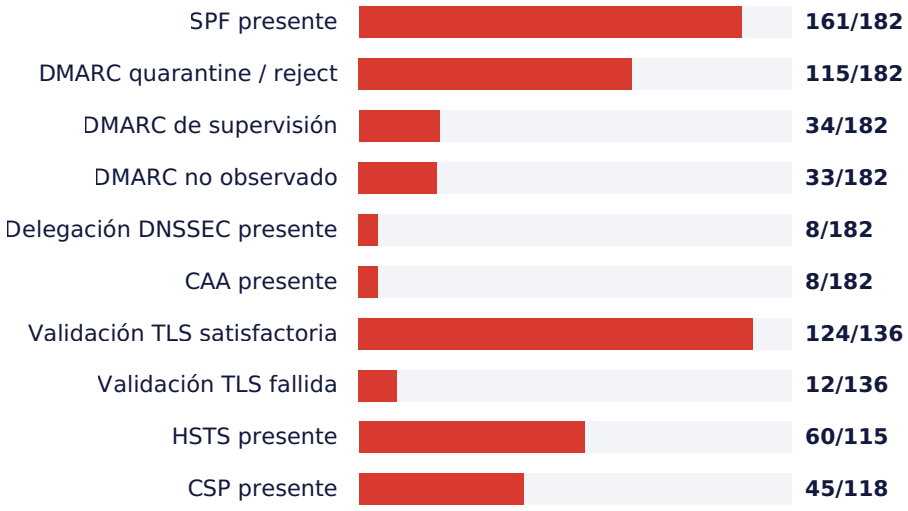
Para una cuenta privilegiada vigente, el equipo de identidad debería revisar inicios de sesión, permisos de sesión, métodos de autenticación añadidos y cambios administrativos. La contención debe seguir la evidencia validada. Antes de reabrir, compruebe que el acceso revocado ya no funciona; no dependa solo de una constancia de cambio de contraseña.

Para material histórico o ajeno, registre el motivo y cierre la alerta con el alcance adecuado. Una resolución histórica documentada sirve más que una declaración de vulneración sin límites. Los casos no resueltos necesitan responsable y momento de revisión.

3.4 Cada control de correo y web necesita su propio denominador

Véase el Apéndice D para las definiciones de SPF, CAA y TLS.

Las observaciones pasivas de controles utilizan denominadores disponibles separados



Fuente: observaciones pasivas, 22 de noviembre de 2026 [S3]. Los denominadores disponibles varían por observación; las políticas no demuestran eficacia.

Los 250 dominios candidatos aportaron observaciones pasivas para 183; 67 no tienen un resultado de dominio utilizable. Los resultados DNS son utilizables para 182 y uno está incompleto. Estas poblaciones describen la cartera seleccionada al 22 de noviembre, no la prevalencia nacional de controles. La titularidad del dominio y la identidad independiente de la organización siguen sin validarse. [S3]

Observación	Conteo observado	Denominador disponible
Registro SPF presente	161	182
Política DMARC de cuarentena o rechazo	115	182
Política DMARC de monitoreo	34	182
Sin política DMARC observada	33	182
Registro de delegación DNSSEC presente	8	182
Registro CAA presente	8	182
Validación del certificado TLS satisfactoria	124	136
Validación del certificado TLS fallida	12	136
HSTS presente en una respuesta HTTPS disponible	60	115
Content Security Policy presente en una respuesta web disponible	45	118

Fuente: Odin by Brandefense [S3]. Las categorías DMARC suman 182. TLS tiene 136 resultados determinados y 47 desconocidos entre los 183 dominios observados. Hay respuestas web disponibles para 118 dominios, incluidas 115 respuestas HTTPS. Las respuestas no disponibles son desconocidas, no controles ausentes.

Una validación fallida del certificado es una observación que requiere comprobación propia, no un hallazgo de intrusión. Una política de correo publicada no establece una alineación correcta de todos los remitentes. Una delegación DNS o una cabecera web no establece la calidad completa de implementación ni la seguridad de la aplicación.

Revise los remitentes autorizados antes de endurecer la política de correo. Valide los hallazgos de certificados frente al servicio previsto y la cadena de confianza soportada. Pruebe los cambios de políticas web frente a los procesos legítimos de la aplicación. Conserve un responsable y un motivo para cada resultado no disponible, sin contarlo como falla de seguridad.

La autenticación de correo, la validez de certificados y las cabeceras web son observaciones de configuración. No miden éxito del phishing ni robo de información. Una observación ausente no demuestra un control ausente; una página inicial que responde no demuestra disponibilidad completa del servicio. [S3]

Para correo, el responsable debería inventariar remitentes legítimos y probar la alineación antes de cambiar la aplicación de políticas. Para certificados, confirme el servicio, la cadena de confianza y el despliegue. Para controles web, verifique el comportamiento efectivo de la aplicación y sus dependencias.

La revisión local sigue siendo útil cuando el conjunto externo es incompleto. La organización puede probar directamente rutas de correo autorizadas y funciones del servicio. El informe nacional no debería reemplazar esos resultados por una clasificación sectorial inferida de dominios seleccionados.

3.5 Una alerta preventiva de software no es un recuento de incidentes

El diario oficial informa de una alerta preventiva del CNSD sobre PHP, emitida el 21 de octubre y descrita el 26 de octubre. La cantidad de instituciones destinatarias no demuestra explotación ni organizaciones afectadas. Los responsables deberían revisar los despliegues reales. [S11]

Ambas vulnerabilidades de PHP citadas tienen registros en NVD. Los avisos del fabricante identifican las versiones afectadas y corregidas de sus respectivas ramas compatibles. Son hechos globales de vulnerabilidades, no evidencia de explotación en Perú. [S12][S13][S14][S15]

Vulnerabilidad	Rama	Versiones afectadas	Versión corregida del fabricante
CVE-2026-109618 y CVE-2026-109619	8.2	Anteriores a 8.2.35	8.2.35
Las mismas dos vulnerabilidades	8.3	Anteriores a 8.3.36	8.3.36
Las mismas dos vulnerabilidades	8.4	Anteriores a 8.4.27	8.4.27
Las mismas dos vulnerabilidades	8.5	Anteriores a 8.5.12	8.5.12

Compruebe la versión que realmente se ejecuta después de corregir. Para software de un distribuidor o fabricante de equipos, siga el aviso aplicable y su ruta de actualización compatible. Cambiar un paquete sin comprobar el despliegue no demuestra que el servicio esté corregido.

3.6 Límites de integración e interpretación

Toda observación posterior de exposición debe conservar su fecha y denominador. Los registros acumulados deben quedar separados del periodo del informe por fecha de publicación. Dominios relacionados y registros superpuestos no deben convertirse en totales de personas únicas u organizaciones independientes.

Los recuentos sectoriales de señales pueden orientar la revisión; la cifra principal nacional de Atlas aporta un resumen diferente de la selección. Este informe no publica calificaciones sectoriales ni individuales. Si hubiera respaldo para un índice de higiene pasiva, se identificaría como índice analítico, no como resultado de Atlas.

Mantenga separadas las tareas de validación de cuentas, investigación de dispositivos, protección del cliente, revisión de documentos y corrección de configuraciones. Cada una necesita equipo responsable, evidencia y criterio de cierre. Un total agregado no determina qué sistema individual debe desconectarse.

CONCLUSIONES CLAVE

01

La selección es una población descriptiva de dominios.

02

Las observaciones de exposición no disponibles son desconocidas, no cero.

03

Valide titularidad, estado de la cuenta y uso real antes de elegir una contención que interrumpa servicios.

CAPÍTULO 04

Actividad clandestina e interpretación de afirmaciones

ESTE CAPÍTULO RESPONDE

¿Qué demuestran las publicaciones conservadas y qué afirmaciones todavía necesitan validación?

9

casos de afirmaciones ilustrados mediante diez fichas de publicaciones

4.1 Ficha de la población 23

4.2 Una controversia visible sobre material reutilizado 27

4.3 Acceso anunciado y documentos organizacionales 29

4.4 Actividad reciente: 8–22 de noviembre 32

4.5 Otros temas y exclusiones 36

4.6 Preguntas de validación que cambian una respuesta 37

CAPÍTULO 04

Actividad clandestina e interpretación de afirmaciones

EN RESUMEN

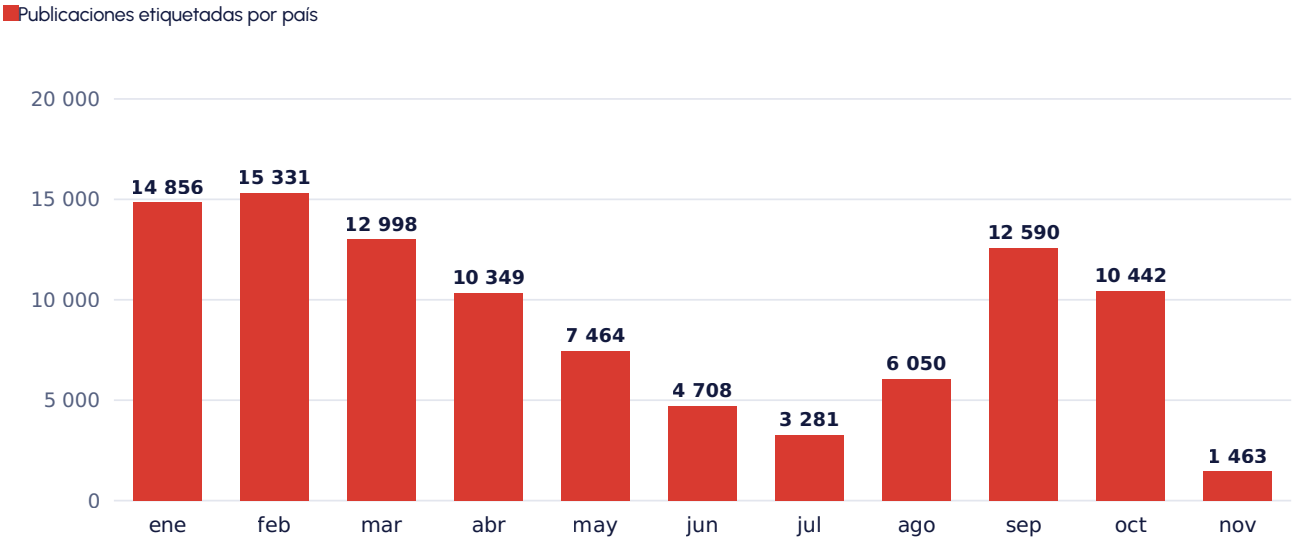
Las publicaciones ofrecen identidades, acceso a servicios públicos, documentos de salud, acceso comercial y datos educativos. Nueve casos separan esas afirmaciones de los resultados comprobados. Una conversación de enero identifica material anterior; las ofertas de noviembre describen temas educativos y registros públicos distintos. Mensajes repetidos y campos coincidentes no demuestran nuevas intrusiones ni archivos idénticos. Derive cada alerta pertinente a quien pueda validar procedencia, estado de cuentas, categorías de datos y efecto real sobre el servicio.

4.1 Ficha de la población

Elemento	Significado
Periodo	1 de enero–22 de noviembre de 2026, por fecha de publicación
Asociación con el país	Perú puede ser un presunto origen, mercado, grupo de clientes o referencia incidental
Población de evidencia	Mensajes conservados, incluidos anuncios y conversaciones de foros
Casos ilustrados	9, con 10 fichas de publicaciones anonimizadas
Estado de las afirmaciones	La publicación demuestra que se hizo la afirmación, no que sea correcta
Cobertura	El contenido conservado no constituye un censo nacional de incidentes
Ransomware	Población separada de 58 entradas en el capítulo 7

El informe separa publicación observada, presunta posesión, acceso utilizable, venta realizada e incidente confirmado de forma independiente. Una lista de campos puede ser plausible y dejar sin resolver origen, antigüedad y cantidad. La solicitud de un comprador no demuestra que alguien haya entregado el material. [S1]

Los volúmenes mensuales de publicaciones asociadas al país no miden intrusiones exitosas



Fuente: Odin by Brandefense, publicaciones etiquetadas como Perú, 1 de enero-22 de noviembre de 2026; noviembre parcial [S1]. Las publicaciones no son incidentes.

Mes	Publicaciones asociadas
2026-01	14 856
2026-02	15 331
2026-03	12 998
2026-04	10 349
2026-05	7 464
2026-06	4 708
2026-07	3 281
2026-08	6 050
2026-09	12 590
2026-10	10 442
2026-11	1 463
Total	99 532

Fuente: Odin by Brandefense [S1].

Telegram concentra la mayoría de publicaciones observadas asociadas al país



Fuente: Odin by Brandefense, publicaciones etiquetadas como Perú, 1 de enero-22 de noviembre de 2026; noviembre parcial [S1]. Las publicaciones no son incidentes.

Plataforma	Publicaciones asociadas
Telegram	99 076
Forum	430
Discord	9
Paste	17
Tor	0

La suma por plataformas es 99 532. Coincide con el total mensual de publicaciones. [S1]

Asociaciones de idioma seleccionadas; no exhaustivas y potencialmente solapadas



Las asociaciones de idioma seleccionadas no son exhaustivas y pueden solaparse. Fuente: Odin by Brandefense, publicaciones etiquetadas como Perú, 1 de enero-22 de noviembre de 2026; noviembre parcial [S1]. Las publicaciones no son incidentes.

Asociación de idioma	Publicaciones asociadas
Español	64 021
Inglés	11 438
Portugués	85
Ruso	1 509

Las asociaciones de idioma seleccionadas no son exhaustivas y pueden solaparse. No establecen nacionalidad, residencia ni un conteo de víctimas nacionales. [S1]

Los volúmenes regionales de publicaciones aportan contexto de visibilidad, no una clasificación de riesgo por país



Los conteos describen visibilidad; no se ajustan por tamaño del país ni cobertura de la fuente. Fuente: Odin by Brandefense, publicaciones etiquetadas como Perú, 1 de enero-22 de noviembre de 2026; noviembre parcial [S1]. Las publicaciones no son incidentes.

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

País	Publicaciones asociadas
Perú	99 532
Chile	27 891
Colombia	776 338
Ecuador	11 000
Bolivia	6 263

Fuente: Odin by Brandefense [S1]. Los tamaños de los países, la visibilidad de las fuentes y la publicidad internacional difieren. No se infiere una probabilidad nacional de ataque.

Las observaciones descriptivas de publicaciones miden visibilidad. Los cambios pueden reflejar comportamiento de publicación y cobertura de fuentes. No demuestran cambios en ataques exitosos, pérdidas o capacidad defensiva nacional. El mes final y el día de corte son parciales. [S1]

4.2 Una controversia visible sobre material reutilizado

A

CASO A

Anuncio de registros ciudadanos y corrección como republicación (B01, B02)

Temas de registros públicos

Afirmación sin verificar

AFIRMACIÓN	Un anuncio de foro del 7 de enero describe campos de identidad y contacto de una base de datos ciudadanos asociada a Perú. Afirma una cantidad de alcance nacional, que el informe no trata como personas medidas. [S1]
CRONOLOGÍA	Otros participantes describen el material como anterior y mencionan años distintos. Uno pide etiquetarlo como republicación; después, el autor dice haber cambiado el título. La secuencia respalda una conversación visible de corrección.
ESTABLECIDO	Se publicaron el anuncio y la controversia. El registro no establece de forma independiente la identidad del archivo, un año concreto de obtención, la fuente original ni una intrusión nueva en enero.
ALTERNATIVAS	Los datos anteriores pueden reagruparse, copiarse o combinarse. Una lista de campos aparentemente correcta también puede corresponder a una exportación histórica. La conversación no permite escoger un año comprobado entre afirmaciones de participantes.
RESPUESTA	El custodio debería comparar una alerta autorizada pertinente con divulgaciones y medidas anteriores. Conserve la diferencia entre una publicación nueva y un evento de seguridad recién establecido.

En definitiva

El custodio debería comparar una alerta autorizada pertinente con divulgaciones y medidas anteriores. Conserve la diferencia entre una publicación nueva y un evento de seguridad recién establecido.

Ficha de evidencia B01	7 ene 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Data : DNI, full names, birth date, age, address, location, phones, civil status

TRADUCCIÓN

Datos: DNI, nombres completos, fecha de nacimiento, edad, dirección, ubicación, teléfonos, estado civil

Lo que consta

Un anuncio de registros de ciudadanos describe campos de identidad y contacto.

Lo que no consta

Autenticidad, fuente y antigüedad del archivo, una nueva intrusión, personas únicas ni transferencia consumada.

Ficha de evidencia B02	7 ene 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Just rename the thread as a REPOST with the correct title.

TRADUCCIÓN

Solo cambien el nombre del hilo a una REPUBLICACIÓN con el título correcto.

