Revisión de seguridad del correo — Reporte de muestra

Nov 22, 2026 · @Pablo Huertas

> **Documento de muestra.** Andina Logística S.A. y sus dominios son ficticios: usan el dominio de nivel superior reservado `.example` (RFC 2606), que no puede pertenecer a ninguna empresa real. Los hallazgos reproducen patrones frecuentes en empresas medianas. El formato, la metodología y el nivel de detalle son los de una revisión real.

Cliente: Andina Logística S.A. (ficticio) · importación y logística, unas 60 personas ·
Preparado por: Pablo Huertas

1. Resumen ejecutivo

Estado del dominio principal: Observando a ciegas. El registro DMARC existe, pero no produce un solo dato, y hoy no bloquea ningún correo falso.

Hoy es posible enviar correo que diga venir de Andina Logística y que llegue a la bandeja de entrada de sus clientes. Para una empresa que envía facturas e instrucciones de pago por correo, este es el escenario que hace posible el fraude por cambio de cuenta bancaria.

Lo más importante

- **El dominio regional `andinalogistica-mx.example` está expuesto.** No tiene DMARC ni SPF. Cualquiera puede enviar correo con ese dominio, y para un cliente se ve tan legítimo como el principal.
- **El SPF del dominio principal hace 11 consultas DNS, y el límite del estándar es 10.** Los servidores receptores lo evalúan como error permanente, así que en la práctica no protege nada, aunque parezca completo.
- **Los reportes DMARC no están llegando.** El registro envía los reportes a un proveedor externo que no publicó la autorización que exige el protocolo. Google y Microsoft descartan el envío sin avisar a nadie.
- **Las facturas electrónicas fallan DMARC.** La plataforma de facturación firma con su propio dominio y no con el suyo. Hoy no pasa nada porque la política es `p=none`, pero el día que se active el rechazo, sus clientes dejarían de recibir las facturas.

Las tres acciones prioritarias

#	Acción	Esfuerzo	Plazo sugerido
1	Proteger el dominio regional con tres registros DNS (no envía ni recibe correo)	Bajo	Esta semana
2	Reducir el SPF a 10 consultas o menos, retirando un proveedor que ya no se usa y dos mecanismos redundantes	Bajo	Esta semana
3	Pedir a la plataforma de facturación que firme con el dominio de la empresa (DKIM propio)	Medio	2–3 semanas

Con esas tres acciones y la corrección de los reportes, el dominio queda listo para empezar el camino hacia el rechazo del correo suplantado (`p=reject`) sin riesgo de bloquear correo legítimo. El plan completo está en la sección 7.

2. Alcance

La revisión cubrió dos dominios y tres mensajes reales, y se hizo sin acceso a ningún sistema de la empresa.

Qué se revisó

Elemento	Detalle
Dominios	`andinalogistica.example` (principal) y `andinalogistica-mx.example` (variante regional registrada para proteger la marca)
Registros DNS públicos	DMARC, SPF (con el conteo recursivo de consultas), DKIM, MX, MTA-STS, TLS-RPT, BIMI y DNSSEC
Mensajes reales	Tres correos enviados a una cuenta de prueba: uno de un colaborador, una factura electrónica y un boletín comercial
Remitentes	Identificación de las plataformas que envían correo en nombre de la empresa, a partir del SPF, los selectores DKIM y los encabezados

Cómo se hizo

- Consultas DNS desde un resolutor externo, para ver lo mismo que ve cualquier servidor de correo en internet.
- Lectura de los encabezados `Authentication-Results` de cada mensaje, que muestran cómo el servidor receptor evaluó SPF, DKIM y DMARC.
- Cada hallazgo se clasificó por severidad y por esfuerzo de corrección (escalas en el anexo B).

Qué no incluye

- Cambios en el DNS ni en ninguna plataforma. Este reporte dice qué corregir y en qué orden; la implementación es un servicio aparte (sección 7).
- Revisión de los buzones, del filtrado antispam ni de la configuración interna de Microsoft 365.
- Análisis de reportes DMARC históricos: no existen, porque los reportes no están llegando (hallazgo H3).

