

SEGURIDAD DE LA INFORMACIÓN

# Caso de éxito Implementación de DMARC



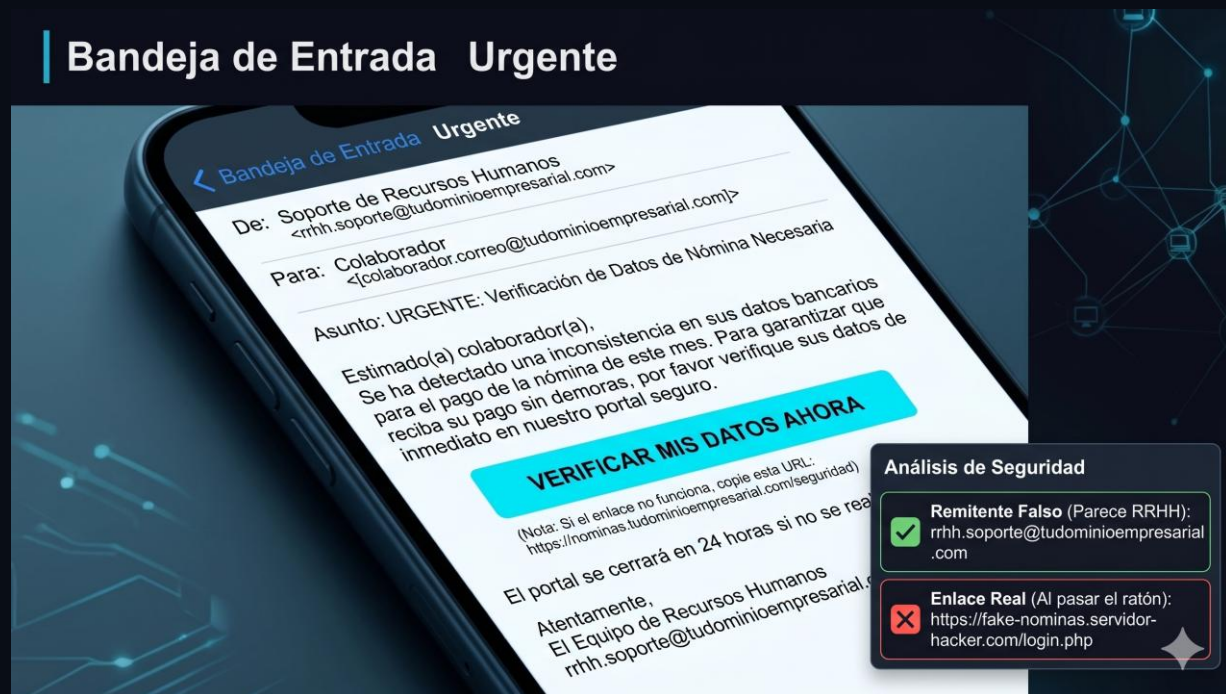
# El Reto



El correo electrónico estándar es inherentemente inseguro.

# | El reto en Ciberseguridad del correo electrónico

- **El correo electrónico es cada vez más vulnerable** a los ciberataques, usando la suplantación de identidad (Spoofing) como medio de ataque de Spear phishing o el whaling, entre otros.
- **Con la IA,** los ataques son cada vez más convincentes y difíciles de detectar.
- ¿Cómo le aseguramos a nuestros clientes y aliados que el correo que enviamos **es legítimo**?



## | Posibles riesgos de la suplantación de identidad

- **Riesgos reputacionales**
- **Riesgos legales**
- **Riesgos financieros**

# La Solución



Los protocolos de autenticación de correo electrónico en basado en DNS

## ¿Qué son DMARC, DKIM y SPF?

- El **SPF**, el **DKIM** y el **DMARC** ayudan a autenticar a los remitentes de correo electrónico verificando que los correos electrónicos proceden del **dominio** del que dicen proceder.
- Son importantes para evitar el spam, los ataques de phishing y otros riesgos de seguridad del correo electrónico.