Lo que consta

Un participante pide identificarlo como republicación después de que otros lo describen como material antiguo.

Lo que no consta

Identidad del archivo subyacente, fecha de adquisición verificada ni intrusión confirmada de 2026.

Este caso cambia la decisión cronológica. Un anuncio reciente es un evento actual de publicación. Puede seguir importando para la suplantación, pero no reinicia la fecha del presunto robo original. El reconocimiento de un participante tampoco demuestra que el archivo ofrecido sea idéntico, byte por byte, a una publicación anterior.

Un registro útil debería indicar qué coincidió: título, campos, muestra autorizada, aviso histórico o registro propio confirmado. Cada elemento aporta un respaldo distinto. El informe no describe una comparación de archivos subyacentes ni una adquisición al vendedor.

4.3 Acceso anunciado y documentos organizacionales

B

CASO B

Acceso privilegiado anunciado para un portal de servicios públicos

Afirmación sin verificar

Ficha de evidencia B03 | 10 feb 2026 | Foro | Servicios públicos

AFIRMACIÓN	Una publicación del 10 de febrero ofrece acceso de administrador raíz, firewall y administración de red para un portal de servicios públicos. El vendedor pide 200 USD. Son capacidades y precio anunciados, no acceso validado ni valor de una transacción. [S1]
ESTABLECIDO	La fuente describe una oferta de acceso privilegiado. No demuestra una cuenta funcional, al titular actual, una vulnerabilidad explotable ni un efecto sobre servicios públicos.
ALTERNATIVAS	El acceso puede ser antiguo, estar mal descrito, limitarse a un entorno del proveedor o anunciarse sin posesión. Describir un panel no demuestra alcance sobre todos los sistemas conectados al servicio público.
RESPUESTA	Un responsable autorizado debería validar el activo y la cuenta; después, revisar administración remota, privilegios, sesiones y cambios. Contenga solo el acceso respaldado por evidencia de la organización.

En definitiva

Un responsable autorizado debería validar el activo y la cuenta; después, revisar administración remota, privilegios, sesiones y cambios. Contenga solo el acceso respaldado por evidencia de la organización.

C

CASO C

Presunta publicación de documentos relacionados con salud

Afirmación sin verificar

Ficha de evidencia B04 | 16 feb 2026 | Foro | Salud

AFIRMACIÓN	Una publicación de foro del 16 de febrero anuncia documentos de una entidad regional de salud. Describe formatos habituales de oficina. Los documentos y el volumen anunciado siguen sin comprobarse. [S1]
ESTABLECIDO	La publicación registra una afirmación de difusión documental. No demuestra impacto sobre pacientes, vía de intrusión, acceso actual ni cantidad de afectados. Una respuesta posterior sobre acceso al material anunciado no verifica su autenticidad.

ALTERNATIVAS	El material puede ser histórico, estar en poder de un proveedor, ser público o estar mal descrito. Mencionar a una entidad de salud en un documento no demuestra acceso a sistemas clínicos.
RESPUESTA	El custodio debería establecer categorías y titularidad mediante una alerta autorizada. Los responsables clínicos deberían evaluar la continuidad de forma independiente de la afirmación documental.

En definitiva

El custodio debería establecer categorías y titularidad mediante una alerta autorizada. Los responsables clínicos deberían evaluar la continuidad de forma independiente de la afirmación documental.

Ficha de evidencia B03 — 10 feb 2026

[alias reservado] · Foro · Forum · Inglés

ORIGINAL

Permissions: Root RCE + Shell + Network Admin Panel

TRADUCCIÓN

Permisos: RCE de root + shell + panel de administración de red

Lo que consta

Un vendedor anuncia acceso privilegiado al firewall y al portal. Afirma tener ejecución remota de código, privilegios del nivel más alto y acceso por línea de comandos; nada de ello está validado.

Lo que no consta

Acceso actual utilizable, titularidad, explotación verificada, venta consumada ni efecto operativo.

Ficha de evidencia B04 — 16 feb 2026

[alias reservado] · Foro · Forum · Inglés

ORIGINAL

Type of documents: XLSX, PDF, DOCX, and so on

TRADUCCIÓN

Tipo de documentos: XLSX, PDF, DOCX, etcétera

Lo que consta

Una publicación afirma divulgar documentos de un organismo regional de salud.

Lo que no consta

Autenticidad, efecto en pacientes, una nueva intrusión, acceso actual ni volumen verificado.

D

CASO D

Registros relacionados con prestaciones ofrecidos a la venta

Afirmación sin verificar

Ficha de evidencia B05 · 4 mar 2026 · Foro · Servicios públicos

AFIRMACIÓN	Un anuncio del 4 de marzo describe identidad, fecha de nacimiento, periodos de aportación y periodos laborales asociados a la gestión de prestaciones. Las cantidades de registros y beneficiarios afirmadas siguen sin comprobarse y no se reproducen como personas afectadas. [S1]
ESTABLECIDO	Los campos y la afirmación de venta aparecen en la publicación. No se establece la fuente subyacente, la fecha de obtención, beneficiarios únicos, acceso actual ni venta realizada.

ALTERNATIVAS	Exportaciones administrativas históricas o registros superpuestos podrían explicar el material anunciado. La función de una institución en la gestión de prestaciones no demuestra que su sistema central fuera el punto de obtención.
RESPUESTA	El custodio debería comparar categorías con registros y avisos propios. Protección del cliente debería autenticar de forma independiente las solicitudes de cambio de pagos o datos de identidad.

En definitiva

El custodio debería comparar categorías con registros y avisos propios. Protección del cliente debería autenticar de forma independiente las solicitudes de cambio de pagos o datos de identidad.

E

CASO E

Acceso a cuentas comerciales y documentos operativos

Ficha de evidencia B06 | 27 mar 2026 | Foro | Comercio minorista

Afirmación sin verificar

AFIRMACIÓN	Un anuncio del 27 de marzo ofrece acceso mediante usuario y contraseña y describe documentos operativos comerciales. Pide 20 000 USD, negociables. Algunas fechas documentales descritas son anteriores al año del estudio. [S1]
ESTABLECIDO	La oferta combina una afirmación de acceso con publicidad de documentos. No demuestra privilegios actuales, intrusión en toda la empresa, autenticidad documental ni una transacción realizada.
ALTERNATIVAS	Una exportación antigua, una cuenta de proveedor, un rol limitado de aplicación o publicidad incorrecta podrían producir la misma descripción. El precio no valida la afirmación.
RESPUESTA	Identidad y responsables del negocio deberían establecer titularidad, estado y alcance de la cuenta. Finanzas debería verificar de forma independiente cambios de pago o proveedores si se validan documentos operativos pertinentes.

En definitiva

Identidad y responsables del negocio deberían establecer titularidad, estado y alcance de la cuenta. Finanzas debería verificar de forma independiente cambios de pago o proveedores si se validan documentos operativos pertinentes.

Ficha de evidencia B05 — 4 mar 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Type of data: national ID, last name, name, birth date, contribution period, employment period

TRADUCCIÓN

Tipo de datos: identificación nacional, apellido, nombre, fecha de nacimiento, periodo de aportes, periodo laboral

Lo que consta
Una publicación ofrece registros descritos como relacionados con la administración de beneficios.

Lo que no consta
Autenticidad, beneficiarios únicos, fecha de adquisición, acceso actual ni venta consumada.

Ficha de evidencia B06 — 27 mar 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Selling LOGIN AND PASSWORD

TRADUCCIÓN

Vendo USUARIO Y CONTRASEÑA

Lo que consta
Un vendedor anuncia acceso y describe documentos operativos de comercio minorista.

Lo que no consta
Acceso válido, privilegios actuales, documentos auténticos, venta consumada ni intrusión en toda la empresa.

Los dos anuncios describen alcances y precios diferentes. No establecen un rango representativo de precios de mercado. Un precio pedido puede reflejar negociación, presentación o una afirmación sin respaldo. El informe no estima ingresos de ventas ni el costo de una intrusión exitosa.

4.4 Actividad reciente: 8–22 de noviembre

Los cuatro casos siguientes corresponden al periodo reciente según la fecha conservada de publicación. Esas fechas no establecen cuándo se obtuvo información subyacente. Una respuesta oficial relacionada debe acompañar a la afirmación pertinente, sin tratarse como confirmación de todos sus detalles. [S1]

CASO F

F

Registros empresariales presentados como una filtración nueva

Afirmación sin verificar

Ficha de evidencia B07 · 8 nov 2026 · Foro · Temas de registros públicos

AFIRMACIÓN	Una publicación del 8 de noviembre con marca de grupo describe registros empresariales y presenta su difusión como filtración. Utiliza la etiqueta MortemTeam. Esa marca no establece de forma independiente la identidad ni responsabilidad del autor. [S1]
ESTABLECIDO	Los campos incluyen identificadores empresariales, razones sociales, estados y direcciones. La publicación no demuestra procedencia no pública, acceso no autorizado a sistemas, robo reciente ni una población verificada de empresas.

CONTRAPUNTO	La prensa recoge el desmentido de un organismo del sector público sobre intrusión o extracción interna y su cuestionamiento de la procedencia alegada. Sigue siendo la evaluación del organismo que respondió, no una validación independiente del archivo. [S27]
ALTERNATIVAS	Material público o histórico de registros podría presentarse como una intrusión nueva. Sigue siendo una alternativa; el informe no ha establecido coincidencia del archivo ofrecido con un conjunto público concreto.
RESPUESTA	Determine si la alerta contiene información realmente no pública y evidencia de acceso no autorizado. Conserve como afirmaciones separadas lo dicho por el actor, la respuesta de la autoridad y la procedencia no resuelta.

En definitiva

Determine si la alerta contiene información realmente no pública y evidencia de acceso no autorizado. Conserve como afirmaciones separadas lo dicho por el actor, la respuesta de la autoridad y la procedencia no resuelta.

G

CASO G

Registros de estudiantes, apoderados y asistencia

Ficha de evidencia B08 | 13 nov 2026 | Foro | Educación

Afirmación sin verificar

AFIRMACIÓN	Una publicación del 13 de noviembre con marca de grupo afirma contener datos de estudiantes, apoderados y asistencia de un prestador educativo. También afirma una vía técnica de entrada, sin validación. Se omite la provocación política del actor. [S1]
ESTABLECIDO	El registro describe varias categorías. Estudiantes, apoderados y asistencias son unidades distintas; no pueden sumarse como personas afectadas. La publicación no demuestra una intrusión exitosa ni una vulnerabilidad funcional.
ALTERNATIVAS	La información anunciada puede ser histórica, superpuesta, estar en poder de un proveedor o estar mal descrita. Compartir una marca con otra publicación no establece el mismo operador ni evento de obtención.
RESPUESTA	Un responsable autorizado debería revisar accesos a la aplicación y registros pertinentes. Si se validan datos reales, involucre a privacidad y protección de menores para delimitar información infantil y comunicaciones apropiadas.

En definitiva

Un responsable autorizado debería revisar accesos a la aplicación y registros pertinentes. Si se validan datos reales, involucre a privacidad y protección de menores para delimitar información infantil y comunicaciones apropiadas.

Ficha de evidencia B07 — 8 nov 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Data Included: [business identifier], Legal Name, [registration status fields], Address

TRADUCCIÓN

Datos incluidos: [identificador empresarial], razón social, [campos de estado registral], dirección

Lo que consta
Una publicación describe campos de registro empresarial y presenta su divulgación como filtración.

Lo que no consta
Procedencia no pública, acceso no autorizado al sistema, robo reciente, empresas únicas ni volumen verificado.

Ficha de evidencia B08 — 13 nov 2026

[alias reservado] Foro Forum Inglés

ORIGINAL

Data Included: full student roster - DNI, names, date of birth, sex, level, grade, section, home address

TRADUCCIÓN

Datos incluidos: lista completa de estudiantes: DNI, nombres, fecha de nacimiento, sexo, nivel, grado, sección, dirección del domicilio

Lo que consta
Una publicación con marca de grupo afirma disponer de registros de estudiantes, apoderados y asistencia de un proveedor educativo.

Lo que no consta
Vulnerabilidad verificada, registros auténticos, totales de estudiantes afectados ni intrusión exitosa.

CASO H

H ■ Información de gestión educativa y acceso a cuentas

Ficha de evidencia B09 · 16 nov 2026 · Foro · Educación

Afirmación sin verificar

AFIRMACIÓN	Una oferta en español del 16 de noviembre combina información de administradores o directores con acceso a una plataforma de gestión educativa. Describe campos de identidad, contacto y fotografías. [S1]
ESTABLECIDO	El anuncio afirma disponer tanto de datos como de acceso. No demuestra credenciales funcionales, privilegios actuales, titularidad de la plataforma, autenticidad de datos ni intrusión nueva.
ALTERNATIVAS	La información y la cuenta pueden tener edades u orígenes diferentes. Una contraseña ofrecida no demuestra que la cuenta siguiera vigente al publicarse el anuncio.
RESPUESTA	Valide titularidad, estado y privilegios de la cuenta. Delimite por separado los datos personales pertinentes y revoque el acceso cuando lo respalde evidencia de sistemas propios.

En definitiva

Valide titularidad, estado y privilegios de la cuenta. Delimite por separado los datos personales pertinentes y revoque el acceso cuando lo respalde evidencia de sistemas propios.

CASO I

Historiales laborales y campos relacionados con cuentas

Ficha de evidencia B10 | 20 nov 2026 | Foro | Servicios públicos

Afirmación sin verificar

AFIRMACIÓN	Dos observaciones de foro del 20 de noviembre contienen publicidad sustancialmente coincidente de historiales laborales y datos personales asociados a una entidad de servicios públicos. Difieren en detalles de presentación del foro. [S1]
ESTABLECIDO	Se publicó publicidad coincidente. No demuestra archivos subyacentes idénticos, dos intrusiones independientes, personas únicas, cuentas funcionales ni una venta realizada.
ALTERNATIVAS	Las observaciones podrían corresponder a un anuncio repetido o una exportación histórica superpuesta. Describir datos personales y campos de cuentas no demuestra que alguna cuenta anunciada pudiera utilizarse.
RESPUESTA	El custodio debería validar categorías y antigüedad. Identidad y fraude deberían evaluar por separado el uso real de cuentas y la evidencia de cambios de pagos.

En definitiva

El custodio debería validar categorías y antigüedad. Identidad y fraude deberían evaluar por separado el uso real de cuentas y la evidencia de cambios de pagos.

Ficha de evidencia B09 16 nov 2026

[alias reservado] Foro Forum Español

ORIGINAL

ACCESO A UNA DE SUS PLATAFORMAS DE GESTION POR USUARIO Y CONTRASEÑA

Lo que consta
Una publicación combina una oferta de datos de gestión educativa con una afirmación de acceso a cuentas.

Lo que no consta
Credenciales funcionales, privilegios actuales, datos auténticos, titularidad ni una nueva intrusión.

Ficha de evidencia B10 20 nov 2026

[alias reservado] Foro Forum Español

ORIGINAL

TIPO DE USUARIO, TIPO DE CONTRATO, NOMBRES, APELLIDOS, ESTADO DE ACTIVIDAD

Lo que consta
Una publicación anuncia registros de historiales laborales y campos relacionados con cuentas de un organismo de servicio público.

Lo que no consta
Autenticidad, personas únicas, una nueva intrusión, cuentas válidas ni venta consumada.

4.5 Otros temas y exclusiones

Periodo de publicación	Afirmación conservada	Tratamiento y decisión útil
Enero	Registros de clientes de telecomunicaciones en una cita de foro	Mención; la conversación citada no establece una intrusión independiente en una operadora
Abril	Oferta de documentos oficiales, algunos descritos como anteriores	Mención; valide categorías y cronología antes de asignar un evento nuevo
Abril–mayo	Bases de suscriptores con descripciones de campos similares	Mención; la similitud no demuestra archivos idénticos ni intrusiones distintas
Junio y octubre	Narrativa sobre datos de paquetería en respuestas de foro	Mención; la publicación posterior no es confirmación independiente
Agosto	Datos de clientes de alimentación descritos como material anterior	Mención; distinga una oferta posterior de la fecha de obtención
Octubre	Registros de salud de origen no resuelto	Mención; la evaluación de privacidad depende de registros validados
Octubre	Directorio educativo anunciado como filtración	Mención; un directorio público es una procedencia alternativa plausible
Noviembre	Afirmaciones sobre capacitación y documentos tributarios	Mención; las muestras personales y las afirmaciones técnicas no están verificadas
Noviembre	Afirmación de un servicio de consulta relacionado con justicia	Mención; no se publica una prueba de acceso ni una ruta funcional

Periodo de publicación	Afirmación conservada	Tratamiento y decisión útil
14 de noviembre	Una republicación de un registro de desfiguraciones menciona un sitio asociado a Perú	Mención; aparecer en una republicación no demuestra impacto comprobado de forma independiente
15 de noviembre	Una solicitud busca expresamente servicios de punto de venta en Perú	Demanda observada; no se establece adquisición, servicio funcional ni transacción realizada
22 de noviembre	Una respuesta de bot de consulta muestra campos de identidad	Mención; procedencia, antigüedad y acceso al sistema fuente sin verificar
Durante el periodo	Catálogos internacionales de tarjetas, proxies, SMS y cuentas incluyen Perú	Contexto de visibilidad; no se infiere una intrusión nacional
Durante el periodo	Solicitudes de listas de contactos o pares de usuario y contraseña	Demanda observada; no se establece posesión ni entrega
Durante el periodo	Respuestas de cortesía y mensajes para desbloquear contenido	Excluidos como corroboración de la afirmación de incidente

Fuente: publicaciones conservadas [S1]. Son temas, no un total adicional de incidentes confirmados. Una conversación puede producir varios mensajes conservados; varios anuncios pueden describir material superpuesto.