Fecha de la revisión: 22 de noviembre de 2026. El DNS puede cambiar después de esa fecha.

3. Estado por dominio y resumen de hallazgos

Ninguno de los dos dominios bloquea hoy el correo suplantado. El regional está completamente abierto, y el principal tiene DMARC publicado, pero sin efecto ni datos.

Dominio	Estado	Qué significa
`andinalogistica-mx.example`	**Expuesto**	Hoy cualquiera puede enviar correo en nombre de este dominio
`andinalogistica.example`	**Observando a ciegas**	El registro existe, pero no produce un solo dato

La escala completa de estados está en el anexo B. El objetivo para los dos dominios es **Protegido**: el correo suplantado se rechaza en el servidor del destinatario.

Hallazgos priorizados

Primero van los que anulan la protección, después los que la dejan sin visibilidad, luego los que bloquean el camino al rechazo y al final las observaciones.

#	Hallazgo	Dominio	Severidad	Esfuerzo
H1	Sin DMARC ni SPF	Regional	Crítico	Bajo
H2	El SPF excede el límite de 10 consultas (error permanente)	Principal	Crítico	Bajo
H3	Los reportes DMARC no llegan: falta la autorización del destino externo	Principal	Alto	Bajo
H4	La plataforma de facturación no firma con el dominio de la empresa	Principal	Alto	Medio
H5	Política `p=none`: observa, no bloquea	Principal	Alto	Medio
H6	Selector DKIM con clave revocada, residuo de un proveedor anterior	Principal	Observación	Bajo
H7	MTA-STS, TLS-RPT y DNSSEC no publicados	Principal	Observación	—

El esfuerzo de H2 es bajo porque la corrección consiste en retirar entradas del registro, no en agregarlas.

4. Hallazgos en detalle

Cada hallazgo responde cuatro preguntas en el mismo orden. El detalle técnico va en un bloque aparte, para quien administre el DNS.

H1. El dominio regional no tiene DMARC ni SPF — Crítico · Esfuerzo bajo

Qué encontramos. `andinalogistica-mx.example` no publica DMARC, SPF ni registros MX. El dominio se registró para proteger la marca y no envía ni recibe correo.

Qué significa para el negocio. Cualquiera puede enviar un correo desde `facturacion@andinalogistica-mx.example`. Un cliente no tiene cómo saber que ese dominio no es de ustedes, y ningún servidor receptor tiene instrucciones para rechazarlo.

Qué pasa si no se corrige. Quien intente un fraude de cambio de cuenta bancaria va a preferir el dominio sin protección. Proteger solo el principal deja abierta la puerta de al lado.

Esfuerzo: bajo. Tres registros DNS. Como el dominio no envía correo, se puede pasar directo a rechazo, sin etapa de observación.

```
Estado actual
_dmarc.andinalogistica-mx.example   TXT   (no existe)
andinalogistica-mx.example          TXT   (sin SPF)
andinalogistica-mx.example          MX    (no existe)

Corrección propuesta
andinalogistica-mx.example          TXT   "v=spf1 -all"
_dmarc.andinalogistica-mx.example   TXT   "v=DMARC1; p=reject; sp=reject;
adkim=s; aspf=s"
andinalogistica-mx.example          MX    0 .        (MX nulo, RFC 7505)
```

H2. El SPF excede el límite de 10 consultas — Crítico · Esfuerzo bajo

Qué encontramos. Al recorrer el SPF del dominio principal y todos los registros que incluye, la evaluación necesita 11 consultas DNS. El estándar corta en 10. Una de ellas, además, es una consulta vacía: apunta a un proveedor de hosting que ya no responde.

Qué significa para el negocio. Cuando se pasa del límite, el resultado es un error permanente (`permerror`). El registro parece completo, pero en la práctica no declara ningún servidor autorizado.

Qué pasa si no se corrige. Cuando la política DMARC endurezca, el correo que dependa de SPF para pasar va a fallar. Y cada proveedor nuevo que se agregue empeora el conteo.