## ¿Qué son DMARC, DKIM y SPF?

- El **SPF**, es una lista de servidores autorizados para enviar correos desde tu dominio.
- El **DKIM** es una firma digital que valida quién envió el correo y que nadie lo modificó en tránsito.
- El **DMARC** es un protocolo que coordina SPF y DKIM para dictar cómo actuar ante correos falsos y prevenir la suplantación de identidad.



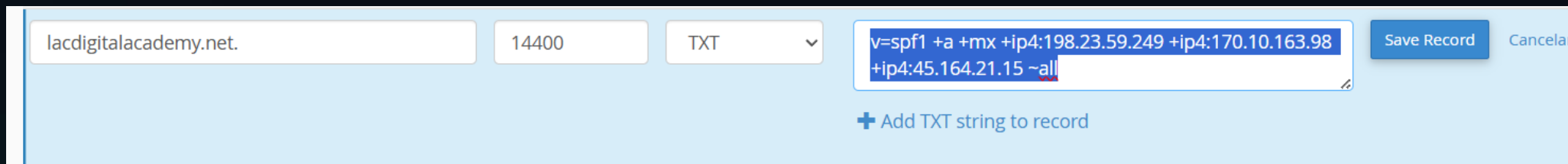
# Los Resultados



La configuración de los protocolos

## | ¿Cómo configurarlo?

- El **SPF**, el **DKIM** y el **DMARC** se almacenan en el Sistema de Nombres de Dominio (DNS), que es de acceso público.
- Los registros **DKIM**, **SPF** y **DMARC** se almacenan como registros TXT de DNS.



The screenshot shows a DNS configuration interface. On the left, there is a text input field containing 'lacdigitalacademy.net.'. To its right is a numeric input field with '14400'. Further right is a dropdown menu currently set to 'TXT'. To the right of the dropdown is a large text area containing the SPF record: 'v=spf1 +a +mx +ip4:198.23.59.249 +ip4:170.10.163.98 +ip4:45.164.21.15 ~all'. Below this text area is a link that says '+ Add TXT string to record'. To the right of the text area are two buttons: 'Save Record' and 'Cancela'.

lacdigitalacademy.net. 14400 TXT

v=spf1 +a +mx +ip4:198.23.59.249 +ip4:170.10.163.98 +ip4:45.164.21.15 ~all

+ Add TXT string to record

Save Record Cancela

# Antes y Después

dmarc:lacdigitalacademy.net

Find Problems

Solve Email Delivery Problems

dmarc



Outlook.com has new sender requirements!

Get ready with MxToolbox Delivery Center!

Learn More

```
v=DMARC1; p=none;
```

| Tag | TagValue | Name    | Description                                                                                                |
|-----|----------|---------|------------------------------------------------------------------------------------------------------------|
| v   | DMARC1   | Version | Identifies the record retrieved as a DMARC record. It must be the first tag in the list.                   |
| p   | none     | Policy  | Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'. |

| Test                        | Result                                                                                      |
|-----------------------------|---------------------------------------------------------------------------------------------|
| ✖ DMARC Policy Not Enabled  | DMARC Quarantine/Reject policy not enabled                                                  |
| ✔ DMARC Record Published    | DMARC Record found                                                                          |
| ✔ DMARC Syntax Check        | The record is valid                                                                         |
| ✔ DMARC Multiple Records    | Multiple DMARC records corrected to a single record.                                        |
| ✔ DMARC External Validation | All external domains in your DMARC record are giving permission to send them DMARC reports. |

More Info

[dns lookup](#) [dns check](#) [mx lookup](#) [spf lookup](#) [dns propagation](#)  
Reported by [dns4.akkyhosting2.mx](#) on 7/31/2026 at 3:44:35 PM (UTC -5), [just for you.](#)

dmarc:lacdigitalacademy.net

Find Problems

Solve Email Delivery Problems

dmarc

```
v=DMARC1;p=quarantine;sp=none;adkim=r;aspf=r;pct=100;fo=0;rf=afrr;ri=86400;rua=mailto:66ftuo00@rua.sa.dmarcmanager.app;ruf=mailto:66ftuo00@rua.sa.dmarcmanager.app;
```