4.6 Preguntas de validación que cambian una respuesta

Afirmación	Evidencia necesaria de un responsable autorizado	Decisión que puede respaldar
Los datos pertenecen a esta institución	Coincidencia confiable de titularidad y contenido	Delimitar datos pertinentes y evaluar notificaciones
Una cuenta ofrecida sigue activa	Estado, privilegios y registros de acceso	Contener acceso y sesiones validados
El anuncio describe un evento nuevo	Cronología adicional a la nueva publicación	Abrir un incidente nuevo o relacionar una divulgación histórica
Se utilizó una vía técnica	Evidencia de aplicaciones y sistemas propios	Corregir la debilidad demostrada y delimitar el acceso
Dos publicaciones describen el mismo material	Más que títulos o cantidades coincidentes	Evitar doble recuento conservando la incertidumbre
Se interrumpió un servicio público	Evidencia del servicio y de tareas de usuarios	Activar el plan de continuidad apropiado

El informe no adquiere archivos anunciados, compra acceso ni contacta vendedores. Evalúa evidencia conservada y corroboración pública. Una conclusión más fuerte necesitaría evidencia de la afirmación concreta, no una lectura más confiada del mismo anuncio.

CONCLUSIONES CLAVE

01

Nueve casos conservan afirmaciones distintas, no nueve intrusiones confirmadas.

02

El periodo reciente incluye publicaciones con fechas de obtención no resueltas.

03

Anuncios coincidentes, campos plausibles y precios pedidos no validan posesión, acceso ni ventas realizadas.

CAPÍTULO 05

Incidentes públicos y respuesta por sector

05

ESTE CAPÍTULO RESPONDE

¿Qué reportes públicos establecen un evento y cómo debería responder cada sector?

5

casos públicos con evidencia y unidades de incidente diferentes

5.1 Reglas de lectura y recuento 40

5.2 Acceso mediante una cuenta de proveedor y mensajes públicos 40

5.3 Seguros: acceso a información sin interrupción significativa 41

5.4 Salud: autorización de pagos y continuidad clínica 42

5.5 Alertas oficiales de fraude y actuaciones de investigación 43

5.6 Otras campañas, desmentidos y exclusiones leídos en sus fuentes 44

5.7 Decisiones sectoriales sin calificaciones de riesgo sectorial 45

CAPÍTULO 05

Incidentes públicos y respuesta por sector

EN RESUMEN

Los reportes públicos respaldan decisiones distintas sobre acceso de proveedores, información de clientes, transferencias no autorizadas, suplantación de marcas y presuntas ventas ilegales de datos. Los cinco casos no equivalen a cinco intrusiones de red confirmadas. Separe los hechos establecidos de las cantidades delictivas y la especulación técnica. Elija contención, protección del cliente, revisión de pagos o apoyo investigativo según la evidencia concreta, manteniendo los servicios esenciales.

5.1 Reglas de lectura y recuento

Los casos siguientes incluyen tres eventos reportados de seguridad o fraude, una alerta oficial de suplantación y un operativo. No constituyen un total nacional de incidentes. Los nueve casos clandestinos del capítulo 4 son evaluaciones separadas de afirmaciones y no se suman a estos eventos. [S17][S18][S23][S20][S22]

Una confirmación puede establecer acceso o una transferencia cuestionada sin establecer al autor, la vía de entrada o la población final afectada. Las declaraciones reproducidas por la prensa se atribuyen como tales. Un desmentido de una autoridad es su posición, no una prueba independiente sobre un archivo ofrecido.

Solo se usan nombres cuando los respaldan una confirmación oficial y amplia cobertura. Los demás objetivos se describen mediante funciones generales. Las direcciones de artículos que revelarían una identidad reservada se citan con la raíz del editor y la indicación de URL omitida.

5.2 Acceso mediante una cuenta de proveedor y mensajes públicos

J

CASO J

Mensajes no autorizados mediante un servicio de alertas públicas

Caso de información pública

Relato de la fuente; límites conservados

CONFIRMACIÓN REPORTADA	El 20 de mayo, la autoridad responsable informó del uso no autorizado de una cuenta de proveedor para enviar mensajes falsos de emergencia. Latina Noticias reproduce su comunicado. [S17]
LÍMITE	El reporte no establece un mecanismo DDoS, un operador político, acceso interno más amplio ni relación con el anuncio de febrero. Las noticias posteriores sobre el evento de mayo no son intrusiones nuevas.

INTERPRETACIÓN	Emitir mensajes públicos confiables es un privilegio crítico. La disponibilidad del servicio y la integridad de los mensajes requieren garantías distintas antes de reabrir.
RESPUESTA	El responsable debería inventariar privilegios de emisión, probar la suspensión de cuentas de proveedores, conservar autorizaciones y ensayar un canal confiable de corrección.

En definitiva

El responsable debería inventariar privilegios de emisión, probar la suspensión de cuentas de proveedores, conservar autorizaciones y ensayar un canal confiable de corrección.

El ejercicio práctico debería partir de un mensaje no autorizado, sin asumir un servidor cifrado. Determine quién puede detener nuevas emisiones y quién aprueba una corrección legítima. Pruebe el proceso cuando el contacto o administrador habitual del proveedor no esté disponible.

La supervisión debe conservar la diferencia entre titularidad de la cuenta y responsabilidad organizacional. El reporte identifica la relación por la que se produjo el acceso. No demuestra acceso a todo el entorno del proveedor ni afectación de todos sus clientes.

5.3 Seguros: acceso a información sin interrupción significativa

K

CASO K

Acceso a información de clientes de una aseguradora

Caso de información pública

Relato de la fuente; límites conservados

CONFIRMACIÓN REPORTADA	La aseguradora dijo a El Comercio que detectó acceso no autorizado a información de clientes el 7 de octubre. El supervisor confirmó haber sido notificado y estar siguiendo el incidente. [S18][S19]
LÍMITE	La detección no es la fecha inicial de la intrusión. Cantidad de clientes, vía de entrada y alcance final seguían sin resolverse. No se adopta la cantidad de datos afirmada por el actor.
INTERPRETACIÓN	La operación normal y un incidente de confidencialidad pueden coexistir. Recuperar el servicio no cierra la delimitación de datos personales ni la atención al cliente.
RESPUESTA	Establezca las categorías reales de datos, conserve la cronología de conocimiento y mantenga orientación delimitada a clientes mientras continúa la investigación.

En definitiva

Establezca las categorías reales de datos, conserve la cronología de conocimiento y mantenga orientación delimitada a clientes mientras continúa la investigación.

El caso cambia un atajo frecuente de decisión. La ausencia de una caída importante no debería cerrar la evaluación de acceso a información. El registro de privacidad debería identificar las categorías establecidas y las preguntas pendientes, con responsable para cada actualización.

La recepción de un reporte por el supervisor no valida de forma independiente todas las afirmaciones del actor. Establece el proceso de supervisión descrito por la fuente. El informe no atribuye el incidente a un operador concreto solo porque una etiqueta de extorsión nombró después a la organización.

5.4 Salud: autorización de pagos y continuidad clínica

CASO L

L

Transferencias no autorizadas reportadas por una red de salud

Caso de información pública

Relato de la fuente; límites conservados

CONFIRMACIÓN REPORTADA	La institución informó de cinco transferencias que no reconocía como autorizadas, fechadas el 14 de agosto, por S/1 406 991. Dos medios reproducen su reporte. [S23][S24]
LÍMITE	La fuente no establece vía técnica de entrada, intrusión en sistemas del banco ni responsable. El monto corresponde a esas transferencias, no a una estimación nacional de pérdidas por ciberdelincuencia.
INTERPRETACIÓN	Autorización de pagos, conservación de evidencia y continuidad clínica necesitan responsables distintos. Una denuncia no es una condena; reclamar a una contraparte financiera no demuestra acceso a sus sistemas.
RESPUESTA	Tesorería debería conservar registros, revisar aprobaciones y cambios de beneficiarios, y coordinar una solicitud fundamentada de recuperación mediante contactos bancarios confiables.

En definitiva

Tesorería debería conservar registros, revisar aprobaciones y cambios de beneficiarios, y coordinar una solicitud fundamentada de recuperación mediante contactos bancarios confiables.

Los responsables de salud también deberían mantener la continuidad al restringir accesos financieros. Identifique pagos críticos y aprobaciones para sostener servicios seguros. Reabrir un flujo de pagos debería demostrar autorización válida y un proceso auditable de excepciones.

Las afirmaciones documentales del capítulo 4 y las entradas de ransomware de salud del capítulo 7 son poblaciones distintas. No se establece un actor común, una base compartida ni una relación causal con estas transferencias.

5.5 Alertas oficiales de fraude y actuaciones de investigación

M

CASO M

Petroperú advierte sobre un video de inversión manipulado

Caso de información pública

Relato de la fuente; límites conservados

REPORTE OFICIAL	El 12 de junio, Petroperú advirtió que un video manipulaba la voz e imagen de un ejecutivo para promover una inversión que la empresa declaró inexistente. Después hubo mayor cobertura. [S20][S21]
LÍMITE	La alerta no demuestra acceso a sistemas de la empresa, una cantidad de inversionistas afectados ni pérdidas cuantificadas.
INTERPRETACIÓN	Una imagen ejecutiva creíble puede crear un problema de verificación para los clientes sin una intrusión en la empresa suplantada.
RESPUESTA	Publique el proceso legítimo de inversión y pagos, ofrezca verificación independiente e informe al personal que atiende clientes sobre el engaño concreto.

En definitiva

Publique el proceso legítimo de inversión y pagos, ofrezca verificación independiente e informe al personal que atiende clientes sobre el engaño concreto.

N

CASO N

Operativo contra presuntas ventas ilegales de datos personales

Caso de información pública

Relato de la fuente; límites conservados

REPORTE OFICIAL	Un aviso de la autoridad de identidad del 3 de julio describe un operativo policial conjunto del 29 de junio por presunta venta de información personal y certificados falsos. Registra acciones investigativas y material incautado. [S22]

LÍMITE	El aviso no demuestra una intrusión nueva en la base central de la autoridad ni una condena. Presunta venta, presunto acceso y un evento probado del sistema fuente son afirmaciones distintas.
INTERPRETACIÓN	La protección de datos va más allá de investigar una intrusión central. Distribución, suplantación y verificación documental pueden exigir acciones separadas.
RESPUESTA	Conserve reportes pertinentes por canales autorizados, verifique documentos con su fuente legítima y distinga los hechos probados de las alegaciones de la investigación.

En definitiva

Conserve reportes pertinentes por canales autorizados, verifique documentos con su fuente legítima y distinga los hechos probados de las alegaciones de la investigación.

5.6 Otras campañas, desmentidos y exclusiones leídos en sus fuentes

Publicación	Reporte de la fuente	Tratamiento en este informe
Febrero	El supervisor financiero publica una hoja de ruta de finanzas abiertas por fases [S29]	Contexto regulatorio; no controles implementados ni incidente de seguridad
Abril	El supervisor financiero anuncia cambios del marco sancionador [S30]	Contexto regulatorio; no se infieren multas ni resultados de casos
Agosto	El diario oficial recoge una alerta de suplantación con multas de transporte y códigos QR [S26]	Contexto de fraude; las denuncias reportadas no son intrusiones confirmadas
Septiembre	Una agencia pública de noticias informa de 42 161 denuncias por delitos informáticos ante el Ministerio Público en 2024, 42 980 en 2025 y 29 118 en enero–julio de 2026 [S25]	Población de denuncias (totales anuales comparables de 2024–2025 y periodo parcial de 2026), separada de publicaciones, entradas e intrusiones confirmadas
Noviembre	Avisos del servicio de identidad atribuyen una interrupción a un evento eléctrico [S34]	Contexto de continuidad; excluido del recuento de ciberataques hostiles
Noviembre	Una discusión regulatoria revisita un incidente bancario anterior [S28]	Seguimiento histórico; no se infiere una nueva intrusión en 2026
Agosto	Una investigación pública abarca eventos estatales de seguridad de datos de 2020–2026 [S35]	Contexto de varios años; no total de eventos de 2026

El reporte de septiembre con estadísticas del Ministerio Público registra 42 161 denuncias por delitos informáticos en 2024, 42 980 en 2025 y 29 118 en enero–julio de 2026 [S25]. Los totales anuales comparables subieron de 2024 a 2025, mientras que la cifra de 2026 cubre siete meses y sigue separada de publicaciones, entradas de ransomware e intrusiones confirmadas.

La interrupción de noviembre del servicio de identidad también queda fuera del periodo reciente. Publicación de una noticia, fecha del incidente e hito regulatorio posterior deben conservarse separados. El informe no añade causas técnicas ni conclusiones legales finales que la fuente no haya establecido.

5.7 Decisiones sectoriales sin calificaciones de riesgo sectorial

Sector	Distinción de evidencia	Primera decisión en el entorno propio
Administración pública	Las afirmaciones de acceso, mensajes falsos y ventas documentales difieren	Establecer la función afectada y controlar sus privilegios reales
Finanzas y seguros	Puede haber acceso a información sin una caída importante	Evaluar privacidad y protección de clientes junto con la respuesta técnica
Salud	Afirmaciones documentales, eventos de pago y entradas de ransomware son distintos	Mantener continuidad clínica al validar datos o pagos
Educación	Estudiantes, apoderados y asistencias son unidades distintas	Validar categorías y acceso, con responsable de protección de menores
Energía e industria	La suplantación puede afectar clientes sin acceso interno	Verificar pagos e inversiones por canales conocidos
Comercio, transporte y proveedores	Los registros operativos pueden dar contexto a un fraude	Verificar de forma independiente cambios de beneficiarios y proveedores

Son distinciones de respuesta respaldadas por los casos. No son calificaciones sectoriales, estimaciones de prevalencia nacional ni afirmaciones de que todas las organizaciones tengan los mismos sistemas. La selección de exposición tiene denominador y límites propios en el capítulo 3.

CONCLUSIONES CLAVE

01

Los cinco casos públicos incluyen eventos, alertas e investigaciones diferentes.

02

Continuidad, privacidad, autorización de pagos y protección de marca requieren decisiones separadas.

03

Conserve fechas de evento, detección, publicación y seguimiento sin crear intrusiones nuevas a partir de cobertura posterior.

CAPÍTULO 06

Mensajes no autorizados, afirmaciones de acceso y disponibilidad de servicios

ESTE CAPÍTULO RESPONDE

¿Qué efectos están establecidos y qué justificaría una atribución más fuerte?

3

preguntas distintas: integridad de mensajes, disponibilidad y acceso a datos

6.1 Cronología con etiquetas de evidencia 47

6.2 Afirmación frente a reporte de la autoridad 48

6.3 Disponibilidad e integridad requieren pruebas distintas 48

6.4 Prepárese para interrupciones sin inventar una campaña 48

6.5 La comunicación debe conservar la incertidumbre 49

CAPÍTULO 06

Mensajes no autorizados, afirmaciones de acceso y disponibilidad de servicios

EN RESUMEN

El evento de alertas públicas de mayo estableció uso no autorizado de una cuenta de proveedor y mensajes falsos, según el reporte de la autoridad recogido por la prensa. No establece un mecanismo DDoS ni un operador político. Otras afirmaciones de acceso y datos no están verificadas. Prepare por separado la indisponibilidad del servicio, los mensajes no autorizados y la posible pérdida de información, con evidencia y pruebas de reapertura diferentes.

