# Email Security Review — Sample Report

Nov 22, 2026 · @Pablo Huertas

> **Sample document.** Andina Logistics Inc. and its domains are fictitious. They use the reserved top-level domain `.example` (RFC 2606), which cannot belong to any real company. The findings reproduce patterns that are common in mid-sized companies. The format, methodology and level of detail are those of a real review.

**Client:** Andina Logistics Inc. (fictitious) · import and logistics, about 60 people · **Prepared by:** Pablo Huertas

## 1. Executive summary

**Main domain status: Monitoring blind.** The DMARC record exists, but it produces no data at all, and today it blocks no spoofed email.

Today it is possible to send email that claims to come from Andina Logistics and have it reach your customers' inboxes. For a company that sends invoices and payment instructions by email, this is the scenario that makes bank-account-change fraud possible.

**What matters most**

- **The regional domain `andinalogistica-mx.example` is exposed.** It has no DMARC and no SPF. Anyone can send email from that domain, and to a customer it looks as legitimate as the main one.
- **The main domain's SPF takes 11 DNS lookups, and the standard's limit is 10.** Receiving servers evaluate it as a permanent error, so in practice it protects nothing, even though it looks complete.
- **DMARC reports are not arriving.** The record sends reports to an external provider that has not published the authorization the protocol requires. Google and Microsoft drop them without telling anyone.
- **E-invoices fail DMARC.** The invoicing platform signs with its own domain, not yours. Nothing happens today because the policy is `p=none`, but the day rejection is turned on, your customers would stop receiving invoices.

**The three priority actions**

| # | Action | Effort | Suggested timing |
|---|---|---|---|
| 1 | Protect the regional domain with three DNS records (it neither sends nor receives email) | Low | This week |
| 2 | Bring SPF down to 10 lookups or fewer by removing an unused provider and two redundant mechanisms | Low | This week |
| 3 | Ask the invoicing platform to sign with the company's domain (custom DKIM) | Medium | 2–3 weeks |

With those three actions and the reporting fix, the domain is ready to start the path toward rejecting spoofed email ( `p=reject` ) without risk of blocking legitimate mail. The full plan is in section 7.

## 2. Scope

The review covered two domains and three real messages, and was done without access to any company system.

### What was reviewed

| Item | Detail |
|---|---|
| Domains | `andinalogistica.example` (main) and `andinalogistica-mx.example` (regional variant registered to protect the brand) |
| Public DNS records | DMARC, SPF (with recursive lookup count), DKIM, MX, MTA-STS, TLS-RPT, BIMI and DNSSEC |
| Real messages | Three emails sent to a test mailbox: one from an employee, one e-invoice and one newsletter |
| Senders | Identification of the platforms that send email on the company's behalf, from SPF, DKIM selectors and headers |

### How it was done

- DNS queries from an external resolver, to see what any mail server on the internet sees.
- Reading each message's `Authentication-Results` headers, which show how the receiving server evaluated SPF, DKIM and DMARC.
- Each finding was rated by severity and by remediation effort (scales in appendix B).

**What it does not include**

- Changes to DNS or to any platform. This report says what to fix and in what order; implementation is a separate service (section 7).
- Review of mailboxes, spam filtering or the internal Microsoft 365 configuration.
- Analysis of historical DMARC reports: there are none, because reports are not arriving (finding H3).

**Review date:** November 22, 2026. DNS may change after that date.

## 3. Status by domain and summary of findings

Neither domain blocks spoofed email today. The regional one is completely open, and the main one has DMARC published, but with no effect and no data.

| Domain | Status | What it means |
|---|---|---|
| `andinalogistica-mx.example` | **Exposed** | Anyone can send email on behalf of this domain today |
| `andinalogistica.example` | **Monitoring blind** | The record exists, but it produces no data at all |

The full status scale is in appendix B. The goal for both domains is **Protected**: spoofed email is rejected by the recipient's server.

**Prioritized findings**

First come those that cancel protection, then those that leave it without visibility, then those that block the path to rejection, and finally observations.

| # | Finding | Domain | Severity | Effort |
|---|---|---|---|---|
| H1 | No DMARC and no SPF | Regional | Critical | Low |

| # | Finding | Domain | Severity | Effort |
|---|---|---|---|---|
| H2 | SPF exceeds the 10-lookup limit (permanent error) | Main | Critical | Low |
| H3 | DMARC reports are not arriving: the external destination's authorization is missing | Main | High | Low |
| H4 | The invoicing platform does not sign with the company's domain | Main | High | Medium |
| H5 | `p=none` policy: monitors, does not block | Main | High | Medium |
| H6 | DKIM selector with a revoked key, left over from a previous provider | Main | Observation | Low |
| H7 | MTA-STS, TLS-RPT and DNSSEC not published | Main | Observation | — |

H2's effort is low because the fix removes entries from the record instead of adding them.

