

# Guía de Configuración de Autenticación de Email

## Para Salir de Spam - Red Team Xal Digital

**Objetivo:** Configurar SPF, DKIM y DMARC en [xaldigital.com](http://xaldigital.com) para que los correos de phishing test lleguen a inbox (no a spam)

**Tiempo estimado:** 30-45 minutos

**Dificultad:** Media

**Herramientas necesarias:** Acceso al panel de control del dominio

---

### ¿Qué haremos?

Configuraremos **3 autenticaciones de email**:

Protocolo	Función	Prioridad
<b>SPF</b>	Dice qué servidores pueden enviar emails del dominio	
<b>DKIM</b>	Firma digitalmente los emails	
<b>DMARC</b>	Política de cómo manejar emails no autenticados	

**Resultado:** Los correos irán a inbox, no a spam

---

### Paso 0: Verificación Previa

Antes de empezar, verifica que tienes acceso al panel:

- Acceso a cPanel / Plesk / Panel de control del hosting
  - Acceso a DNS Zone Editor o similar
  - Dominio: **xaldigital.com** (con la “i” que falta )
- 

### PASO 1: Configurar SPF (Sender Policy Framework)

#### ¿Qué es SPF?

SPF le dice a Gmail: “Estos servidores pueden enviar emails en nombre de [xaldigital.com](http://xaldigital.com)”

## Dónde Configurar

1. Accede a tu **Panel de Control** del hosting
2. Busca: **DNS Zone Editor / Advanced DNS / Manage DNS**
3. Encuentra tu dominio: **xaldigital.com**

## Agregar Registro SPF

### Opción A: Si usas cPanel

Ir a: Home → Domains → xaldigital.com → Zone Editor

### Opción B: Si usas Plesk

Ir a: Domains → xaldigital.com → DNS Settings

## El Registro SPF que Debes Agregar

**Tipo de Registro:** TXT

**Nombre/Host:** xaldigital.com (o dejar en blanco)

**Valor:**

v=spf1 include:google.com include:sendgrid.net include:mailgun.org ~all

**¿Por qué este registro?** - v=spf1 = Versión 1 de SPF - include:google.com = Google puede enviar emails - include:sendgrid.net = SendGrid puede enviar (si lo usas) - include:mailgun.org = Mailgun puede enviar (si lo usas) - ~all = Otros servidores pueden intentar, pero no están garantizados

## ¿Cómo Agregarlo en cPanel?

**Pasos exactos:**

1. Haz clic en el ícono + para agregar nuevo registro
2. Selecciona **TXT** en el dropdown
3. En “Name” escribe: **xaldigital.com** (o déjalo en blanco)
4. En “TTL” escribe: **3600** (1 hora)
5. En “Text” pega:

v=spf1 include:google.com include:sendgrid.net include:mailgun.org ~all

6. Haz clic en **Add Record**

## ¿Cómo Verificar que Funcionó?

En terminal (o PowerShell en Windows):

**nslookup -type=TXT xaldigital.com**

O usa el sitio: <https://mxtoolbox.com/spf.aspx> - Ingresa: `xaldigital.com` - Debe mostrar: PASS (en verde)

**Si no funciona:** Espera 15-30 minutos (propagación DNS)

---

## PASO 2: Configurar DKIM (DomainKeys Identified Mail)

### ¿Qué es DKIM?

DKIM firma cada email digitalmente. Gmail verifica la firma y confía más en el correo.

### Dónde Conseguir DKIM

#### Opción A: Generarlo en cPanel (Recomendado)

1. Ve a: **Home → Email → Email Deliverability**
2. En la sección **DKIM**, haz clic en **Enable DKIM Signing**
3. Selecciona el dominio: `xaldigital.com`
4. Haz clic en **Install a DKIM record for this domain**

#### Opción B: Si no aparece en Email Deliverability

Ve a: **Home → Domains → xaldigital.com → DKIM** (si está disponible)

### Si tu hosting es Plesk

1. Ve a: **Domains → xaldigital.com → Mail → DKIM**
2. Haz clic en **Enable DKIM Signing**
3. Se genera automáticamente

### El Registro DKIM (Si debes agregarlo manualmente)

**Tipo de Registro:** TXT

**Nombre/Host:** `default._domainkey.xaldigital.com`

**Valor:** Se verá algo como esto (depende de tu hosting):

`v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC...`

**NOTA:** Este valor es muy largo. Cópialo exactamente, sin cambios.

### ¿Cómo Verificar que Funcionó?

En: <https://dmarcian.com/dkim-survey/>

Ingresa: `default._domainkey.xaldigital.com`

Debe mostrar: **DKIM record found and valid**

---

## PASO 3: Configurar DMARC (Domain-based Message Authentication)

### ¿Qué es DMARC?

DMARC es una política que dice a Gmail: “Si este email no pasa SPF y DKIM, ¿qué haces?”