6.1 Cronología con etiquetas de evidencia

7 ene 2026	**Participantes de foro** Anuncio de datos ciudadanos cuestionado como material anterior; no se establece intrusión nueva (B01, B02) [S1]
10 feb 2026	**Anunciante de foro** Afirma acceso privilegiado a un servicio público; utilidad sin verificar (B03) [S1]
20 may 2026	**Declaración de autoridad recogida por la prensa** Reconoce acceso mediante cuenta de proveedor y falsas alertas [S17]
12 jun 2026	**Petroperú** Alerta de video de inversión manipulado con IA; no se establece intrusión interna [S20]
7 oct 2026	**Declaración de aseguradora recogida por la prensa** Detección de acceso a información de clientes; fecha inicial sin resolver [S18]
8 nov 2026	**Publicación de foro con marca de grupo** Registros empresariales presentados como filtración (B07) [S1]
9 nov 2026	**Respuesta de autoridad recogida por la prensa** Niega intrusión o extracción interna respecto de la base anunciada [S27]
14 nov 2026	**Registro republicado de desfiguraciones** Afirma aparición de un sitio; impacto operativo sin verificar [S1]
16 nov 2026	**Investigación de Kaspersky** Publica investigación sobre intentos anteriores bloqueados en varios países [S32]

La cronología combina fechas de publicaciones, una detección y declaraciones públicas. Las etiquetas identifican el tipo de evidencia, no la confirmación independiente de cada afirmación. Una investigación publicada en noviembre puede describir actividad anterior. [S1][S17][S18][S32]

6.2 Afirmación frente a reporte de la autoridad

Punto	Afirmación del actor	Reporte oficial	Límite independiente
Acceso a un servicio público	Un anunciante de febrero afirma acceso privilegiado a un portal [S1]	No se estableció confirmación oficial coincidente	No se demuestra vínculo con el evento de mayo
Falsas alertas públicas	La conversación pública describió un evento malicioso	El reporte de mayo identifica uso no autorizado de cuenta de proveedor y alertas falsas, según la prensa [S17]	Identidad, motivo y alcance adicional sin resolver
Registros empresariales de noviembre	Una publicación con marca de grupo presenta datos como filtración [S1]	La autoridad niega evidencia de intrusión o extracción institucional [S27]	Sin evaluación independiente de autenticidad o procedencia del archivo ofrecido
Lenguaje político	Parte del material incorpora un encuadre político	No se establece atribución estatal en este informe	La retórica no demuestra nacionalidad, dirección ni interferencia electoral

Un efecto operativo visible y la participación afirmada de un actor necesitan evidencia distinta. El informe no vincula el anuncio de febrero, el evento de mayo y la afirmación de noviembre solo por compartir país o sector.

6.3 Disponibilidad e integridad requieren pruebas distintas

La respuesta DDoS pregunta si los usuarios pueden llegar al servicio y completar tareas críticas. La integridad de mensajes pregunta quién puede emitir contenido y si está autorizado. La respuesta de acceso a datos pregunta qué registros se consultaron y por quién.

En un servicio de alertas, una web que responde no demuestra que la emisión de mensajes sea segura. En un portal transaccional, recuperar el inicio de sesión no demuestra que se revocaron sesiones indebidas. En una base de clientes, operar sin interrupción no descarta acceso no autorizado a información.

La dirección del incidente debería identificar la función afectada antes de elegir un hito de recuperación. Los equipos técnicos conservarán la evidencia necesaria: datos operativos del servicio, actividad de cuentas, cambios administrativos o registros pertinentes de acceso a datos.

6.4 Prepárese para interrupciones sin inventar una campaña

El material revisado no establece una campaña DDoS medida nacionalmente ni una operación política comprobada contra el proceso electoral. Ese resultado de cobertura no demuestra ausencia de actividad fuera de la evidencia examinada.

Las organizaciones pueden preparar la continuidad. Acuerde quién solicita mitigación al proveedor, qué información pública se mantiene en un canal independiente y qué tareas reciben prioridad. Pruebe contactos mientras el servicio habitual de identidad o mensajería está fuera de operación.

Evite restricciones generales que excluyan usuarios sin evaluación. Toda medida de emergencia de control de tráfico debería tener duración, responsable y una vía para usuarios legítimos. Reevalúela según efectos reales y evidencia disponible.

6.5 La comunicación debe conservar la incertidumbre

Una primera declaración útil identifica función afectada, momento conocido, acción tomada y siguiente actualización. Separe la afirmación y el efecto confirmado en oraciones distintas. No publique cantidades o motivos sin respaldo solo porque circulan ampliamente.

Cuando intervenga una cuenta de proveedor, distinga la relación de suministro de una alegación sobre todo su entorno. Indique solo el alcance respaldado por la autoridad u organización. La orientación a clientes debe usar un canal confiable y omitir el enlace fraudulento.

CONCLUSIONES CLAVE

01

Mensajes falsos, DDoS y acceso a datos requieren evidencia distinta.

02

Un anuncio cercano no demuestra vínculo con un incidente oficial.

03

Las pruebas de reapertura deben corresponder a la función afectada y la comunicación debe conservar incertidumbre.

CAPÍTULO 07

Actores, ransomware y relaciones respaldadas

07

ESTE CAPÍTULO RESPONDE

¿Qué etiquetas importan para operar y qué evidencia respalda sus relaciones?

58

entradas de ransomware sobre Perú, cada una una afirmación delictiva

7.1 Entradas de ransomware y contexto regional 51
7.2 Etiquetas de actores y respuesta que justifican 53
7.3 Tres observaciones de entradas en el periodo reciente 55
7.4 Investigación de espionaje que incluye a Perú 55
7.5 Matriz de técnicas y validación autorizada 56
7.6 Una investigación reciente de malware no cuenta víctimas de noviembre 57
7.7 Mapa de relaciones y límites de evidencia 58

CAPÍTULO 07

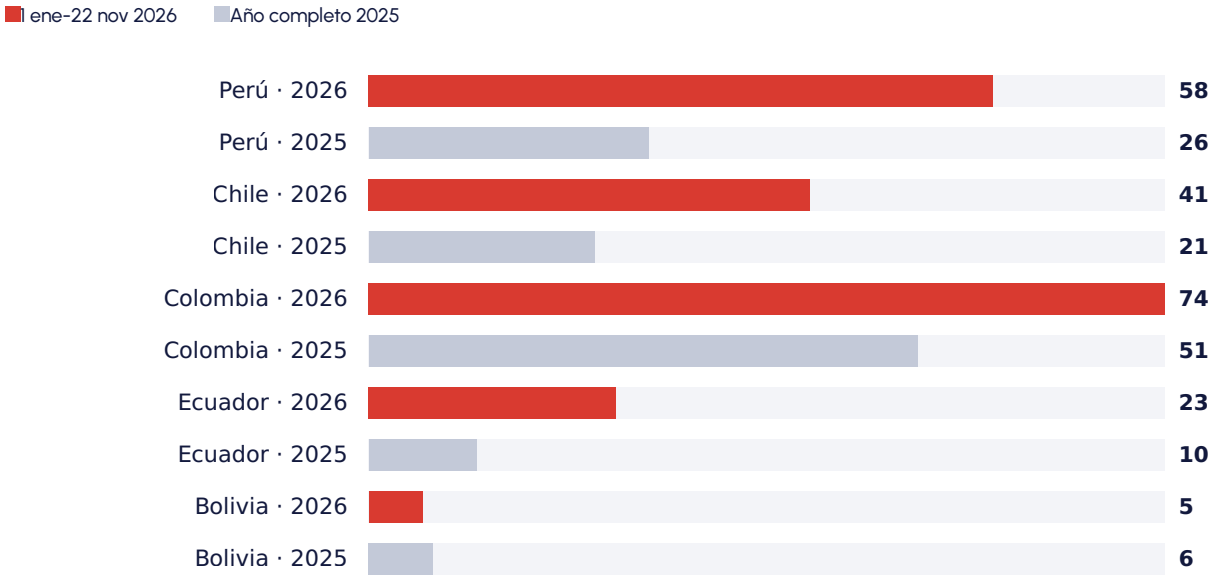
Actores, ransomware y relaciones respaldadas

EN RESUMEN

Ransompedia registra 58 entradas sobre Perú con 20 etiquetas de actores. Qilin, The Gentlemen y Nova reúnen 28. No son intrusiones comprobadas ni organizaciones únicas. Investigaciones separadas de proveedores incluyen a Perú en una campaña de espionaje y una observación de malware de varios países. Atribuya cada evaluación a su fuente y prepare recuperación, investigación de identidad y revisión de dispositivos sin asumir un operador común entre poblaciones.

7.1 Entradas de ransomware y contexto regional

Perú tiene 58 entradas en el periodo; los pares describen poblaciones visibles diferentes



El periodo de 2026 es parcial; la comparación de 2025 cubre el año completo. Los conteos describen visibilidad de la fuente, no una clasificación nacional de riesgo. Fuente: Brandefense Ransompedia, 1 de enero-22 de noviembre de 2026; noviembre parcial [S2]. Las entradas siguen siendo afirmaciones delictivas.

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

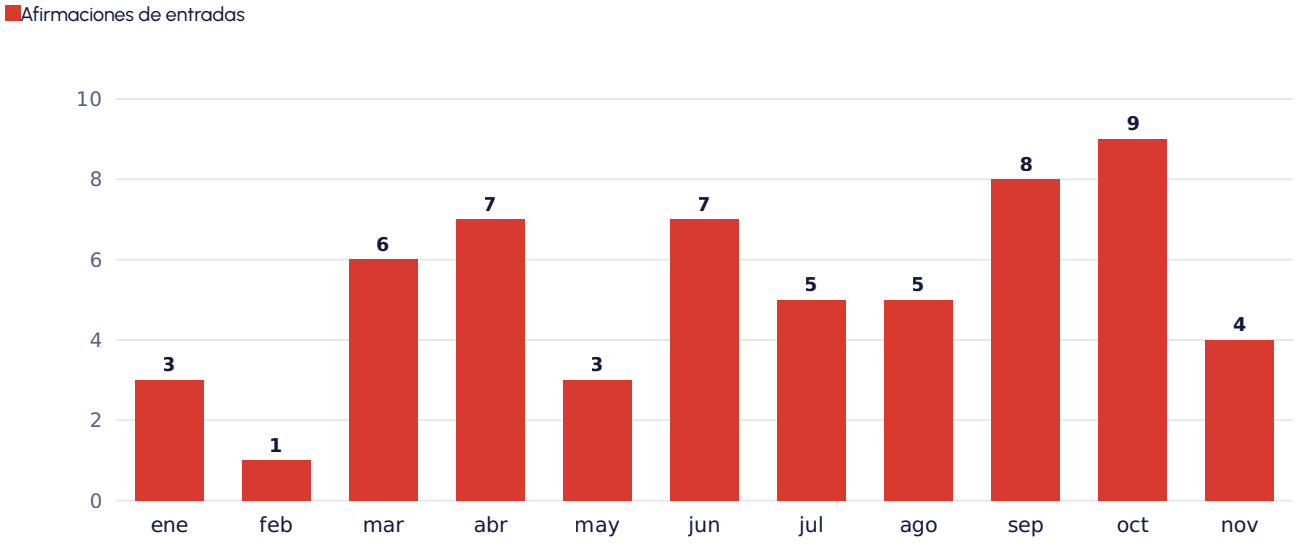
País	Entradas del periodo solicitado de 2026	Entradas de todo 2025
Perú	58	26
Chile	41	21
Colombia	74	51
Ecuador	23	10
Bolivia	5	6

Fuente: Brandefense Ransompedia [S2]. Se compara un año parcial con uno completo. No es una tasa de crecimiento de periodos equivalentes. Las cifras no se ajustan por tamaño del país, población sectorial ni prácticas de divulgación.

La población puede repetir una organización, usar nombres relacionados o cambiar de etiqueta sectorial. Una entrada pública establece una afirmación de extorsión. No demuestra cifrado, autenticidad o cantidad del material robado, pago ni una organización afectada única.

La revisión pública también encontró diferencias entre presunta fecha del ataque, fecha de entrada y descubrimiento por un agregador. No son intercambiables. El informe usa la fecha propia de entrada para esa población y separa las fechas de incidentes confirmados.

Las observaciones de entradas se distribuyen durante el año; noviembre es parcial



Fuente: Brandefense Ransompedia, 1 de enero-22 de noviembre de 2026; noviembre parcial [S2]. Las entradas siguen siendo afirmaciones delictivas.

Mes	Entradas	Mes	Entradas
Enero	3	Julio	5
Febrero	1	Agosto	5
Marzo	6	Septiembre	8
Abril	7	Octubre	9
Mayo	3	Noviembre hasta el corte	4
Junio	7	Total	58

Fuente: Brandefense Ransompedia [S2]. El patrón mensual de entradas no es un patrón de inicio de intrusiones. El máximo observado no establece cuándo se accedió por primera vez a las organizaciones mencionadas.

7.2 Etiquetas de actores y respuesta que justifican

Etiqueta de la entrada	Entradas sobre Perú	Interpretación
Qilin	16	Etiqueta más frecuente en esta población
The Gentlemen	7	Observaciones separadas de una etiqueta de extorsión
Nova	5	Observaciones separadas de una etiqueta de extorsión
SafePay	3	Incluye una entrada reciente de servicios financieros
RansomHouse	3	Las observaciones repetidas de salud exigen cuidado al interpretar incidentes únicos
DragonForce	3	Afirmaciones de entradas, no una vía de acceso confirmada independientemente
Kazu	3	Las etiquetas de servicios de salud relacionados no establecen víctimas independientes
APT73	3	La presencia de la etiqueta no establece atribución estatal
Otras etiquetas	15	Observaciones restantes con 12 etiquetas
Total	58	Entradas, no organizaciones independientes

Fuente: Brandefense Ransompedia [S2]. Las primeras tres etiquetas reúnen 28 de 58 observaciones, o 48,3%. Las 30 restantes corresponden a otras etiquetas. La tabla no establece cuántas personas operan cada nombre.

Qilin

Etiqueta de entradas de extorsión | No se evalúa una atribución estatal

EN PERÚ, 2026

2026

16 entradas del Perú en el periodo solicitado

OBJETIVOS REIVINDICADOS

Funciones sectoriales generales; sin nombres de víctimas no verificados

EN FUENTES PÚBLICAS

[S2] Ransompedia registra 16 entradas.

NUESTRA VALORACIÓN

Prepare decisiones validadas de recuperación y divulgación; una entrada no establece cifrado, robo, un operador común ni pago.

CONFIANZA
Alta respecto del conteo observado; las afirmaciones subyacentes siguen siendo afirmaciones

The Gentlemen

Etiqueta de entradas de extorsión | No se evalúa una atribución estatal

EN PERÚ, 2026

2026
7 entradas del Perú en el periodo solicitado

OBJETIVOS REIVINDICADOS

Funciones sectoriales generales; sin nombres de víctimas no verificados

EN FUENTES PÚBLICAS

[S2] Ransompedia registra 7 entradas.

NUESTRA VALORACIÓN

Prepare decisiones validadas de recuperación y divulgación; una entrada no establece cifrado, robo, un operador común ni pago.

CONFIANZA
Alta respecto del conteo observado; las afirmaciones subyacentes siguen siendo afirmaciones

Nova

Etiqueta de entradas de extorsión | No se evalúa una atribución estatal

EN PERÚ, 2026

2026
5 entradas del Perú en el periodo solicitado

OBJETIVOS REIVINDICADOS

Funciones sectoriales generales; sin nombres de víctimas no verificados

EN FUENTES PÚBLICAS

[S2] Ransompedia registra 5 entradas.

NUESTRA VALORACIÓN

Prepare decisiones validadas de recuperación y divulgación; una entrada no establece cifrado, robo, un operador común ni pago.

CONFIANZA
Alta respecto del conteo observado; las afirmaciones subyacentes siguen siendo afirmaciones

La recuperación no debería depender de qué grupo nombre a una organización. Valide efectos reales sobre sistemas y datos, conserve la entrada pertinente y pruebe la restauración desde una copia protegida. Comunicaciones y asesoría legal deberían separar la afirmación delictiva del impacto confirmado.

7.3 Tres observaciones de entradas en el periodo reciente

Fecha de entrada	Función general	Etiqueta del actor	Estado
2026-11-11	Administración pública local	The Gentlemen	Afirmación de entrada; no se establece confirmación oficial de incidente
2026-11-16	Servicios de medios y comunicaciones	Qilin	Afirmación de entrada; no se establece confirmación oficial de incidente
2026-11-21	Servicios financieros	SafePay	Afirmación de entrada; no se establece confirmación oficial de incidente

Fuente: Brandefense Ransompedia [S2]. Otra entrada farmacéutica del 7 de noviembre queda fuera del periodo reciente. Aparecer en noticias posteriores no cambia esa fecha.

Las tres filas forman parte del total de 58. No son incidentes adicionales para sumar a los casos de publicaciones o reportes públicos. Las funciones de las víctimas se mantienen generales; no se publican destinos delictivos ni enlaces a archivos expuestos.