## 4. Findings in detail

Each finding answers four questions in the same order. Technical detail goes in a separate block, for whoever manages DNS.

### H1. The regional domain has no DMARC and no SPF — Critical · Low effort

**What we found.** `andinalogistica-mx.example` publishes no DMARC, SPF or MX records. The domain was registered to protect the brand and neither sends nor receives email.

**What it means for the business.** Anyone can send an email from `billing@andinalogistica-mx.example`. A customer has no way of knowing the domain isn't yours, and no receiving server has instructions to reject it.

**What happens if it isn't fixed.** Anyone attempting bank-account-change fraud will prefer the unprotected domain. Protecting only the main domain leaves the door next to it open.

**Effort: low.** Three DNS records. Since the domain sends no email, it can go straight to rejection, with no monitoring stage.

```
Current state
_dmarc.andinalogistica-mx.example   TXT   (does not exist)
andinalogistica-mx.example          TXT   (no SPF)
andinalogistica-mx.example          MX    (does not exist)

Proposed fix
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 .        (null MX, RFC 7505)
```

## H2. SPF exceeds the 10-lookup limit — Critical · Low effort

**What we found.** Walking the main domain's SPF and every record it includes, evaluation needs 11 DNS lookups. The standard stops at 10. One of them is also a void lookup: it points to a hosting provider that no longer responds.

**What it means for the business.** Past the limit, the result is a permanent error (`permerror`). The record looks complete, but in practice it authorizes no server at all.

**What happens if it isn't fixed.** When the DMARC policy tightens, mail that relies on SPF to pass will fail. And every new provider added makes the count worse.

**Effort: low.** The fix removes three entries that add nothing, and brings the count to 8 of 10.

```
Current record (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

Count: 7 top-level + 4 nested = 11 of 10 → permerror
Void lookup: _spf.hosting-anterior.example (NXDOMAIN)

What is removed and why
- include:_spf.hosting-anterior.example
    provider no longer used (void lookup)
- mx
    MX records point to Microsoft 365, already covered by its include
- a
```

```
    the web server does not send email (confirm first that the
    site's contact form does not send from that server either)

Proposed record (8 of 10)
v=spf1
  include:spf.protection.outlook.com
  include:_spf.boletines.example
  include:_spf.facturador.example
  include:_spf.crm-ventas.example
  ~all

(SPF records are shown on several lines for readability;
they are published on a single line.)
```

Ending with `~all` instead of `-all` is recorded as an observation, not a failure: it matters less once DMARC is at `p=reject`.

### H3. DMARC reports are not arriving — High · Low effort

**What we found.** The DMARC record sends reports to `reportes-proveedor.example`, a domain different from yours. In that case, the protocol requires the owner of the receiving domain to publish an authorization. That authorization does not exist.

**What it means for the business.** You set up a reporting service that is not receiving reports. Google and Microsoft drop the reports silently, so there is no visible error anywhere.

**What happens if it isn't fixed.** Without reports, there is no way to know who sends email on your behalf, or to confirm that every legitimate system passes before tightening the policy. If the record was set up months ago, it has produced no data for months.

**Effort: low.** Two options: ask the reporting provider to publish the authorization, or receive reports in a mailbox on your own domain, which doesn't need it.

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

Authorization that should exist (in the provider's zone)
andinalogistica.example._report._dmarc.reportes-proveedor.example
  TXT  (does not exist)
*._report._dmarc.reportes-proveedor.example
  TXT  (does not exist)

Expected record: "v=DMARC1"
```

### H4. The invoicing platform does not sign with the company's domain — High · Medium effort

**What we found.** E-invoices are sent from `billing@andinalogistica.example`, but the platform signs them with its own domain and uses its own domain for bounces. Neither check aligns with the company's domain, so the message fails DMARC (see message 2 in section 5).

**What it means for the business.** Today invoices are delivered only because the policy is `p=none`. To receiving servers, a legitimate invoice and a fake one look the same: both fail.

**What happens if it isn't fixed.** The day the policy moves to quarantine or reject, invoices would start landing in spam or not arriving at all. It is the classic DMARC project mistake: a forgotten system that breaks the day of the change.

**Effort: medium.** It requires coordinating with the invoicing provider. Most of these platforms let you set up DKIM signing with the customer's domain by publishing one or two records the provider supplies.