| Tag   | TagValue                                | Name                | Description                                                                                                                                                         |
|-------|-----------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v     | DMARC1                                  | Version             | Identifies the record retrieved as a DMARC record. It must be the first tag in the list.                                                                            |
| p     | quarantine                              | Policy              | Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.                                                          |
| sp    | none                                    | Sub-domain Policy   | Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.                                                           |
| adkim | r                                       | Alignment Mode DKIM | Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).         |
| aspf  | r                                       | Alignment Mode SPF  | Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).          |
| pct   | 100                                     | Percentage          | Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.                  |
| fo    | 0                                       | Forensic Reporting  | Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by '.'.                               |
| rf    | afrr                                    | Forensic Format     | Format to be used for message-specific failure reports. Valid values are 'afrr' and 'odef'.                                                                         |
| ri    | 86400                                   | Reporting Interval  | Indicates a request to Receivers to generate aggregate reports separated by no more than the requested number of seconds. Valid value is a 32-bit unsigned integer. |
| rua   | mailto:66ftuo00@rua.sa.dmarcmanager.app | Receivers           | Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.                                                                 |
| ruf   | mailto:66ftuo00@rua.sa.dmarcmanager.app | Forensic Receivers  | Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.                                           |

| Test                        | Result                                                                                      |
|-----------------------------|---------------------------------------------------------------------------------------------|
| ✔ DMARC Record Published    | DMARC Record found                                                                          |
| ✔ DMARC Syntax Check        | The record is valid                                                                         |
| ✔ DMARC Multiple Records    | Multiple DMARC records corrected to a single record.                                        |
| ✔ DMARC Policy Not Enabled  | DMARC Quarantine/Reject policy enabled                                                      |
| ✔ DMARC External Validation | All external domains in your DMARC record are giving permission to send them DMARC reports. |

[dns lookup](#) [dns check](#) [mx lookup](#) [spf lookup](#) [dns propagation](#)  
Reported by [dns3.akkyhosting2.mx](#) on 8/5/2026 at 1:35:49 PM (UTC -5), [just for you.](#)

Transcript

# Configurando SPF

**v=spf1 ip4:198.23.59.249 ip4:170.10.163.98 ~all**

**Versión**

**Direcciones IP Autorizadas**

**Política**

lacidigitalacademy.net SPF Record Lookup

spf:lacidigitalacademy.net Find Problems Solve Email Delivery Problems

v=spf1 ip4:198.23.59.249 ip4:170.10.163.98 ip4:45.164.21.15 ~all

| Prefix | Type | Value         | PrefixDesc | Description                                        |
|--------|------|---------------|------------|----------------------------------------------------|
|        | v    | spf1          |            | The SPF record version                             |
| +      | ip4  | 198.23.59.249 | Pass       | Match if IP is in the given range.                 |
| +      | ip4  | 170.10.163.98 | Pass       | Match if IP is in the given range.                 |
| +      | ip4  | 45.164.21.15  | Pass       | Match if IP is in the given range.                 |
| ~      | all  |               | SoftFail   | Always matches. It goes at the end of your record. |