7.4 Investigación de espionaje que incluye a Perú

La investigación de ESET del 17 de septiembre describe despliegues de SparroWocky contra entidades gubernamentales en Perú dentro de una campaña de 2025–2026. ESET atribuye la campaña a FamousSparrow y lo describe como un grupo de ciberespionaje vinculado a China. La atribución sigue siendo la evaluación de ESET. [S31]

El informe de ESET del 28 de octubre para Q2–Q3 2026 reporta actividad continuada de FamousSparrow en Sudamérica entre abril y septiembre de 2026, sin dar un conteo del Perú [S45]. Ese seguimiento marca un límite de visibilidad por país y no evidencia de incidentes adicionales en el Perú.

FamousSparrow

Campaña de espionaje atribuida por un proveedor | Vinculado a China, según la evaluación de ESET

EN PERÚ, 2026

2025–2026
ESET incluye al Perú en su información regional sobre la campaña

OBJETIVOS REIVINDICADOS

Entidades de gobierno, según ESET; sin víctima peruana nombrada

EN FUENTES PÚBLICAS

[S31] Investigación de proveedor; la atribución sigue siendo la evaluación de la fuente.

[S45] La actualización de octubre para Q2–Q3 2026 señala actividad continuada en Sudamérica sin conteo del Perú.

NUESTRA VALORACIÓN

Revise equipos y aplicaciones propios pertinentes. No se establece una frecuencia de técnicas específica del Perú.

CONFIANZA
Evaluación de campaña atribuida a la fuente

El informe no convierte esa investigación regional en una víctima peruana identificada, un total nacional ni prueba de que cada técnica ocurriera en Perú. Tampoco adopta la explicación geopolítica de la fuente. La campaña y los anuncios clandestinos son poblaciones separadas.

7.5 Matriz de técnicas y validación autorizada

TÉCNICAS CITADAS EN LA INVESTIGACIÓN DEL PROVEEDOR, POR TÁCTICA

Acceso inicial	Persistencia	Recopilación
T1190 Explotación de aplicación pública	T1543.003 Servicio de Windows	T1113 Captura de pantalla

Mapa de campaña y capacidades del proveedor; no es una tabla de frecuencia en el Perú. [S31]

Técnica identificada por el proveedor	Alcance	Tarea de validación sugerida
T1190: explotación de aplicaciones públicas	Relación de la campaña de ESET [S31]	Inventariar aplicaciones propias y revisar actividad pertinente de servidores
T1543.003: persistencia mediante servicios de Windows	Capacidad descrita por ESET [S31]	Comparar servicios nuevos o modificados con despliegues aprobados
T1113: captura de pantalla	Capacidad descrita por ESET [S31]	Correlacionar capturas inesperadas con contexto del dispositivo y software autorizado

La matriz relaciona investigación del proveedor con técnicas; no es una tabla de frecuencias en Perú. Las tareas son preguntas defensivas de revisión. No se afirma disponer de una regla de producción ni un resultado de validación en un motor.

Una revisión útil combina observaciones y las compara con administración aprobada. Instalar un servicio o disponer de captura de pantalla puede tener explicaciones legítimas. Confirme contexto del proceso, responsable del negocio y actividad relacionada antes de atribuir un actor por una sola observación.

7.6 Una investigación reciente de malware no cuenta víctimas de noviembre

La publicación de Kaspersky del 16 de noviembre informa de unos 15 000 intentos Retadup bloqueados en varios países entre enero y septiembre de 2026, incluido Perú. Describe propagación por USB y distribución de CoffeeLoader. La cifra no es un total peruano ni infecciones exitosas. [S32]

Retadup / CoffeeLoader

Relación de malware en investigación de proveedor | No se evalúa una atribución estatal

EN PERÚ, 2026

2026-11-16
Publicación sobre intentos anteriores en varios países

OBJETIVOS REIVINDICADOS

Los países incluyen al Perú; sin conteo nacional de víctimas

EN FUENTES PÚBLICAS

[S32] Investigación de Kaspersky; se distinguen intentos e infecciones.

NUESTRA VALORACIÓN

Revise el manejo de medios extraíbles y el contexto de los equipos con pruebas autorizadas.

CONFIANZA
Investigación de malware atribuida a la fuente

Esto añade una revisión de medios extraíbles a las decisiones recientes. Los responsables deberían controlar el ingreso de dispositivos de almacenamiento antiguos y probar la respuesta mediante un ejercicio autorizado. La fecha de publicación de noviembre no debe asignarse a todos los intentos reportados.

7.7 Mapa de relaciones y límites de evidencia

Etiqueta MortemTeam

Marca en publicaciones conservadas de foro | No se establece motivación ni atribución estatal

EN PERÚ, 2026

2026-11-08
Afirmación sobre registros empresariales, B07

2026-11-13
Afirmación sobre datos educativos, B08

OBJETIVOS REIVINDICADOS

Temas generales de registros públicos y educación

EN SUS PROPIAS PALABRAS

"Data Included: [business identifier], Legal Name"
B07

EN FUENTES PÚBLICAS

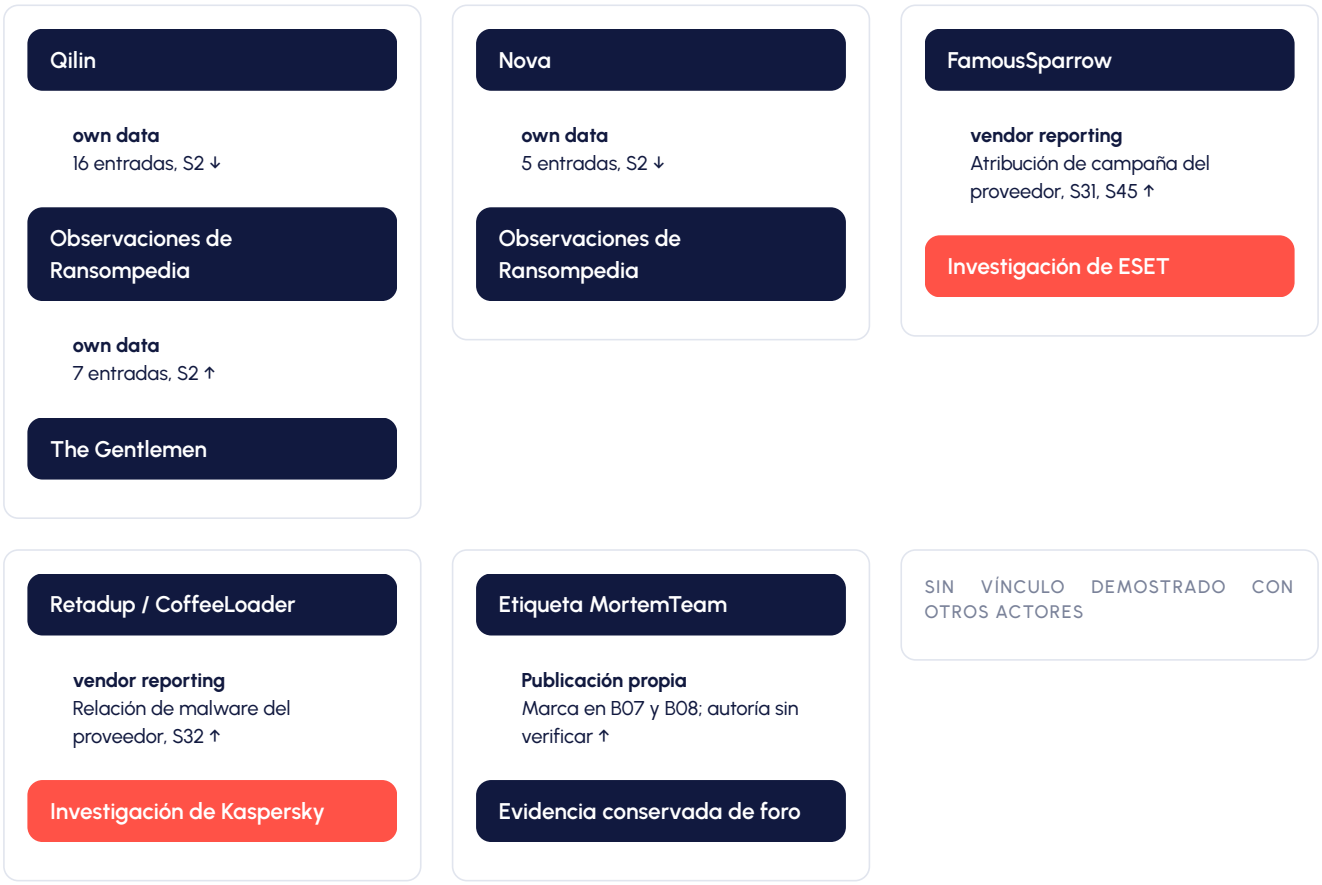
[S1] La etiqueta aparece en los textos; su autoría no está establecida independientemente.

NUESTRA VALORACIÓN

Una etiqueta común no establece un operador común, archivos idénticos ni una intrusión verificada.

CONFIANZA
Alta respecto de la marca visible; autoría y afirmaciones subyacentes sin verificar

Publicación propia · Reenvío · Declaración oficial · Información pública · Nuestra observación



El mapa conecta cada etiqueta o campaña con su fuente. Las relaciones de Ransompedia son **datos propios**. Las de ESET y Kaspersky son **reportes de proveedores**. Las relaciones de marca en foros describen una etiqueta en una publicación, no autoría comprobada. [S1][S2][S31][S32][S45]

No hay una relación respaldada de operador común entre etiquetas de extorsión, publicaciones educativas con marca de grupo, la campaña de espionaje y Retadup. Compartir país no establece ese vínculo. Toda relación futura necesita un elemento común concreto y su propia evaluación de confianza.

CONCLUSIONES CLAVE

01

Las 58 entradas siguen siendo afirmaciones y pueden repetir organizaciones.

02

La atribución y las capacidades del proveedor conservan límites de campaña y geografía.

03

Prepare recuperación y revisión de dispositivos sin asumir un operador común entre poblaciones ajenas.

CAPÍTULO 08

Economía del fraude: identidad, persuasión y pagos

ESTE CAPÍTULO RESPONDE

¿Cómo pueden los datos y mensajes aparentemente confiables crear riesgo de fraude sin probar una intrusión original?

15

registros distintos de tarjetas en observaciones limitadas de publicaciones conservadas

8.1 Modelo analítico, no cadena de transacciones observada 61
8.2 Las observaciones de tarjetas tienen alcance limitado 61
8.3 Venta de identidades y certificados 62
8.4 La suplantación puede utilizar una imagen de autoridad 62
8.5 Temas institucionales y señuelos de multas de transporte 62
8.6 Los precios anunciados no son valor de mercado realizado 63

CAPÍTULO 08

Economía del fraude: identidad, persuasión y pagos

EN RESUMEN

La evidencia separa anuncios de identidades, ofertas de acceso, alertas de suplantación y transferencias reportadas como no autorizadas. Son etapas distintas; no establecen una cadena delictiva conectada. La respuesta consiste en validar la cuenta o información y ofrecer a clientes una vía confiable de comprobación. Autentique los cambios de pago y recuperación de cuentas mediante un canal independiente de confianza.

8.1 Modelo analítico, no cadena de transacciones observada

Un modelo útil de planificación tiene cuatro etapas: información que da credibilidad al relato, un contacto persuasivo, una decisión de cuenta o autorización y un pago o transferencia de datos. Es un **modelo analítico**. El informe no establece un operador común, una venta realizada ni una cadena causal entre los ejemplos.

Las afirmaciones de registros ciudadanos y laborales ilustran información anunciada. La alerta de Petroperú ilustra un intento de suplantación reconocido públicamente. El reporte de transferencias de salud ilustra un evento financiero comunicado. Cada uno respalda un control diferente; combinarlos exageraría la evidencia. [S1][S20] [S23]

Ante alertas de información, valide procedencia y antigüedad. Ante contactos persuasivos, confirme la solicitud por un canal conocido. Para decisiones sobre cuentas, revise privilegios reales y cambios recientes. Para pagos, conserve aprobaciones y evidencia de beneficiarios mientras contacta a la entidad financiera por vías establecidas.

8.2 Las observaciones de tarjetas tienen alcance limitado

ALCANCE DE LAS CIFRAS DE TARJETAS

Las publicaciones revisadas contienen 15 observaciones de registros de tarjetas. Su validez, titularidad y uso no están verificados. Esta población limitada no permite estimar la exposición nacional de tarjetas ni las pérdidas por fraude.

Las observaciones contienen 15 registros distintos de tarjetas en 13 publicaciones, con 16 apariciones. Seis registros tienen asociación con un emisor y nueve no. Son grupos excluyentes que suman 15. No se establece validez, titularidad de la cuenta ni uso real. [S1]

Un estado de verificación o la afirmación de que una tarjeta está «activa» sigue siendo lo dicho por quien publica. No es evidencia independiente de autorización exitosa, compra realizada ni pérdida económica. Los emisores deberían validar alertas con sus propios registros antes de contactar clientes, restringir o reemitir.

Las observaciones asociadas a emisores y la selección de dominios financieros del capítulo 9 son poblaciones distintas. No establecen una unión entre un titular, dispositivo y organización concretos. No se publican datos de tarjetas, identificadores individuales de cuentas ni estimación de pérdidas nacionales.

8.3 Venta de identidades y certificados

El operativo oficial de julio describe presuntas ventas ilegales de datos personales y certificados falsos. Por separado, los casos clandestinos anuncian información ciudadana, de prestaciones y laboral. No se establece que el operativo correspondiera a esos anuncios o archivos. [S22][S1]

El formato aparentemente oficial de un documento no resuelve una decisión de identidad. Los procesos de clientes y personal deberían verificar documentos importantes con el emisor legítimo o mediante un procedimiento aprobado. Registre el resultado sin distribuir material personal innecesario a un grupo de respuesta más amplio.

Teléfonos y detalles de recuperación también necesitan responsable. Que un interlocutor conozca la historia personal no significa que haya superado una verificación independiente. Defina qué cambios requieren otro factor o vía confiable, sobre todo cuando afectan pagos o accesos privilegiados.

8.4 La suplantación puede utilizar una imagen de autoridad

La alerta oficial de Petroperú respalda una decisión concreta de marca: publicar el proceso real y ofrecer comprobación independiente. No demuestra intrusión en la empresa ni un aumento nacional medido del fraude asistido por IA. [S20]

La lección es de verificación. El personal no debería aceptar un rostro, voz o cargo ejecutivo familiar como aprobación suficiente de un pago o cambio de cuenta. Mantenga el proceso establecido aunque la solicitud parezca urgente o llegue por un canal inusual.

Para clientes, una alerta útil identifica qué acción evitar y qué vía legítima utilizar. No debería repetir contactos fraudulentos, dirigir hacia páginas del actor ni prometer que todo engaño se reconoce por su calidad visual.

8.5 Temas institucionales y señuelos de multas de transporte

El reporte de agosto del diario oficial describe una alerta de suplantación de multas de transporte mediante mensa-
jes, enlaces y códigos QR. Aporta contexto de campaña, no un recuento de intrusiones de red confirmadas. [S26]

Un tema de servicio público puede inducir una acción sin explotar una vulnerabilidad en la institución suplantada. Atención al cliente debería explicar cómo comprobar un aviso legítimo de manera independiente. Seguridad debería conservar reportes y coordinar solicitudes de retiro mediante el procedimiento autorizado.

El informe no infiere motivo ni nacionalidad del idioma de un mensaje. Un logotipo institucional o plazo administrativo plausible es parte de la afirmación que se evalúa. No prueba que el mensaje provenga de la institución.

8.6 Los precios anunciados no son valor de mercado realizado

Fecha de publicación	Tipo de oferta	Precio anunciado	Qué no se establece
2026-02-10	Acceso privilegiado a un servicio público	200 USD	Acceso funcional, alcance, posesión y venta
2026-03-27	Acceso comercial y registros operativos	20 000 USD, negociables	Privilegios actuales, autenticidad documental y venta

Fuente: anuncios conservados [S1]. Son dos precios seleccionados de los casos. No establecen mediana nacional, transacción realizada, rango representativo ni valor económico del material ofrecido.

Un precio alto no valida posesión. Uno bajo no demuestra fabricación. Evalúe la afirmación con evidencia propia pertinente y conserve el precio solo como parte de lo afirmado por el vendedor.

CONCLUSIONES CLAVE

01

La secuencia de información a pago es un modelo de planificación, no una cadena delictiva demostrada.

02

Los 15 registros de tarjetas pertenecen a una población limitada de publicaciones; su validez, titularidad y uso siguen sin verificarse.