```
Message 2 (invoice), Authentication-Results:
spf=pass smtp.mailfrom=rebotes.facturador.example
    → does not align with From
dkim=pass header.d=facturador.example
    → does not align with From
dmarc=fail action=none header.from=andinalogistica.example

Fix: DKIM with d=andinalogistica.example on the invoicing
platform (CNAME or TXT records supplied by the provider).
Optional: custom bounce domain.
```

### H5. The DMARC policy only monitors — High · Medium effort

**What we found.** The main domain publishes `p=none`.

**What it means for the business.** The domain is watching, not defending. Spoofed email is still delivered as if nothing were published.

**What happens if it isn't fixed.** The company stays where most organizations stop: DMARC published, a sense of being protected, and no spoofed email blocked.

**Effort: medium.** It isn't fixed by changing the policy right away. First H2, H3 and H4 have to be resolved, and at least three weeks of reports have to confirm that every legitimate sender passes. Then the policy tightens in stages (section 7).

### H6. DKIM selector with a revoked key — Observation · Low effort

**What we found.** Selector `k1` exists, but its key is empty (revoked). This is usually left over from a provider no longer in use.

**What it means.** It is not a risk: a revoked key cannot sign. Removing it keeps DNS clean and avoids confusion in future reviews.

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

### H7. MTA-STS, TLS-RPT and DNSSEC not published — Observation

**What we found.** The main domain does not publish MTA-STS or TLS-RPT, and its zone is not signed with DNSSEC.

**What it means.** These are not failures, but improvements for a second stage. MTA-STS requires inbound email to travel encrypted, and TLS-RPT reports when that fails. BIMI, which shows the company's logo next to its emails, requires `p=reject` first.

## 5. Review of real message headers

DNS says who is authorized to send; headers show what actually happens to each message. Of the three systems reviewed, two pass DMARC and one fails: invoicing.

For each message we read the `Authentication-Results` header added by the receiving server. A message passes DMARC if SPF or DKIM passes **and** is aligned, meaning it uses the same domain shown in the visible sender (`From`).

| # | Message | System | SPF | DKIM | DMARC | With `p=reject` |
|---|---|---|---|---|---|---|
| 1 | Employee email | Microsoft 365 | Pass, aligned | Pass, aligned (`selector1`) | **Pass** | Delivered |
| 2 | E-invoice | Invoicing platform | Pass, **not aligned** | Pass, **not aligned** | **Fail** | **Would be rejected** |
| 3 | Newsletter | Newsletter platform | Pass, not aligned | Pass, aligned (`bol1`) | **Pass** | Delivered |

### What they tell us

- **Microsoft 365 is configured well.** It signs with the company's domain and passes both ways.
- **Invoicing is the sender to fix before tightening** (finding H4). It's the most common pattern: the system that matters most to the business is the one nobody checked.
- **The newsletter passes through DKIM only.** SPF does not align because the platform uses its own domain for bounces, and that is normal. One aligned check is enough.
- **Selector `bol1` is not on the list of common names** probed from outside. It was identified from the headers. That is why reviewing real messages complements the DNS review: each provider chooses its DKIM selector name, and it cannot be enumerated from outside.

```
Message 1 — employee (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

Message 2 — e-invoice
spf=pass smtp.mailfrom=rebotes.facturador.example
dkim=pass header.d=facturador.example
dmarc=fail action=none header.from=andinalogistica.example

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

In a real review, messages are requested from every system that sends on the company's behalf. Three messages are the minimum; the full sender inventory is then confirmed with DMARC reports.

## 6. What is configured well

The foundation is good: the main email is properly authenticated, and most of the pending work is putting existing pieces in order, not building from scratch.

- **Microsoft 365 signs with the company's domain.** Selectors `selector1` and `selector2` have valid keys, and employee email passes DMARC through both SPF and DKIM.
- **The newsletter platform has its own DKIM** (`bol1`), aligned with the company's domain.
- **There is a single DMARC record and a single SPF record**, with valid syntax. A duplicate record would cancel the whole policy.
- **MX records point to Microsoft 365** and respond correctly.
- **The decision to use DMARC is already made.** Someone set it up and hired a reporting service. What's left is finishing the path, not convincing anyone to start it.