### El Registro DMARC

Tipo de Registro: TXT

Nombre/Host: \_dmarc.xaldigital.com

Valor:

v=DMARC1; p=quarantine; rua=mailto:security-test@xaldigital.com; ruf=mailto:security-test@xal

¿Qué significa? - v=DMARC1 = Versión 1 de DMARC - p=quarantine = Si falla, manda a cuarentena (spam) - rua=mailto: = Envíame reportes diarios - ruf=mailto: = Envíame reportes de fallos - fo=1 = Reporta cualquier fallo

### Cómo Agregarlo

1. Ve al **DNS Zone Editor** (como en SPF)
2. Haz clic en **+ Add Record**
3. Selecciona: **TXT**
4. En “Name” escribe: **\_dmarc.xaldigital.com**
5. En “TTL” escribe: **3600**
6. En “Text” pega:  
**v=DMARC1; p=quarantine; rua=mailto:security-test@xaldigital.com; ruf=mailto:security-test@xal**
7. Haz clic en **Add Record**

### ¿Cómo Verificar que Funcionó?

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

Ingresar: **xaldigital.com**

Debe mostrar: **DMARC record found**

---

## RESUMEN DE REGISTROS DNS

Después de configurar todo, deberías tener estos registros en tu DNS:

Tipo	Nombre	Valor
TXT	xaldigital.com	v=spf1 include:google.com include:sendgrid.net include:mailgun.org ~all
TXT	default._domainkey.xaldigital.com	DKIM1; k=rsa; p=MIGfMA... (muy largo)
TXT	_dmarc.xaldigital.com	v=DMARC1; p=quarantine; rua=mailto:security-test@xaldigital.com; ...

---

## PASO 4: Pruebas de Validación

### Test 1: Mail-tester (Recomendado)

1. Ve a: <https://www.mail-tester.com/>
2. Copia tu dirección de prueba (ej: [test-xxxxx@mail-tester.com](mailto:test-xxxxx@mail-tester.com))
3. Envía un correo DE [recursos.humanos@xaldigital.com](mailto:recursos.humanos@xaldigital.com) A esa dirección
4. Espera 30 segundos
5. Regresa al sitio y haz clic en **Then check your score**

Resultado esperado: **8-10 de 10**

### Test 2: Check-mail.org

1. Ve a: <https://check-mail.org/>
2. Ingresa: [recursos.humanos@xaldigital.com](mailto:recursos.humanos@xaldigital.com)
3. Verifica que aparezca en todos los tests

### Test 3: Gmail Real

1. Envía un correo a tu cuenta personal de Gmail
2. Verifica que llegue a **Inbox**, NO a Spam
3. Haz clic en el correo
4. Verifica que muestre (autenticado)

---

## PASO 5: Verificar Propagación DNS

Los cambios en DNS pueden tomar **15 minutos a 48 horas** en propagarse completamente.

Para verificar el estado:

**Opción A:** <https://dnschecker.org/> - Ingresa: `xaldigital.com` - Busca los 3 registros TXT que agregaste - Si ves en todos = Completamente propagado

**Opción B:** En terminal

```
nslookup -type=TXT xaldigital.com
nslookup -type=TXT default._domainkey.xaldigital.com
nslookup -type=TXT _dmarc.xaldigital.com
```

---

### Si Algo Sale Mal

“No puedo encontrar DNS Zone Editor”

**Solución:** - Si tienes **cPanel**: Home → Domains → Zone Editor - Si tienes **Plesk**: Domains → DNS Settings - Si tienes **otro hosting**: Contacta a soporte

“Agregué el registro pero no funciona”

**Soluciones:** 1. **Espera:** Propagación puede tomar hasta 48 horas 2. **Verifica:** Copia exactamente, sin espacios extras 3. **Revisa:** ¿Escribiste bien `xaldigital.com`? (con la “i” que falta) 4. **TTL:** Intenta bajar a 300 y vuelve a esperar

“Los emails siguen yendo a spam”

**Pasos de debugging:**

1. **Verifica SPF:** <https://mxtoolbox.com/spf.aspx> → ingresa `xaldigital.com`
  2. **Verifica DKIM:** <https://dkmarcian.com/dkim-survey/>
  3. **Verifica DMARC:** <https://mxtoolbox.com/dmard.aspx> → ingresa `xaldigital.com`
- 

## CHECKLIST DE CONFIGURACIÓN

Marca cada paso conforme lo completes:

### Configuración DNS

- SPF:** Registro agregado y verificado
- DKIM:** Habilitado en cPanel O registro agregado manualmente
- DMARC:** Registro agregado en DNS

## **Verificación**

- Mail-tester score 8/10
  - MXToolbox SPF = PASS
  - MXToolbox DMARC = Found
  - Correo de prueba llega a Inbox de Gmail (no Spam)
- 

## **Preguntas Frecuentes**

**P:** ¿Puedo cambiar el valor de SPF?

**R:** Sí, pero ten cuidado. Usa ~all (soft fail) para testing.

**P:** ¿Cuánto tiempo tarda en propagarse?

**R:** 5-15 minutos (inmediato), pero puede tomar hasta 48 horas en algunos ISPs.

**P:** ¿Necesito hacer algo en el servidor de email?

**R:** No, solo DNS. Todo se configura ahí.

---

## **Confirmación Final**

Cuando termines TODOS los pasos, reporta a Alex:

SPF: Configurado y verificado  
DKIM: Habilitado y verificado  
DMARC: Configurado y verificado  
Mail-tester score: 9/10  
Correo de prueba: Llegó a Inbox  
Listo para campaña

---

**¡Mucho éxito configurando los registros DNS!**