03

Mantenga verificación independiente de documentos, cambios de cuentas y pagos, aunque la solicitud parezca autorizada.

CAPÍTULO 09

Banca y protección del cliente

09

ESTE CAPÍTULO RESPONDE

¿Qué decisiones financieras se desprenden de la evidencia sin inventar un total bancario de exposición?

25

dominios candidatos financieros y de seguros en la selección

9.1 Alcance y resultados disponibles 65

9.2 Acceso en la aseguradora y orientación a clientes 66

9.3 La revisión de pagos corresponde al titular de la cuenta 66

9.4 Los incidentes históricos deben seguir siendo históricos 67

9.5 Finanzas abiertas y preparación para la supervisión 67

9.6 Qué probar con el responsable del servicio financiero 67

CAPÍTULO 09

Banca y protección del cliente

EN RESUMEN

La selección financiera contiene 25 dominios candidatos; la población limitada de tarjetas y los eventos públicos financieros tienen otras unidades. Hay señales de exposición, pero ninguna vinculación individual entre clientes, tarjetas y equipos. El reporte de la aseguradora, las transferencias de salud y el seguimiento bancario histórico respaldan decisiones distintas de privacidad, pagos y cronología. Valide evidencia vigente de cuentas propias, conserve las autorizaciones y distinga un incidente de información de una caída o intrusión en sistemas bancarios.

9.1 Alcance y resultados disponibles

Población	Afirmación disponible	Límite
Dominios financieros y de seguros	25 candidatos	Servicios relacionados e independencia jurídica sin validar
Exposición de credenciales y equipos	6 dominios con ofertas actuales; 24 con asociaciones de equipos; 24 con registros de credenciales	Asociaciones de dominios, no incidentes confirmados en sistemas bancarios
Población limitada de tarjetas en publicaciones	15 registros de tarjetas en las publicaciones conservadas del informe	No son clientes únicos, exposición nacional ni acceso a sistemas bancarios
Incidente de información de clientes	Un caso de aseguradora atribuido a las fuentes	No es una población completa de incidentes financieros
Evento de pagos de salud	Cinco transferencias cuestionadas de una cuenta institucional concreta	No demuestra intrusión en sistemas bancarios
Discusión bancaria histórica	Reporte posterior sobre un incidente anterior	No es una intrusión nueva establecida en 2026

El alcance de las observaciones seleccionadas no establece bancos independientes, clientes únicos ni intrusiones confirmadas. Las cifras separadas de tarjetas describen 15 observaciones de registros de tarjetas en las publicaciones revisadas. Su validez, titularidad y uso no están verificados. Esta población limitada no permite estimar la exposición nacional de tarjetas ni las pérdidas por fraude. [S1]

Las señales de dominios financieros y los registros de tarjetas siguen siendo poblaciones separadas



Los dominios candidatos y los registros de tarjetas asociados al emisor son poblaciones distintas; no se vinculan con clientes, cuentas ni dispositivos. Fuente: Odin by Brandefense, 250 dominios candidatos seleccionados, 22 de noviembre de 2026 [S3]. Las asociaciones pueden solaparse e incluir observaciones anteriores. [S1]

El grupo seleccionado de finanzas y seguros tiene 25 dominios. Las ofertas actuales corresponden a 6; las asociaciones de equipos, a 24; las de equipos etiquetadas como de empleados, a 20; y las de registros de credenciales, a 24. Estas señales requieren validación propia y no establecen bancos independientes ni clientes afectados. [S3]

9.2 Acceso en la aseguradora y orientación a clientes

El reporte de octubre establece una investigación de confidencialidad aunque el supervisor no informó de una interrupción significativa. No establece un total final de clientes ni la cantidad anunciada por el actor. El capítulo 5 conserva esos límites. [S18]

La respuesta debería identificar qué pueden hacer los clientes de manera útil. Si se valida afectación de datos de contacto o pólizas, advierta sobre suplantaciones plausibles con esas categorías. No implique exposición de todas las credenciales financieras ni necesidad de reemplazar todo medio de pago.

Un aviso debería ofrecer contacto independiente, explicar categorías conocidas e identificar lo pendiente. Atención al cliente debería conservar los reportes de fraude recibidos para que el equipo distinga el uso indebido previsto de eventos posteriores reales.

9.3 La revisión de pagos corresponde al titular de la cuenta

Las transferencias de salud muestran por qué importan titularidad institucional y autorización. Un reclamo contra una contraparte bancaria no prueba una intrusión en ese banco. Tesorería y el responsable de seguridad deberían conservar los registros reales de pagos y aprobaciones. [S23]

Revise quién podía crear o modificar beneficiarios, aprobar operaciones, cambiar autenticación o aplicar una excepción de emergencia. Confirme que la vía de contacto confiable funcione sin el correo habitual. Registre el resultado de una solicitud de recuperación sin prometer reversión.

Cuando restringir una cuenta proteja la investigación, el responsable del negocio debería decidir cómo mantener pagos esenciales legítimos. Una alternativa controlada necesita aprobador identificado y trazabilidad. El informe no establece que una institución concreta careciera de esos controles.

9.4 Los incidentes históricos deben seguir siendo históricos

La discusión bancaria de noviembre trata un incidente anterior y un proceso regulatorio. No se considera una intrusión nueva confirmada en 2026. El informe no emite una conclusión jurídica final de responsabilidad ni una exención general de sanciones. [S28]

Esto afecta monitoreo y comunicaciones. Un anuncio repetido puede exigir revisar usos indebidos actuales sin crear un evento nuevo en el sistema fuente. Relaciónelo con divulgaciones previas solo con respaldo, conservando incertidumbre sobre el archivo o cuenta real.

El registro debería permitir tanto la fecha del evento subyacente como la publicación nueva. La respuesta puede ser actual y el material histórico. El cliente no debería recibir una declaración engañosa de intrusión nueva solo porque una noticia anterior vuelve a circular.

9.5 Finanzas abiertas y preparación para la supervisión

La hoja de ruta de febrero del supervisor describe un desarrollo de finanzas abiertas por fases. Las fases futuras no se presentan como controles implementados. Identifique los servicios y permisos de terceros que realmente opera, sin asumir que una hoja de ruta ya cambió todas las interfaces. [S29]

El reglamento vigente aborda autenticación, registros de acceso y responsabilidades de proveedores. Una revisión pertinente debería comprobar si la organización identifica al tercero autorizado, sus datos permitidos y el momento en que se revoca el acceso. [S7]

Para reportar incidentes, use la norma vigente y el alcance real de supervisión. La propuesta de septiembre es un elemento a seguir. El capítulo 10 la separa de las obligaciones actuales y las futuras disposiciones de comunicación al cliente. [S8][S10]

9.6 Qué probar con el responsable del servicio financiero

Utilice como ejercicios separados una alerta sintética sobre información de clientes, un pago cuestionado y el retiro de acceso de un proveedor. Cada uno debería producir una decisión clara y responsable. Un ejercicio genérico de «filtración» puede ocultar sus diferencias.

En la alerta de información, identifique categorías y decisión de comunicación. En el pago, conserve evidencia de autorización y beneficiarios. Para el proveedor, demuestre el retiro de permisos y la continuidad legítima mediante la alternativa acordada.

Una métrica para el directorio puede mostrar alertas validadas pendientes, ejercicios completados y excepciones aceptadas. No debería sustituir la evidencia de controles efectivos por totales históricos de credenciales o volumen publicitario clandestino.

CONCLUSIONES CLAVE

01

Dominios financieros, tarjetas, clientes e incidentes bancarios son unidades diferentes.

02

La evaluación de privacidad y las autorizaciones de pago deben acompañar la contención técnica.

03

Conserve la cronología histórica y siga la norma de supervisión realmente vigente.

CAPÍTULO 10

Respuesta regulatoria y decisiones de notificación

10

ESTE CAPÍTULO RESPONDE

¿Qué obligaciones rigen y qué cambios requieren prepararse para una fecha posterior?

48 horas

máximos desde el conocimiento en dos regímenes diferentes

10.1 Tabla de aplicación 70
10.2 Los incidentes de datos personales necesitan una decisión fundamentada 71
10.3 La notificación de seguridad digital es una determinación distinta 71
10.4 Obligaciones financieras, propuestas y comunicaciones futuras 72
10.5 Qué debería demostrar un ejercicio de notificación 72

CAPÍTULO 10

Respuesta regulatoria y decisiones de notificación

EN RESUMEN

Las obligaciones peruanas de datos personales, servicios digitales y reportes financieros requieren determinar su aplicación por separado. Dos regímenes usan un máximo de 48 horas, pero difieren en alcance y destinatarios. El reporte financiero de ciberseguridad ya rige; el procedimiento unificado de septiembre se presentó como propuesta. Las modificaciones de comunicación a clientes tienen una vigencia posterior. Conserve el momento de conocimiento, determine la obligación y ensaye con proveedores y responsables del negocio.

Este capítulo orienta la planificación operativa. Asesoría legal debe determinar la aplicación según los textos oficiales vigentes y la función real de la organización. No reemplaza asesoramiento jurídico.

10.1 Tabla de aplicación

Instrumento	Estado y alcance	Desencadenante o plazo	Responsable operativo y evidencia
Decreto Supremo 016-2024-JUS, artículo 34	Reglamento de datos personales; vigente antes del periodo estudiado	Incidente que reúna las condiciones: ANPD dentro de 48 horas del conocimiento; un retraso necesita motivos	Privacidad y responsable del tratamiento; registro del conocimiento y justificación [S6]
Mismo reglamento, artículos 34–36	Son distintas las obligaciones del responsable, la comunicación a afectados y el deber del encargado	Comunicación al titular según afectación de derechos; el encargado informa al responsable inmediatamente	Privacidad, atención al cliente y proveedores; aviso delimitado y constancia [S6]
Decreto Supremo 126-2025-PCM, artículo 32	Reglamento del Marco de Confianza Digital, vigente desde el 2 de febrero de 2026	Incidentes críticos: CNSD dentro de 48 horas del conocimiento del proveedor; otros niveles siguen reglas aplicables	Oficial de seguridad digital y responsable del servicio; clasificación y registro [S5]
Resolución SBS 504-2021, artículo 15	Entidades financieras supervisadas comprendidas	Reportar al advertir un incidente significativo; importa el impacto adverso comprobado o presumible	Seguridad y cumplimiento; reporte e investigación forense [S7]

Instrumento	Estado y alcance	Desencadenante o plazo	Responsable operativo y evidencia
Procedimiento unificado de septiembre de SBS	Propuesta en consulta en el material verificado de septiembre	Las fases inicial, intermedia y final propuestas no se consideran aquí un reemplazo promulgado	Responsable regulatorio; verificar norma final antes de modificar plazos operativos [S8][S9]
Resolución SBS 01741-2026, artículos 55–56	Cambios de comunicación a clientes, con vigencia general a los 360 días de publicarse	Las disposiciones de comunicación de incidentes requieren preparación para vigencia posterior según el texto	Cumplimiento y comunicaciones; plan y comprobación de vigencia [S10]

10.2 Los incidentes de datos personales necesitan una decisión fundamentada

El artículo 34.1 establece desencadenantes alternativos. Incluyen exposición de grandes volúmenes por cantidad o tipo, gran número de afectados, datos sensibles o perjuicio evidente a otros derechos o libertades. Resolver internamente el incidente no elimina la notificación a ANPD cuando corresponde. El artículo 34.5 también contempla al CNSD cuando ocurre mediante el entorno digital. [S6]

La comunicación a personas afectadas tiene condición y excepción propias. Si se cumple la condición de afectación de derechos, el reglamento exige comunicar con claridad, sin dilación indebida y dentro de las 48 horas indicadas. El artículo 34.4 trata incidentes sin esa afectación y totalmente superados. [S6]

No reemplace la evaluación de datos por «sin interrupción del servicio». El caso de la aseguradora demuestra por qué disponibilidad y confidencialidad necesitan registros separados. Un servicio restablecido puede necesitar evaluación de afectados; una caída puede no implicar exposición personal.

10.3 La notificación de seguridad digital es una determinación distinta

El reglamento del Marco de Confianza Digital se publicó el 4 de noviembre de 2025. Su cláusula de 90 días sitúa la vigencia el 2 de febrero de 2026. El artículo 32 fija el máximo para incidentes críticos desde el conocimiento del proveedor. El artículo 34.4 trata la comunicación de sus proveedores al prestador del servicio. [S5]

En la práctica, se necesita obtener hechos oportunos de los proveedores. Contratos y contactos deberían identificar quién avisa al responsable del servicio, qué información está disponible y cómo llega una evaluación urgente a quien notifica. No espere una afirmación delictiva pública para definir el momento de conocimiento interno.

El registro debería distinguir criticidad, efecto real sobre el servicio y presencia de datos personales. Si aplican varias obligaciones, conserve destinatarios y determinaciones separados. La intervención de un regulador no cierra automáticamente las exigencias de otro.

10.4 Obligaciones financieras, propuestas y comunicaciones futuras

El reglamento SBS verificado ya exige reportar incidentes significativos y poner el informe forense a disposición del supervisor. Los efectos adversos enumerados incluyen pérdida de información, fraude, reputación e interrupción operativa. El deber no se limita a cifrado ni a una entrada pública de extorsión. [S7]

La propuesta de septiembre de 2026 buscó un procedimiento unificado de incidentes operacionales. El aviso del emisor describe consulta hasta el 16 de octubre. Los plazos propuestos de dos horas, cinco horas y un día hábil no deben incorporarse como obligaciones vigentes solo con esa evidencia. [S8][S9]

La Resolución 01741-2026 se publicó el 2 de julio. Su artículo tercero fija una espera general de 360 días, con excepciones inmediatas ajenas a los artículos de comunicación de incidentes. La cláusula sitúa los artículos 55–56 el 27 de junio de 2027. [S10]

Esas disposiciones separan comunicación masiva dentro de 24 horas y directa dentro de 10 días hábiles, con ampliación justificada de otros 10 días hábiles. Atienden condiciones especificadas de impacto y significancia. Prepare los canales, pero verifique modificaciones y aplicación antes de activar un plazo legal. [S10]

10.5 Qué debería demostrar un ejercicio de notificación

Elija un incidente sintético de proveedor con un servicio crítico y posibles datos de clientes. Registre cuándo el prestador sabe lo suficiente para comenzar a evaluar. Pida a cada responsable indicar desencadenante, destinatario, máximo aplicable y hechos faltantes.

El ejercicio debería producir una decisión breve y aprobada. Incluya hechos conocidos, persona jurídica, servicio y categorías, motivo para notificar o no, responsable y próxima actualización. Conserve un acuse real cuando se envíe una notificación.

Separe denuncias penales, asistencia técnica y mensajes públicos de las notificaciones regulatorias. Un operativo, una supervisión y una afirmación de vendedor son eventos probatorios distintos. Este informe no afirma una notificación salvo que la establezca la fuente citada.

CONCLUSIONES CLAVE

01

Máximos parecidos no crean deberes jurídicos idénticos.

02

Separe normas vigentes de consultas y fechas de vigencia posteriores.

03

Ensaye un registro común de hechos con responsables, destinatarios y decisiones de notificación diferenciados.

CAPÍTULO 11

11

Perspectivas y supuestos condicionales de planificación

ESTE CAPÍTULO RESPONDE

¿Qué preparativos se desprenden de la evidencia y qué cambiaría la evaluación?

4

escenarios condicionales con señales explícitas para decidir

11.1 Evaluaciones principales y sus límites 74

11.2 Cuatro escenarios condicionales 75

11.3 Qué cambia con el periodo reciente 75

11.4 Señales que este informe no puede proporcionar 76

CAPÍTULO 11

Perspectivas y supuestos condicionales de planificación

EN RESUMEN

Prepárese para la continuidad de anuncios de datos de identidad, afirmaciones de extorsión, incidentes de acceso de proveedores y fraude contextual. Son supuestos condicionales de planificación, no pronósticos de ataques nacionales. El material histórico puede servir para usos indebidos actuales, mientras una publicación reciente puede describir actividad anterior. Asigne a cada escenario un responsable, una señal que cambie la respuesta y una condición que reduzca la preocupación. Revise el plan con evidencia local validada.