## 7. Remediation plan and next step

The path to Protected takes about 12 weeks. The policy never moves to the next stage while a legitimate sender is still failing, and rolling back is a single DNS record change.

| Stage | Weeks | What happens | Who | Condition to advance |
|---|---|---|---|---|
| 0. Quick wins | 1 | Protect the regional domain (H1), bring SPF to 8 of 10 (H2), fix the report destination (H3) and remove the revoked selector (H6) | Whoever manages DNS | Reports start arriving within 24–72 hours |

| Stage | Weeks | What happens | Who | Condition to advance |
|---|---|---|---|---|
| 1. Fix senders | 1–3 | Custom DKIM on the invoicing platform (H4); check reports for any system that wasn't in the inventory | IT with the invoicing provider | Every legitimate system passes DMARC in the reports |
| 2. Monitoring | 3–6 | Keep `p=none` and review reports weekly | Report review | Three consecutive weeks with no legitimate sender failures |
| 3. Gradual quarantine | 6–10 | `p=quarantine` with `pct=25`, then 50, then 100, reviewing reports after each step | Whoever manages DNS | No legitimate email affected at each step |
| 4. Reject | ~12 | `p=reject` and `sp=reject`; tighten alignment only if every sender supports it | Whoever manages DNS | Domain **Protected** |
| 5. Improvements | Later | MTA-STS, TLS-RPT and, if of interest, BIMI (H7) | IT | — |

```
DMARC records by stage (main domain)
Stages 0–2   v=DMARC1; p=none; rua=mailto:<report-destination>
Stage 3      v=DMARC1; p=quarantine; pct=25; rua=mailto:<report-destination>
             (then pct=50 and pct=100)
Stage 4      v=DMARC1; p=reject; sp=reject; rua=mailto:<report-destination>
```

**What the company needs to provide:** someone who can publish DNS changes on the agreed dates, and the technical contact at the invoicing platform. That is usually the real bottleneck, so it's worth settling at the start.

**Next step.** Your IT team can run this plan on its own with this report. If you'd rather I do it, the DMARC rollout service covers stages 0 to 4: coordination with providers, weekly report review, every policy change on its date, and a closing report. The cost of this review

is credited toward the rollout. After rejection, ongoing monitoring can continue on a specialized platform; if you're interested, I can recommend options based on the company's size and needs.

## Appendix A. DNS records queried

```
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  valid RSA key (Microsoft 365)
  selector2       DKIM  valid RSA key (Microsoft 365)
  bol1            DKIM  valid RSA key (newsletter platform;
                        identified from headers)
  k1              DKIM  v=DKIM1; p=   (revoked)
  _mta-sts        TXT   (does not exist)
  _smtp._tls      TXT   (does not exist)
  default._bimi   TXT   (does not exist)
  DNSSEC                zone not signed

andinalogistica-mx.example
  _dmarc          TXT   (does not exist)
  @ (SPF)         TXT   (does not exist)
  @               MX    (does not exist)

reportes-proveedor.example
  andinalogistica.example._report._dmarc   TXT   (does not exist)
  *._report._dmarc                         TXT   (does not exist)
```

## Appendix B. Scales and criteria

### Domain status

| Status | Condition |
|---|---|
| Exposed | No DMARC, or DMARC that is invalid or duplicated |
| Monitoring | `p=none` with working reports |
| Monitoring blind | `p=none` without reports, or with an external destination that lacks authorization |
| Partial protection | `quarantine`, `reject` with `pct` below 100, or `reject` with subdomains at `sp=none` |
| Protected | `p=reject`, `pct=100`, subdomains protected, healthy SPF and DKIM |
| Indeterminate | The domain does not resolve or the result does not allow a conclusion; it is reviewed by hand and never treated as Exposed |

A status is used instead of a 0–100 score: the useful question isn't "what grade did we get" but "what's missing to move up a status."

### Finding severity

| Severity | Criterion | Examples |
|---|---|---|
| Critical | Cancels all protection for the domain | No DMARC; duplicate or invalid DMARC; SPF over 10 lookups or duplicated; SPF with `+all` or `?all` |
| High | Leaves protection without effect or visibility, or blocks the path to rejection | `p=none`; missing or unauthorized reports; a legitimate sender without alignment; no SPF |
| Medium | Partial protection or risk of future error | `quarantine` or `pct` below 100; subdomains at `sp=none`; more than 2 void lookups in SPF; `ptr` mechanism; SPF without a final `all`; DKIM key under 1024 bits |
| Observation | Improvement, hygiene or informational, with no current risk | `~all` or relaxed alignment with `p=reject`; revoked selector; MTA-STS, TLS-RPT, DNSSEC or BIMI missing |

### Remediation effort

| Effort | What it involves |
|---|---|
| Low | One or a few DNS record changes |
| Medium | Coordinating with an external provider |
| High | Internal inventory of systems that send email |

### Rigor criteria

- **DKIM:** when no selector is found, the report says “we found no selectors among common names,” never “they have no DKIM.” Each provider chooses the selector name, and it cannot be enumerated from outside.
- **Unverified is not the same as nonexistent:** if a query does not respond, the item is marked as unverified.
- **Capability, not accusation:** the report says a domain can be spoofed, never that it was used for fraud.
- **No industry figures:** findings rely only on verifiable data about the domain reviewed.