Esfuerzo: bajo. La corrección consiste en retirar tres entradas que no aportan nada, y deja el conteo en 8 de 10.

```
Registro actual (andinalogistica.example, TXT)
v=spf1 a mx
  include:spf.protection.outlook.com
  include:_spf.boletines.example
  include:_spf.facturador.example
  include:_spf.crm-ventas.example
  include:_spf.hosting-anterior.example
  ~all

Conteo: 7 de primer nivel + 4 anidadas = 11 de 10 → permerror
Consulta vacía: _spf.hosting-anterior.example (NXDOMAIN)

Qué se retira y por qué
- include:_spf.hosting-anterior.example
    proveedor que ya no se usa (consulta vacía)
```

```
- mx
    los MX apuntan a Microsoft 365, ya cubierto por su include
- a
    el servidor web no envía correo (confirmar antes que el
    formulario del sitio tampoco envía desde ese servidor)

Registro propuesto (8 de 10)
v=spf1
  include:spf.protection.outlook.com
  include:_spf.boletines.example
  include:_spf.facturador.example
  include:_spf.crm-ventas.example
  ~all

(Los registros SPF se muestran en varias líneas para leerlos mejor;
se publican en una sola.)
```

El cierre con `~all` en lugar de `-all` se registra como observación, no como falla: pierde importancia cuando DMARC esté en `p=reject`.

H3. Los reportes DMARC no están llegando — Alto · Esfuerzo bajo

Qué encontramos. El registro DMARC envía los reportes a `reportes-proveedor.example`, un dominio distinto del suyo. En ese caso, el protocolo exige que el dueño del dominio receptor publique una autorización. Esa autorización no existe.

Qué significa para el negocio. Configuraron un servicio de reportes que no está recibiendo reportes. Google y Microsoft descartan el envío sin avisar, así que no hay ningún error visible en ninguna parte.

Qué pasa si no se corrige. Sin reportes, no hay forma de saber quién envía correo en su nombre, ni de confirmar que todos los sistemas legítimos pasan antes de endurecer la política. Si el registro se configuró hace meses, lleva meses sin producir un solo dato.

Esfuerzo: bajo. Dos opciones: pedir al proveedor de reportes que publique la autorización, o recibir los reportes en un buzón del propio dominio, que no la necesita.

```
Registro actual
_dmarc.andinalogistica.example  TXT
  "v=DMARC1; p=none; rua=mailto:dmarc@reportes-proveedor.example"

Autorización que debería existir (en la zona del proveedor)
andinalogistica.example._report._dmarc.reportes-proveedor.example
  TXT  (no existe)
*._report._dmarc.reportes-proveedor.example
  TXT  (no existe)

Registro esperado: "v=DMARC1"
```

H4. La plataforma de facturación no firma con el dominio de la empresa — Alto · Esfuerzo medio

Qué encontramos. Las facturas electrónicas salen con remitente `facturacion@andinalogistica.example`, pero la plataforma las firma con su propio dominio y usa su propio dominio para los rebotes. Ninguna de las dos verificaciones queda alineada con el dominio de la empresa, así que el mensaje falla DMARC (ver el mensaje 2 en la sección 5).

Qué significa para el negocio. Hoy las facturas se entregan solo porque la política está en `p=none`. Para los servidores receptores, una factura legítima y una falsa se ven igual: las dos fallan.

Qué pasa si no se corrige. El día que la política pase a cuarentena o rechazo, las facturas empezarían a llegar a spam o a no llegar. Es el error clásico de los proyectos DMARC: un sistema olvidado que se rompe el día del cambio.