11.1 Evaluaciones principales y sus límites

Evaluación	Confianza y fundamento	Qué podría cambiarla
Los nuevos anuncios pueden referirse a registros antiguos	Alta respecto de la conversación observada en enero; la identidad del archivo sigue sin resolverse [S1]	Registros propios validados y una cronología independiente de su adquisición
Las afirmaciones de acceso a servicios públicos merecen validación por cuenta	Alta respecto de la existencia del anuncio; baja respecto de la utilidad del acceso [S1]	Evidencia autorizada del estado de la cuenta y de sus inicios de sesión
La respuesta de confidencialidad puede seguir siendo necesaria sin una interrupción importante	Alta respecto del relato de la aseguradora, con la atribución de la fuente [S18]	Una actualización posterior que establezca categorías o efectos diferentes
Varias etiquetas de extorsión requieren preparación para la recuperación	Alta respecto de la población de entradas, no de cada afirmación subyacente [S2]	Efectos locales validados o correcciones autorizadas de una entrada
La revisión de medios extraíbles debe acompañar la seguridad de cuentas	Respaldada por la investigación citada; la escala específica del Perú es desconocida [S32]	Evidencia de equipos propios y del uso real de medios extraíbles en la organización

La confianza corresponde a una proposición. Tener confianza en la existencia de una publicación no implica confiar en la exactitud de su contenido. La atribución de una fuente se mantiene como su evaluación, sin convertirla en un hallazgo independiente de este informe.

11.2 Cuatro escenarios condicionales

Supuesto de planificación	Señal que aumenta la preocupación	Responsable y acción	Señal que reduce la preocupación
Se reutilizan datos históricos de identidad en un contacto convincente	Aparece información propia validada junto con una solicitud sospechosa de acceso o pago	Fraude y atención al cliente autentican la solicitud por una vía independiente y conservan la evidencia	El material no guarda relación o ya fue remediado, sin evidencia actual de uso indebido
Una cuenta privilegiada anunciada sigue funcionando	La cuenta propia está activa, coincide de manera adecuada y presenta accesos preocupantes	Identidad y respuesta a incidentes contienen la cuenta y las sesiones validadas	La cuenta está inactiva o no guarda relación y se documenta la conclusión
Una cuenta de proveedor puede emitir mensajes confiables o modificar un servicio crítico	Se confirma actividad inesperada del proveedor o un mensaje no autorizado	Los responsables del servicio y del proveedor suspenden el privilegio pertinente y activan una corrección o una vía alternativa	Las acciones revisadas están autorizadas y la vía de emisión supera la prueba de reapertura
Una organización incluida en una entrada de ransomware enfrenta un evento real de continuidad o pérdida de información	La investigación interna establece sistemas, registros o funciones afectados	El mando del incidente prueba la restauración segura y activa decisiones delimitadas sobre privacidad y clientes	La evidencia reduce el alcance del evento o la afirmación concreta recibe una corrección creíble

Estos escenarios no establecen que los anuncios revisados causaran los eventos públicos. Identifican condiciones ante las cuales un responsable de seguridad debe cambiar una decisión operativa. Su valor está en una señal observable y en la evidencia de cierre, no en una probabilidad sin respaldo.

11.3 Qué cambia con el periodo reciente

La quincena final añade anuncios de registros empresariales, gestión educativa e historiales laborales. También incluye tres entradas de ransomware y una investigación de proveedor sobre intentos anteriores de malware. Son aportes distintos a la visibilidad, no un total conjunto de nuevos incidentes. [S1][S2][S32]

La respuesta inmediata consiste en asignar cada señal pertinente a su responsable de validación. Una afirmación sobre datos escolares requiere revisar los datos y la protección de las personas si se validan los registros. Una afirmación sobre cuentas requiere evidencia de su estado y uso actuales. Una entrada de ransomware requiere evaluar el efecto interno y decidir sobre continuidad.

Un desmentido reciente también debe cambiar la redacción. Conserve la procedencia alegada y la respuesta de la autoridad o empresa, sin tratar ninguna como sustituto de una validación independiente del archivo. Así el análisis sigue siendo útil mientras la proposición subyacente permanezca sin resolver.

11.4 Señales que este informe no puede proporcionar

La evidencia disponible no establece pérdidas nacionales, probabilidad de ataque, personas afectadas únicas ni un censo completo de intrusiones. Tampoco establece un operador común entre las poblaciones revisadas ni un efecto en un resultado electoral.

No se deriva un pronóstico del idioma de una fuente, del precio de un vendedor ni de una gran cantidad anunciada de registros. La cartera de exposición es seleccionada y tiene límites propios de cobertura. Los valores no disponibles no permiten establecer una tendencia nacional.

Los responsables deben revisar los escenarios cuando llegue nueva evidencia propia. Una actualización debe indicar qué proposición cambió, qué evidencia la modificó y qué decisión de respuesta corresponde. Conserve la incertidumbre anterior en lugar de reescribir una afirmación histórica como si siempre hubiera estado confirmada.

CONCLUSIONES CLAVE

01

Los escenarios condicionales necesitan una señal observable y un responsable.

02

Una publicación reciente no establece automáticamente una adquisición o intrusión reciente.

03

Cambie la respuesta cuando cambie la evidencia y registre el motivo.

CAPÍTULO 12

Plan de acción de 30/60/90 días

ESTE CAPÍTULO RESPONDE

¿Quién actúa sobre la evidencia y qué demuestra el cumplimiento?

18

acciones condicionales con responsables y evidencia de cumplimiento

12.1 Etapas de acción 78

12.2 Primeras decisiones por función 81

12.3 Cuadro de cumplimiento 81

12.4 Cómo puede ayudar Brandefense 82

CAPÍTULO 12

Plan de acción de 30/60/90 días

EN RESUMEN

Comience con una vía confiable para las alertas pertinentes y luego valide la cuenta, información o efecto en el servicio. En paralelo, prepare decisiones de continuidad y notificación con los responsables del negocio y los proveedores. El plan propone metas de gestión, no plazos legales ni afirmaciones sobre controles existentes. Conserve las excepciones y la evidencia de cada resultado. Asigne responsables y pruebe el servicio de mayores consecuencias antes de ampliar el programa.

12.1 Etapas de acción

1Días 1–30

Confirmar una vía para alertas pertinentes sobre cuentas y datos; investigar una alerta sintética

RESPONSABLE

CISO y responsable de inteligencia

EVIDENCIA DE CUMPLIMIENTO

La alerta llega al responsable designado y recibe una conclusión documentada

Validar las cuentas propias cuando se recibe una oferta actual pertinente

RESPONSABLE

Responsable de identidad

EVIDENCIA DE CUMPLIMIENTO

Se registran titularidad, estado, privilegios, uso reciente y remediación anterior

Revocar sesiones y autorizaciones de autenticación pertinentes cuando la evidencia validada requiere contención

RESPONSABLE

Identidad y respuesta a incidentes

EVIDENCIA DE CUMPLIMIENTO

Una prueba demuestra la retirada del acceso; se documenta la recuperación legítima

Inventariar privilegios de proveedores sobre servicios críticos y emisión de mensajes confiables

RESPONSABLE

Responsables del servicio y del proveedor

EVIDENCIA DE CUMPLIMIENTO

Se registran cuentas, autoridad para suspender, contactos y alternativa

Mapear deberes aplicables de notificación sobre datos personales, servicios digitales y actividad financiera

RESPONSABLE

Legal, privacidad y cumplimiento

EVIDENCIA DE CUMPLIMIENTO

Se registran condiciones de conocimiento, destinatarios, responsables y textos vigentes

Conservar la aprobación independiente de pagos y cambios de beneficiario durante un incidente

RESPONSABLE

Tesorería y responsable de fraude

EVIDENCIA DE CUMPLIMIENTO

Una solicitud sintética recibe la verificación separada requerida

2Días 31–60

Probar un servicio crítico sin su dependencia habitual de identidad

RESPONSABLE

Continuidad del negocio y responsable del servicio

EVIDENCIA DE CUMPLIMIENTO

Se demuestran el servicio mínimo seguro y los criterios de reapertura

Probar la suspensión del acceso pertinente de un proveedor y un mensaje confiable de corrección

RESPONSABLE

Responsables del proveedor y de comunicaciones

EVIDENCIA DE CUMPLIMIENTO

La suspensión y la corrección funcionan por la vía alternativa acordada

Delimitar datos personales validados por categoría real y grupo afectado

RESPONSABLE

Responsable de datos y de privacidad

EVIDENCIA DE CUMPLIMIENTO

Evaluación aprobada de categorías y fundamento de notificación

Probar la autorización de la aplicación cuando se valida una afirmación pertinente sobre educación o portales

RESPONSABLE

Responsable de la aplicación

EVIDENCIA DE CUMPLIMIENTO

Una revisión autorizada registra resultados y cierra la debilidad demostrada

Verificar la remediación soportada de PHP en instalaciones propias afectadas

RESPONSABLE

Responsables de infraestructura y aplicaciones

EVIDENCIA DE CUMPLIMIENTO

Se comprueba la versión en ejecución o el aviso aplicable del distribuidor después del cambio

Revisar el uso de medios extraíbles frente a los procesos reales de la organización

RESPONSABLE
Responsables de equipos y operaciones

EVIDENCIA DE CUMPLIMIENTO
Vía de manejo aprobada y ejercicio autorizado de detección

3Días 61–90

Restaurar un sistema crítico con una copia de recuperación protegida

RESPONSABLE
Responsables de recuperación y del negocio

EVIDENCIA DE CUMPLIMIENTO
El servicio completa su tarea crítica de forma aislada antes de la reapertura aprobada

Revisar remitentes autorizados antes de cambiar la aplicación de autenticación del correo

RESPONSABLE
Responsable de mensajería

EVIDENCIA DE CUMPLIMIENTO
Se documentan vías legítimas y pruebas controladas de suplantación

Ensayar una advertencia de suplantación al cliente mediante una vía independiente de contacto

RESPONSABLE
Atención al cliente y comunicaciones

EVIDENCIA DE CUMPLIMIENTO
Personal y clientes pueden encontrar y utilizar el proceso legítimo de verificación

Comparar anuncios históricos con avisos y remediaciones anteriores

RESPONSABLE
Responsables de inteligencia y de datos

EVIDENCIA DE CUMPLIMIENTO
Cada elemento pertinente se clasifica como actual, histórico, no relacionado o sin resolver, con su motivo

Revisar el registro de cambios regulatorios para normas finales y fechas de vigencia

RESPONSABLE
Responsable de cumplimiento

EVIDENCIA DE CUMPLIMIENTO
Estado actual y calendario de implementación aprobado

Presentar a la dirección los riesgos validados pendientes y las excepciones aceptadas

RESPONSABLE
CISO y responsables de riesgo del negocio

EVIDENCIA DE CUMPLIMIENTO
Decisiones firmadas con responsables, vencimientos y condiciones de revisión

Los periodos son metas propuestas de planificación. Los máximos legales aplicables pueden exigir actuar mucho antes; una cuenta privilegiada activa y validada puede requerir contención inmediata. No espere una etapa posterior del plan cuando la evidencia o el deber de notificación exijan actuar antes.

12.2 Primeras decisiones por función

Directorio y alta dirección. Pregunten qué servicio crítico ha superado un ejercicio de interrupción y reapertura. Asignen recursos a las dependencias pendientes y exijan un responsable para las excepciones aceptadas. No usen los conteos de publicaciones del informe como medida de eficacia de los controles.

CISO y mando del incidente. Confirmen la vía de alertas y el registro de decisiones. Separen la validación de cuentas, la delimitación de datos, la continuidad y las notificaciones. Registren qué proposición está establecida y qué evidencia cambiaría la respuesta.

SOC y equipos de identidad. Examinen inicios de sesión pertinentes, autorizaciones de sesión, cambios de privilegios y contexto de los equipos tras validar la titularidad. Documenten alertas históricas o no relacionadas. La afirmación de un vendedor no basta para ordenar la deshabilitación de toda una organización.

Equipos de aplicaciones e infraestructura. Validen la autorización efectiva y las versiones instaladas en sistemas propios. Conserven evidencia de remediación y de una nueva prueba funcional. Un mapa de capacidades de proveedor es un insumo de revisión, no prueba de la misma técnica en el entorno local.

Tesorería y protección del cliente. Conserven la verificación independiente para pagos, beneficiarios y cambios de recuperación. Ofrezcan al cliente una vía conocida para comprobar solicitudes sospechosas. Si se sospecha un uso indebido de información, distingan un escenario plausible de un fraude consumado reportado.

Legal, privacidad y comunicaciones. Conserven las horas de conocimiento, determinen cada deber aplicable y fijen la próxima actualización. Mantengan en oraciones distintas las afirmaciones de actores, las confirmaciones de la organización y las incógnitas. No publiquen una conclusión final de responsabilidad a partir de un procedimiento sin resolver.

12.3 Cuadro de cumplimiento

Área de decisión	Meta propuesta de gestión	Evidencia y regla de excepción
Derivación de alertas	Establecida para el día 30	La alerta sintética llega y se asigna; el acceso faltante tiene responsable
Alertas actuales pertinentes sobre cuentas	Toda alerta validada tiene una conclusión	Contención o resultado histórico/no relacionado documentado; los casos pendientes siguen visibles
Acceso de proveedores críticos	Revisado para el día 30 y probado para el día 60	Funciona la autoridad para suspender; el responsable del negocio aprueba excepciones
Servicio mínimo seguro	Probado para el día 60	La tarea crítica real del usuario funciona mediante la alternativa

Área de decisión	Meta propuesta de gestión	Evidencia y regla de excepción
Restauración protegida	Demostrada para el día 90	Registros de recuperación y reapertura segura, incluidos servicios dependientes de identidad
Preparación para notificar	Deberes aplicables mapeados para el día 30	Condición, destinatario y responsable correctos; los plazos legales reales prevalecen sobre el plan
Verificación del cliente	Probada para el día 90	Una solicitud sospechosa puede comprobarse por una vía independiente y confiable

Son resultados de gestión propuestos, no mejoras medidas que haya producido este informe. La organización debe fijar sus metas reales según la criticidad del servicio, la exposición validada y los deberes legales. Conserve un motivo cuando cambie la meta.

12.4 Cómo puede ayudar Brandefense

El informe ilustra el uso de evidencia de publicaciones de Brandefense Blackhole, entradas de Ransompedia y una cartera seleccionada de exposición. Una conversación pertinente debe partir de los activos propios de la organización, sus vías de alertas y las decisiones de validación que necesita tomar.

Lleve un servicio crítico, una dependencia de proveedor y una pregunta actual de respuesta. Consulte cómo llegaría la evidencia al equipo responsable y qué necesitaría validar ese equipo. Una demostración no establece que una organización esté afectada ni garantiza prevención, recuperación o cumplimiento de notificaciones.

Solicitar una demostración de Brandefense. [S36]

CONCLUSIONES CLAVE

01

Empiece con la derivación y validación de alertas, mientras prepara continuidad y notificación en paralelo.

02

Ajuste la contención y reapertura al efecto establecido en servicios, cuentas o datos.

03

Mida decisiones completadas y resultados probados, con responsables explícitos para las excepciones.

ANEXOS

Anexos

A–D

ESTE CAPÍTULO RESPONDE

¿Cómo deben interpretarse la evidencia y sus límites?

2026

periodo principal por fecha de publicación, con fechas de observación separadas cuando se indican

Apéndice A. Alcance, evidencia y confianza 84

Apéndice B. Registro de evidencia de publicaciones 87

Apéndice C. Fuentes 88

Apéndice D. Glosario en lenguaje sencillo 91

Apéndice A. Alcance, evidencia y confianza

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

A.1 Contrato de investigación

El país es el Perú, código PE. El periodo principal va del 1 de enero al 22 de noviembre de 2026, por fecha de publicación. La actividad reciente cubre del 8 al 22 de noviembre. La extracción y comprobación de fuentes se realizaron el 22 de noviembre; el día de corte aún estaba en curso. El informe se publicó por primera vez el 22 de noviembre de 2026 y se revisó el 23 de noviembre de 2026.

El público comprende responsables de seguridad, respuesta a incidentes, identidad y aplicaciones, fraude, asesores legales y responsables de servicios. Las decisiones abarcan validación, contención de cuentas, protección del cliente, servicio mínimo seguro, notificación y recuperación.

A.2 Fuentes y poblaciones separadas

Las fuentes propias incluyen publicaciones de la web oscura recopiladas por Odin by Brandefense y observaciones públicas de sitios de filtraciones de ransomware en Ransompedia. También incluyen una cartera seleccionada de organizaciones y observaciones pasivas de DNS, TLS y controles web cuando están disponibles. Las fuentes externas incluyen textos oficiales, comunicados, investigaciones de proveedores e información pública. [S1][S2][S3]

Una publicación es un mensaje difundido. Un anuncio es una afirmación sobre una oferta. Una entrada de ransomware recoge una afirmación criminal. Una denuncia registra lo reportado según la definición de la fuente. Un expediente reúne una pregunta de decisión y su evidencia. Ninguno equivale automáticamente a una intrusión verificada.

El mismo asunto puede aparecer en varias publicaciones, entradas o artículos posteriores. Los registros pueden solaparse entre fuentes y dominios. El informe no estima personas únicas a partir de esas poblaciones ni las suma en un total nacional de ataques.