# Configurando DKIM

**v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9...QIDAQAB;**

**Versión**

**Tipo de Clave: RSA**

**Clave pública**

dkim:lacdigitalacademy.net:default

Find Problems

dkim

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwM34Bpes18USxiENUZq+VIhpelNO5S9d03JANPci1NjnLmGUwHgoEYcocPKM+OAwPFTmrdVfaZoPU8z+Fx7E44UyRZkgUBpmA83OKy3/zmypi5f8GSBSwXtINj2jtn0A+AFzFKbIeMSm4/X6NsI/rPSVT4WBBZXszbYCOhzczzffOorTV7pvCFRNP6VUFCAH64RVrx7UR20ulf0I+jOurjToua+GPqTew3EJ2jvzkERMSC/Us1L6stV9P+Oa2ZssP3FC1kxdMMz1ecgs8uIVFZJhk1Vg8ML2GgnnBNcdRncHsvAdqjOSXMkThiPNHcDVd1zs49oxzJMjAsqvIcI4tQIDAQAB;
```

| Tag | TagValue                                                                                                                                                                                                                                                                                                                                                                                                 | Name       | Description                                                                                           |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------------------------------|
| v   | DKIM1                                                                                                                                                                                                                                                                                                                                                                                                    | Version    | Identifies the record retrieved as a DKIM record. It must be the first tag in the record.             |
| k   | rsa (Length: 2048 bits)                                                                                                                                                                                                                                                                                                                                                                                  | Key Type   | The type of the key used by tag (p).                                                                  |
| p   | MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwM34Bpes18USxiENUZq+VIhpelNO5S9d03JANPci1NjnLmGUwHgoEYcocPKM+OAwPFTmrdVfaZoPU8z+Fx7E44UyRZkgUBpmA83OKy3/zmypi5f8GSBSwXtINj2jtn0A+AFzFKbIeMSm4/X6NsI/rPSVT4WBBZXszbYCOhzczzffOorTV7pvCFRNP6VUFCAH64RVrx7UR20ulf0I+jOurjToua+GPqTew3EJ2jvzkERMSC/Us1L6stV9P+Oa2ZssP3FC1kxdMMz1ecgs8uIVFZJhk1Vg8ML2GgnnBNcdRncHsvAdqjOSXMkThiPNHcDVd1zs49oxzJMjAsqvIcI4tQIDAQAB | Public Key | The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag. |

# Configurando DMARC

**v=DMARC1; p=reject; rua=mailto:dmarc-reports@tudominio.com;**

**Versión**

**Política: None, Quarantine, Reject**

**Correo electrónico destinado a la recepción de reportes DMARC**

dmARC:lacdigitalacademy.net [Find Problems](#) [Solve Email Delivery Problems](#) [dmARC](#)

```
v=DMARC1;p=quarantine;sp=quarantine;adkim=r;aspf=r;pct=100;fo=0;rf=afrr;ri=86400;rua=mailto:66ftuo00@rua.sa.dmarcmanager.app;ruf=mailto:66ftuo00@ruf.sa.dmarcmanager.app;
```

| Tag   | TagValue                                | Name                | Description                                                                                                                                                         |
|-------|-----------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v     | DMARC1                                  | Version             | Identifies the record retrieved as a DMARC record. It must be the first tag in the list.                                                                            |
| p     | quarantine                              | Policy              | Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.                                                          |
| sp    | quarantine                              | Sub-domain Policy   | Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.                                                           |
| adkim | r                                       | Alignment Mode DKIM | Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).         |
| aspf  | r                                       | Alignment Mode SPF  | Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).          |
| pct   | 100                                     | Percentage          | Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.                  |
| fo    | 0                                       | Forensic Reporting  | Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' separated by '.'.                               |
| rf    | afrr                                    | Forensic Format     | Format to be used for message-specific failure reports. Valid values are 'afrr' and 'odef'.                                                                         |
| ri    | 86400                                   | Reporting Interval  | Indicates a request to Receivers to generate aggregate reports separated by no more than the requested number of seconds. Valid value is a 32-bit unsigned integer. |
| rua   | mailto:66ftuo00@rua.sa.dmarcmanager.app | Receivers           | Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.                                                                 |
| ruf   | mailto:66ftuo00@ruf.sa.dmarcmanager.app | Forensic Receivers  | Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.                                           |

| Test                        | Result                                                                                      |
|-----------------------------|---------------------------------------------------------------------------------------------|
| ✓ DMARC Record Published    | DMARC Record found                                                                          |
| ✓ DMARC Syntax Check        | The record is valid                                                                         |
| ✓ DMARC Multiple Records    | Multiple DMARC records corrected to a single record.                                        |
| ✓ DMARC Policy Not Enabled  | DMARC Quarantine/Reject policy enabled                                                      |
| ✓ DMARC External Validation | All external domains in your DMARC record are giving permission to send them DMARC reports. |

[dns lookup](#) [dns check](#) [mx lookup](#) [spf lookup](#) [dns propagation](#)

Reported by [dns2.akkyhosting2.mx](#) on 8/13/2026 at 4:41:33 PM (UTC -5). [Just for you](#) [Transcript](#)

<https://mxtoolbox.com/dmarc.aspx>

# GRACIAS POR SU ATENCIÓN

La ciberseguridad es responsabilidad de todos.  
#ProtegeTuEmpresa