Esfuerzo: medio. Requiere coordinar con el proveedor de facturación. La mayoría de estas plataformas permite configurar una firma DKIM con el dominio del cliente, publicando uno o dos registros que el proveedor entrega.

```
Mensaje 2 (factura), Authentication-Results:
spf=pass smtp.mailfrom=rebotes.facturador.example
    → no alinea con el From
dkim=pass header.d=facturador.example
    → no alinea con el From
dmarc=fail action=none header.from=andinalogistica.example

Corrección: DKIM con d=andinalogistica.example en la plataforma
de facturación (registros CNAME o TXT que entrega el proveedor).
Opcional: dominio de rebote propio.
```

H5. La política DMARC solo observa — Alto · Esfuerzo medio

Qué encontramos. El dominio principal publica `p=none`.

Qué significa para el negocio. El dominio está mirando, no defendiendo. El correo suplantado se sigue entregando igual que si no hubiera nada publicado.

Qué pasa si no se corrige. La empresa queda en el punto donde se detiene la mayoría: con DMARC publicado, la sensación de estar protegida y ningún correo falso bloqueado.

Esfuerzo: medio. No se corrige cambiando la política de inmediato. Primero hay que resolver H2, H3 y H4, y confirmar con al menos tres semanas de reportes que todos los remitentes legítimos pasan. Después se endurece por etapas (sección 7).

H6. Selector DKIM con clave revocada — Observación · Esfuerzo bajo

Qué encontramos. El selector `k1` existe, pero su clave está vacía (revocada). Suele ser el residuo de un proveedor que ya no se usa.

Qué significa. No es un riesgo: una clave revocada no permite firmar. Conviene retirarlo para mantener el DNS limpio y evitar confusiones en futuras revisiones.

```
k1._domainkey.andinalogistica.example   TXT   "v=DKIM1; p="
```

H7. MTA-STS, TLS-RPT y DNSSEC no publicados — Observación

Qué encontramos. El dominio principal no publica MTA-STS ni TLS-RPT, y su zona no está firmada con DNSSEC.

Qué significa. No son fallas, sino mejoras para una segunda etapa. MTA-STS obliga a que el correo entrante viaje cifrado, y TLS-RPT informa cuando eso falla. BIMI, que muestra el logotipo de la empresa junto a sus correos, requiere tener primero `p=reject`.

5. Revisión de encabezados de mensajes reales

El DNS dice quién está autorizado a enviar; los encabezados muestran qué pasa realmente con cada mensaje. De los tres sistemas revisados, dos pasan DMARC y uno falla: la facturación.

Para cada mensaje se leyó el encabezado `Authentication-Results` que agregó el servidor receptor. Un mensaje pasa DMARC si SPF o DKIM pasan **y** están alineados, es decir, si usan el mismo dominio que aparece en el remitente visible (`From`).

#	Mensaje	Sistema	SPF	DKIM	DMARC	Con `p=reject`
1	Correo de un colaborador	Microsoft 365	Pasa, alineado	Pasa, alineado (`selector1`)	**Pasa**	Se entrega
2	Factura electrónica	Plataforma de facturación	Pasa, **no alineado**	Pasa, **no alineado**	**Falla**	**Se rechazaría**
3	Boletín comercial	Plataforma de boletines	Pasa, no alineado	Pasa, alineado (`bol1`)	**Pasa**	Se entrega

Qué nos dicen

- **Microsoft 365 está bien configurado.** Firma con el dominio de la empresa y pasa por las dos vías.
- **La facturación es el remitente que hay que corregir antes de endurecer** (hallazgo H4). Es el patrón más frecuente: el sistema que más importa para el negocio es el que nadie revisó.
- **El boletín pasa solo por DKIM.** El SPF no alinea porque la plataforma usa su propio dominio para los rebotes, y eso es normal. Basta con que una de las dos vías esté alineada.
- **El selector `bol1` no aparece en la lista de nombres habituales** que se sondean desde fuera. Se identificó por los encabezados. Por eso la revisión de mensajes reales complementa la del DNS: el nombre de un selector DKIM lo elige cada proveedor y no se puede enumerar desde fuera.

```
Mensaje 1 — colaborador (Microsoft 365)
spf=pass smtp.mailfrom=andinalogistica.example
dkim=pass header.d=andinalogistica.example header.s=selector1
dmarc=pass action=none header.from=andinalogistica.example

Mensaje 2 — factura electrónica
spf=pass smtp.mailfrom=rebotes.facturador.example
dkim=pass header.d=facturador.example
dmarc=fail action=none header.from=andinalogistica.example

Mensaje 3 — boletín comercial
spf=pass smtp.mailfrom=rebotes.boletines.example
dkim=pass header.d=andinalogistica.example header.s=bol1
dmarc=pass action=none header.from=andinalogistica.example
```

En una revisión real se piden mensajes de cada sistema que envía en nombre de la empresa. Tres mensajes son el mínimo; el inventario completo de remitentes se confirma después con los reportes DMARC.

6. Lo que está bien configurado

La base es buena: el correo principal está bien autenticado, y la mayor parte del trabajo pendiente consiste en ordenar lo que ya existe, no en construir desde cero.

- **Microsoft 365 firma con el dominio de la empresa.** Los selectores `selector1` y `selector2` tienen claves válidas, y el correo de los colaboradores pasa DMARC por SPF y por DKIM.
- **La plataforma de boletines tiene DKIM propio** (`bol1`), alineado con el dominio de la empresa.
- **Hay un único registro DMARC y un único registro SPF**, con sintaxis válida. Un registro duplicado anularía la política completa.
- **Los MX apuntan a Microsoft 365** y responden correctamente.
- **Ya existe la decisión de usar DMARC.** Alguien lo configuró y contrató un servicio de reportes. Falta terminar el camino, no convencer a nadie de empezarlo.

7. Plan de corrección y siguiente paso

El camino hasta Protegido toma unas 12 semanas. Nunca se pasa a la etapa siguiente mientras quede un remitente legítimo fallando, y volver atrás es cambiar un solo registro DNS.

Etapa	Semanas	Qué se hace	Quién	Condición para avanzar
0. Victorias rápidas	1	Proteger el dominio regional (H1), reducir el SPF a 8 de 10 (H2), corregir el destino de los reportes (H3) y retirar el selector revocado (H6)	Quien administra el DNS	Los reportes empiezan a llegar en 24–72 horas
1. Corregir remitentes	1–3	DKIM propio en la plataforma de facturación (H4); revisar en los reportes si aparece algún sistema que no estaba inventariado	TI con el proveedor de facturación	Todos los sistemas legítimos pasan DMARC en los reportes
2. Observación	3–6	Mantener `p=none` y revisar los reportes cada semana	Revisión de reportes	Tres semanas seguidas sin fallos de remitentes legítimos
3. Cuarentena gradual	6–10	`p=quarantine` con `pct=25`, luego 50 y luego 100, revisando los reportes después de cada salto	Quien administra el DNS	Ningún correo legítimo afectado en cada salto
4. Rechazo	~12	`p=reject` y `sp=reject`; endurecer la alineación solo si todos los remitentes lo soportan	Quien administra el DNS	Dominio **Protegido**

Etapa	Semanas	Qué se hace	Quién	Condición para avanzar
5. Mejoras	Después	MTA-STS, TLS-RPT y, si interesa, BIMI (H7)	TI	—

```
Registros DMARC por etapa (dominio principal)
Etapa 0–2   v=DMARC1; p=none; rua=mailto:<destino-de-reportes>
Etapa 3     v=DMARC1; p=quarantine; pct=25; rua=mailto:<destino-de-reportes>
            (luego pct=50 y pct=100)
Etapa 4     v=DMARC1; p=reject; sp=reject; rua=mailto:<destino-de-reportes>
```

Lo que se necesita de la empresa: una persona que pueda publicar cambios en el DNS en las fechas acordadas, y el contacto técnico de la plataforma de facturación. Ese suele ser el verdadero cuello de botella, así que conviene definirlo desde el inicio.

Siguiente paso. El equipo de TI puede ejecutar este plan por su cuenta con este reporte. Si prefieren que lo haga yo, el servicio de rollout de DMARC cubre las etapas 0 a 4: coordinación con los proveedores, revisión semanal de los reportes, cada cambio de política con su fecha y un informe al cierre. El valor de esta revisión se acredita al rollout. Después del rechazo, el monitoreo continuo puede seguir en una plataforma especializada; si les interesa, les recomiendo opciones según el tamaño y las necesidades de la empresa.

Anexo A. Registros DNS consultados

```
andinalogistica.example
  _dmarc          TXT   v=DMARC1; p=none;
                        rua=mailto:dmarc@reportes-proveedor.example
  @ (SPF)         TXT   v=spf1 a mx include:spf.protection.outlook.com
                        include:_spf.boletines.example
                        include:_spf.facturador.example
                        include:_spf.crm-ventas.example
                        include:_spf.hosting-anterior.example ~all
  @               MX    0 andinalogistica-example.mail.protection.outlook.com
  selector1       DKIM  clave RSA válida (Microsoft 365)
  selector2       DKIM  clave RSA válida (Microsoft 365)
  bol1            DKIM  clave RSA válida (plataforma de boletines;
                        identificado por encabezados)
  k1              DKIM  v=DKIM1; p=   (revocado)
```

```
  _mta-sts        TXT   (no existe)
  _smtp._tls      TXT   (no existe)
  default._bimi   TXT   (no existe)
  DNSSEC                zona no firmada

andinalogistica-mx.example
  _dmarc          TXT   (no existe)
  @ (SPF)         TXT   (no existe)
  @               MX    (no existe)

reportes-proveedor.example
  andinalogistica.example._report._dmarc   TXT   (no existe)
  *._report._dmarc                         TXT   (no existe)
```

Anexo B. Escalas y criterios

Estados de un dominio

Estado	Condición
Expuesto	Sin DMARC, o con DMARC inválido o duplicado
Observando	`p=none` con reportes funcionando
Observando a ciegas	`p=none` sin reportes, o con un destino externo sin autorización
Protección parcial	`quarantine`, `reject` con `pct` menor a 100, o `reject` con subdominios en `sp=none`
Protegido	`p=reject`, `pct=100`, subdominios protegidos, SPF y DKIM sanos
Indeterminado	El dominio no resuelve o el resultado no permite concluir; se revisa a mano y nunca se trata como Expuesto

Se usa un estado y no un puntaje de 0 a 100: la pregunta útil no es «qué nota sacamos», sino «qué falta para subir de estado».

Severidad de los hallazgos

Severidad	Criterio	Ejemplos
Crítico	Anula toda la protección del dominio	Sin DMARC; DMARC duplicado o inválido; SPF con más de 10 consultas o duplicado; SPF con `+all` o `?all`
Alto	Deja la protección sin efecto o sin visibilidad, o bloquea el camino al rechazo	`p=none`; reportes ausentes o sin autorización; un remitente legítimo sin alineación; sin SPF
Medio	Protección parcial o riesgo de error futuro	`quarantine` o `pct` menor a 100; subdominios en `sp=none`; más de 2 consultas vacías en el SPF; mecanismo `ptr`; SPF sin `all` final; clave DKIM menor a 1024 bits
Observación	Mejora, higiene o dato informativo, sin riesgo actual	`~all` o alineación relajada con `p=reject`; selector revocado; MTA-STS, TLS-RPT, DNSSEC o BIMI ausentes

Esfuerzo de corrección

Esfuerzo	Qué implica
Bajo	Uno o pocos cambios de registros DNS
Medio	Coordinar con un proveedor externo
Alto	Inventario interno de sistemas que envían correo

Criterios de rigor

- **DKIM:** cuando no se encuentra un selector, el reporte dice «no encontramos selectores en la lista de nombres habituales», y nunca «no tienen DKIM». El nombre del selector lo elige cada proveedor y no se puede enumerar desde fuera.
- **No verificado no es lo mismo que inexistente:** si una consulta no responde, el punto se marca como no verificado.
- **Capacidad, no acusación:** el reporte dice que es posible suplantar un dominio, nunca que fue usado para fraude.

- **Sin cifras de la industria:** los hallazgos se basan solo en datos verificables del dominio revisado.