A.3 Cartera y observaciones pasivas

La cartera contiene 250 dominios candidatos seleccionados de manera intencional en diez grupos sectoriales fusionados. No es una muestra de prevalencia nacional ni una clasificación por ingresos. La titularidad del dominio, los servicios relacionados y la identidad jurídica independiente siguen sin validarse.

Las asociaciones de exposición y las ofertas actuales de credenciales requieren su propia fecha de observación. Los registros acumulados no constituyen una población de incidentes exclusivamente de 2026. Una asociación con un equipo no establece empleo ni acceso actual a sistemas internos de una organización. Solo puede publicarse una cifra nacional validada de Atlas; no se presentan calificaciones sectoriales ni por organización.

Las observaciones pasivas conservan el denominador disponible para cada control. Los resultados faltantes siguen siendo desconocidos. No encontrar un registro no demuestra que no exista un control; observar un certificado o una página principal no constituye una evaluación completa de la seguridad de la aplicación. [S3]

A.4 Ransomware y comparaciones

Las 58 entradas del Perú están fechadas dentro del periodo solicitado de 2026. Pueden repetir una organización o utilizar etiquetas distintas de función e industria. Una entrada no es prueba independiente de cifrado, robo, pago ni pérdida final. [S2]

La comparación regional utiliza Chile, Colombia, Ecuador y Bolivia. La selección de países comparables se explica en §2.4. Los conteos brutos de entradas y publicaciones no se ajustan por tamaño del país, prácticas de divulgación ni visibilidad de las fuentes. El periodo de 2026 es parcial; la comparación de entradas de 2025 abarca todo el año.

A.5 Alcance de tarjetas

Las publicaciones revisadas contienen 15 observaciones de registros de tarjetas. Su validez, titularidad y uso no están verificados. Esta población limitada no permite estimar la exposición nacional de tarjetas ni las pérdidas por fraude. [S1]

Los registros de tarjetas, las asociaciones con emisores, las observaciones de equipos y los dominios financieros seleccionados son poblaciones distintas. No se establece una vinculación individual entre cliente, equipo y cuenta. Un estado escrito en una publicación no es un resultado de pago validado.

A.6 Evaluación de afirmaciones y confianza

La confianza corresponde a la proposición evaluada. Una publicación fechada y conservada permite tener alta confianza en que se difundió la afirmación. No aporta la misma confianza en el archivo, la cuenta o la vía técnica anunciados.

Cada expediente separa la afirmación, la evidencia establecida, las alternativas, los límites y una respuesta proporcional. Repetir un título o una lista de campos puede respaldar la similitud publicitaria, sin establecer archivos idénticos, una fuente independiente ni una transferencia consumada.

El mapa de relaciones conecta etiquetas con fuentes de respaldo. Se omiten asociaciones de actores sin sustento. La secuencia de fraude se identifica expresamente como modelo analítico, no como una cadena observada de un mismo operador.

A.7 Cobertura de fuentes públicas y cronología

El material público revisado comprende relatos oficiales y de prensa, advertencias de autoridades, textos legales e investigaciones de proveedores. La búsqueda cubrió información en español, inglés, portugués y ruso. La disponibilidad oficial y la cobertura de archivos siguen siendo desiguales; el informe no afirma ofrecer un censo exhaustivo de incidentes nacionales.

Algunos originales oficiales no estuvieron disponibles para lectura. Cuando un artículo original de prensa legible reproduce una declaración de autoridad, el informe la atribuye a ese relato. Las pistas no leídas se excluyen de las conclusiones fácticas sobre incidentes. No se sustituye la fecha anterior de un evento por la de su publicación posterior.

El registro de incidentes incluye decisiones sobre las afirmaciones conservadas y los candidatos de fuentes públicas. La revisión del periodo final distingue publicaciones nuevas, seguimientos históricos, desmentidos, investigaciones y eventos fuera del periodo reciente. Las lagunas de fuentes limitan la cobertura; no demuestran que un evento no ocurriera.

A.8 Nombres y neutralidad

Una organización víctima se nombra solo cuando la confirmación oficial y una cobertura amplia respaldan su nombre. Los demás objetivos utilizan funciones generales. Las citas usan la raíz del editor y un aviso de dirección del artículo omitida cuando dicha dirección identificaría a una víctima cuyo nombre se reserva.

Las afirmaciones de actores y las atribuciones estatales siguen siendo posiciones de sus fuentes. Se omiten insultos, llamados de reclutamiento, contactos y enlaces criminales operativos. El informe no toma posición sobre elecciones, sucesiones presidenciales, Congreso, partidos, protestas, decisiones del gobierno ni relaciones exteriores.

Apéndice B. Registro de evidencia de publicaciones

Las diez tarjetas de publicaciones respaldan nueve expedientes. B01 y B02 pertenecen a la misma conversación sobre reutilización. Las fechas son las de las publicaciones conservadas, no fechas de adquisición establecidas independientemente. Todos los alias se reservan en esta edición; las marcas de grupos se evalúan por separado. [S1]

Tarjeta	Fecha	Medio	Idioma original	Expediente
B01	2026-01-07	Foro	Inglés	A: anuncio de registros de ciudadanos
B02	2026-01-07	Foro	Inglés	A: conversación sobre material anterior
B03	2026-02-10	Foro	Inglés	B: acceso a servicio público
B04	2026-02-16	Foro	Inglés	C: documentos de salud
B05	2026-03-04	Foro	Inglés	D: registros de beneficios
B06	2026-03-27	Foro	Inglés	E: acceso a comercio minorista
B07	2026-11-08	Foro	Inglés	F: registros empresariales
B08	2026-11-13	Foro	Inglés	G: registros de estudiantes y asistencia
B09	2026-11-16	Foro	Español	H: gestión educativa
B10	2026-11-20	Foro	Español	I: historiales laborales

Apéndice C. Fuentes

Los números de fuente que no aparecen se retiraron durante la revisión y no se citan.

S1: Odin by Brandefense. Peru-associated underground posts, post dates 1 January–22 November 2026. Verificado el 22 de noviembre de 2026. Observación de fuente propia.

S2: Brandefense Ransompedia. Peru and four regional peers, ransomware listing observations. Verificado el 22 de noviembre de 2026. Observación de fuente propia.

S3: Odin by Brandefense. Selected portfolio exposure and passive configuration observations. Verificado el 22 de noviembre de 2026. Observación de fuente propia.

S4: DataReportal. Digital 2027: Peru, October 2026 overview. https://datareportal.com/reports/digital-2027-peru Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S5: El Peruano. Regulation of the Digital Trust Framework, Supreme Decree 126-2025-PCM. https://busquedas.elperuano.pe/dispositivo/EX/2455024-1 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S6: El Peruano / ANPD. Personal Data Protection Regulation, Supreme Decree 016-2024-JUS. https://cdn.www.gob.pe/uploads/document/file/7568330/6426760-decreto-supremo-n-016-2024-jus-reglamento-de-la-ley-n-29733-ley-de-proteccion-de-datos-personales-publicado-nov-2024.pdf Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S7: SBS. Information security and cybersecurity regulation, Resolution 504-2021, consolidated version. https://intranet2.sbs.gob.pe/dv_int_cn/2046/v5.0/Adjuntos/504-2021.R%20.pdf Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S8: SBS. Proposed unified operational-incident reporting procedure, 16 September 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/4000 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S9: SBS. Prepublication notice for proposed operational-incident reporting procedure. https://intranet2.sbs.gob.pe/Preproyectos/9732JNQOUDCIR5EEENNVGOJQHTGLK7ZKCBB.PDF Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S10: El Peruano. Financial customer communications, SBS Resolution 01741-2026. https://busquedas.elperuano.pe/dispositivo/NL/2530621-1 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S11: El Peruano. CNSD preventive PHP warning, 26 October 2026. https://www.elperuano.pe/noticia/307672-alerta-por-fallas-informaticas-globales-pcm-activa-medidas-para-proteger-los-datos-de-los-ciudadanos Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S12: PHP Group. Security advisory GHSA-w8hw-w9fx-j79w, 21 October 2026. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S13: PHP Group. Security advisory GHSA-6wmf-4rv5-p3rp, 21 October 2026. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S14: NIST National Vulnerability Database. CVE-2026-109618 record. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S15: NIST National Vulnerability Database. CVE-2026-109619 record. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S17: Latina Noticias. Authority account of unauthorised supplier-account use, 20 May 2026. https://latinanoticias.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S18: El Comercio. Insurer and supervisor statements on customer-information access, 15 October 2026. https://elcomercio.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S19: Infobae. Wider reporting on insurer customer-information incident, 13 October 2026. https://www.infobae.com/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S20: Petroperú. Company warning about an AI-manipulated investment video, 12 June 2026. https://www.petroperu.com.pe/petroperu-alerta-sobre-falso-video-del-presidente-de-directorio-creado-con-inteligencia-artificial Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S21: Gestión. Wider reporting on the company investment-video warning, 14 June 2026. https://gestion.pe/economia/empresas/petroperu-alerta-sobre-video-falso-creado-con-inteligencia-artificial-para-promover-estafa-noticia/ Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S22: RENIEC. Official account of an alleged illegal personal-data sales investigation, 3 July 2026. https://identidad.reniec.gob.pe/b/reniec-participo-de-operativo-contra-la-comercializacion-ilegal-de-datos-personales-en-piura Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S23: El Comercio. Health-service account of unauthorised transfers, 19 August 2026. https://elcomercio.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S24: Infobae. Wider reporting on unauthorised health-service transfers, 19 August 2026. https://www.infobae.com/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S25: Andina. Prosecutor computer-crime complaint statistics for 2024, 2025 and January–July 2026, published 30 September 2026. https://andina.pe/agencia/noticia-como-colaboran-tiktok-roblox-y-meta-las-investigaciones-ciberdelitos-1094008.aspx Verificado el 23 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S26: El Peruano. Officially reported warning on transport-fine impersonation, 4 August 2026. https://elperuano.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S27: La República. Authority response to a business-record dataset claim, 9 November 2026. https://larepublica.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S28: Derechos Digitales. Retrospective discussion of an earlier bank incident, 15 November 2026. https://www.derechosdigitales.org/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S29: SBS. Open-finance roadmap, 25 February 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/3897 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S30: SBS. Announcement of updated sanctions framework, 10 April 2026. https://www.sbs.gob.pe/noticia/detallenoticia/idnoticia/3914 Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S31: ESET. FamousSparrow regional research, 17 September 2026. https://www.welivesecurity.com/es/investigaciones/famoussparrow-america-latina-sparrowocky/ Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S32: Kaspersky. Retadup research, 16 November 2026. https://www.kaspersky.com/about/press-releases/kaspersky-dead-retadup-worm-tried-to-infect-at-least-15000-devices-seven-years-after-its-takedown Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S34: RENIEC. Issuer notice of an electrical service interruption, 2 November 2026. https://identidad.reniec.gob.pe/ (article URL withheld). Verificado el 22 de noviembre de 2026. Dirección del artículo omitida; se leyó el relato de respaldo.

S35: Ojo Público. Multi-year state data-security investigation, 9 August 2026. https://ojo-publico.com/6464/datos-vulnerados-graves-fallas-seguridad-el-estado-peruano Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S36: Brandefense. Platform demonstration information. https://brandefense.io/request-a-demo/ Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S37: RFC Editor / IETF. RFC 9989, DMARC specification. https://www.rfc-editor.org/info/rfc9989/ Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S38: FIRST. Traffic Light Protocol version 2.0. https://www.first.org/tlp/ Verificado el 22 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

S39: RFC Editor / IETF. RFC 7208, Sender Policy Framework. https://www.rfc-editor.org/rfc/rfc7208.html Verificado el 22 de noviembre de 2026. Se comprobó el resumen.

S40: RFC Editor / IETF. RFC 8659, DNS Certification Authority Authorization. https://www.rfc-editor.org/rfc/rfc8659.html Verificado el 22 de noviembre de 2026. Se comprobó el resumen.

S41: RFC Editor / IETF. RFC 8446, Transport Layer Security. https://www.rfc-editor.org/rfc/rfc8446.html Verificado el 22 de noviembre de 2026. Se comprobó el resumen.

S42: Microsoft. Boletín de seguridad MS15-095, abreviatura RCE y descripción de ejecución de código. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-095 Verificado el 22 de noviembre de 2026. Se comprobaron la abreviatura y la descripción de ejecución de código.

S43: Red Hat. Guía de diseño de sistemas RHEL 8, sección 6.3.1: cuenta root. https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/8/html/system_design_guide/customizing-the-system-in-the-installer_system-design-guide Verificado el 22 de noviembre de 2026. Se comprobó la descripción de los privilegios de root.

S44: GNU. Manual de referencia de Bash, sección 1.2: definición de shell. https://www.gnu.org/software/bash/manual/html_node/What-is-a-shell_003f.html Verificado el 22 de noviembre de 2026. Se comprobó la definición de intérprete de comandos.

S45: ESET. ESET APT Activity Report Q2 2026–Q3 2026, 28 October 2026. https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q2-2026-q3-2026/ Verificado el 23 de noviembre de 2026. Se comprobó el pasaje de respaldo o el registro de vulnerabilidad.

Apéndice D. Glosario en lenguaje sencillo

- **Afirmación de actor:** lo que sostiene un autor o grupo; su publicación no establece su exactitud.
- **Cifra nacional de Atlas:** un único resumen validado de exposición para la cartera seleccionada; no es una probabilidad nacional de ataque.
- **BIN:** prefijo de identificación del emisor en un número de tarjeta; aquí no se publica ningún prefijo de tarjeta.
- **CAA:** Certification Authority Authorization, registro DNS que especifica qué autoridades certificadoras pueden emitir certificados para un dominio. [S40]
- **Certificado C4:** certificado peruano de inscripción; su autenticidad requiere verificación mediante el emisor legítimo.
- **CNSD:** Centro Nacional de Seguridad Digital.
- **Oferta de credenciales:** anuncio de información de inicio de sesión, sin prueba de que la cuenta siga funcionando.
- **DDoS:** tráfico distribuido destinado a dejar un servicio fuera de disponibilidad; una afirmación sola no establece una interrupción.
- **DNI:** Documento Nacional de Identidad del Perú.
- **DMARC:** política de autenticación del correo que ayuda a los sistemas receptores a manejar mensajes que no superan las comprobaciones del dominio. [S37]
- **DNSSEC:** firmas que ayudan a validar información DNS; una observación de configuración no establece la seguridad completa del servicio.
- **Equipo final:** dispositivo como una estación de trabajo o un servidor; su titularidad y actividad requieren validación local.
- **HSTS:** política web que indica al navegador que utilice HTTPS para el sitio.
- **Recuperación de identidad:** proceso para recuperar acceso a una cuenta, incluidas las comprobaciones sobre quién puede cambiar sus datos de autenticación.
- **MFA:** autenticación multifactor, que exige más de un factor independiente para iniciar sesión.
- **Phishing:** solicitud engañosa diseñada para obtener información, acceso o una acción mediante suplantación de una fuente confiable.
- **Entrada de Ransompedia:** afirmación criminal pública registrada, no una intrusión confirmada ni una organización única.
- **RCE:** ejecución remota de código, la capacidad de ejecutar código en un sistema desde otro lugar. En B03 es una afirmación del vendedor sin validar. [S42]
- **Root:** la cuenta con los privilegios más altos del sistema. B03 no valida que el vendedor tenga esos privilegios. [S43]
- **Revocación de sesión:** finalización de una sesión autenticada existente para que ya no pueda utilizarse.
- **Shell:** un intérprete de comandos, utilizado para acceso por línea de comandos. B03 no valida que el vendedor tenga ese acceso. [S44]

- **SPF:** Sender Policy Framework, estándar de correo que permite a los administradores especificar qué servidores pueden enviar mensajes usando su dominio. [S39]
- **Privilegio de proveedor:** permiso de un proveedor externo, con alcance y responsable que requieren validación.
- **TLS:** Transport Layer Security, protocolo que protege las conexiones frente a la interceptación y alteración de datos. [S41]
- **TLP:CLEAR:** permite compartir información sin restricciones según el protocolo de semáforo; siguen aplicándose otros deberes legales. [S38]

Acerca de este informe

Preparado por Odin by Brandefense como Brandefense Country Report · Peru 2026. El original en inglés y la edición en español peruano comparten límites de evidencia, números e identificadores. La edición en español muestra un aviso de traducción con IA e identifica el original en inglés como referencia en caso de diferencias.

El informe describe la evidencia disponible a la fecha de corte. No afirma ofrecer un censo nacional, establecer una posición política ni atribuir un delito más allá de la evidencia citada. Las recomendaciones son acciones propuestas, no afirmaciones sobre si una organización concreta las ha implementado.

© 2026 Brandefense. Todos los derechos reservados.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO