

Plan: Resolver Rechazo de Correos por DKIM en Gmail

| **Ámbito:** A07 — dtic-DNS

Código: A07.P002
Fecha: 07 de abril de 2026
Autor: Lic. Ricardo MONLA
Versión: 1.0
Estado:  COMPLETADO
Dependencia: Ninguna (urgente)

Resumen Ejecutivo

Los correos electrónicos enviados desde cuentas institucionales **@frlr.utn.edu.ar** están siendo rechazados o marcados como spam por **Gmail**. La causa raíz es la **falta de publicación de los registros CNAME de DKIM** en el DNS del dominio.

Solución: Agregar 2 registros CNAME en el DNS de `frlr.utn.edu.ar` y habilitar DKIM en Microsoft 365.

Objetivo

Configurar correctamente los registros DNS de DKIM para el dominio `frlr.utn.edu.ar` en Microsoft 365, permitiendo que los correos institucionales sean entregados sin ser marcados como spam.

Nodos Involucrados

Nodo / Entorno	Descripción de la intervención
srvv-DNS	Servidor DNS local (CoreDNS). Modificación de la zona <code>frlr.utn.edu.ar.db</code> para exponer los registros CNAME y DMARC al público.
Microsoft 365 Admin	Consola Cloud (Tenant). Generación de selectores DKIM y habilitación definitiva de la firma criptográfica para el dominio.



Fases de Implementación



FASE 1: Verificación del Estado Actual

Tareas Iniciales

- ✓ 1.1: Verificar registros DKIM actuales en el DNS
- ✓ 1.2: Verificar estado de DKIM en Microsoft 365 Admin Center
- ✓ 1.3: Documentar configuración SPF actual (dig frlr.utn.edu.ar TXT)
- ✓ 1.4: Registrar evento de inicio en bitácora (#1419) (dig selector1._domainkey.frlr.utn.edu.ar CNAME)

Comandos de diagnóstico:

Verificar registros DKIM actuales

```
dig selector1._domainkey.frlr.utn.edu.ar CNAME
```

```
dig selector2._domainkey.frlr.utn.edu.ar CNAME
```

Verificar SPF

```
dig frlr.utn.edu.ar TXT
```

Verificar DMARC (si existe)

```
dig _dmarc.frlr.utn.edu.ar TXT
```



FASE 2: Agregar Registros CNAME en el DNS - COMPLETADA

Implementación: 2026-04-07 21:52

- ✓ Backup creado: bkp_20260407_215207_preDKIM.frlr.utn.edu.ar.db
- ✓ Registros agregados a /docker/coreDNS/zones/frlr.utn.edu.ar.db en srvv-DNS
- ✓ Serial actualizado: 2025120501 → 2025120502
- ✓ CoreDNS reiniciado

Registros a Crear

Tipo	Nombre (Host)	Valor (Target)
CNAME	selector1._domainkey	selector1-frlr-utn-edu-ar._domainkey.o365frlrutneduar.onmicros
CNAME	selector2._domainkey	selector2-frlr-utn-edu-ar._domainkey.o365frlrutneduar.onmicros

Ubicación: Panel de DNS de la UTN (donde se gestiona frlr.utn.edu.ar)

Notas técnicas: - Algunos paneles agregan el dominio automáticamente. Verificar si el nombre debe ser: - selector1._domainkey (el panel agrega .frlr.utn.edu.ar) - selector1._domainkey.frlr.utn.edu.ar. (FQDN completo) - El registro TXT de

DKIM actual (mail._domainkey) es un DKIM local, NO el de Microsoft 365

✅ FASE 3: Habilitar DKIM en Microsoft 365 - COMPLETADA

Implementación: 2026-04-07 21:55

- ✅ Verificación de registros CNAME: OK
- ✅ DKIM habilitado en Microsoft 365 Admin Center
- ✅ Evento #1419 cerrado en bitácora

Pasos en Microsoft 365 Admin Center

1. Ir a **Microsoft 365 Admin Center** → **Security** → **Policies & rules** → **Threat policies** → **DKIM**
2. Seleccionar el dominio `frrl.utn.edu.ar`
3. Hacer clic en **Enable** o **Sign this domain**
4. Esperar la validación de los registros CNAME (15-30 minutos típicamente)
5. Una vez validado, el interruptor se pondrá en azul (Habilitado)

URLs de referencia: - <https://security.microsoft.com/dkimv2> -
<https://admin.cloud.microsoft/?#/Domains/Details/frrl.utn.edu.ar>

✅ FASE 4: Verificación y Testing - COMPLETADA (con observaciones)

Verificación Post-Configuración

- ✅ **4.1:** Verificar propagación de registros CNAME
 - `selector1._domainkey.frrl.utn.edu.ar` → `selector1-frrl-utn-edu-ar._domainkey.o365frrlutneduar.onmicrosoft.com.` ✓
 - `selector2._domainkey.frrl.utn.edu.ar` → `selector2-frrl-utn-edu-ar._domainkey.o365frrlutneduar.onmicrosoft.com.` ✓
- ✅ **4.2:** Confirmar DKIM habilitado en Microsoft 365
- ✅ **4.3:** Enviar correo de prueba a cuenta Gmail - **Completado**
- ✅ **4.4:** Verificar headers del correo recibido - **Confirmado: dkim=pass y entrega correcta**
- ✅ **4.5:** Cerrar evento en bitácora (#1419 cerrado 21:55)

Estado actual (2026-04-10): - ✅ DKIM configurado y validado en DNS público (`o365frrlutneduar.onmicrosoft.com`) - ✅ SPF configurado correctamente - ✅ **DMARC AGREGADO** - `_dmarc.frrl.utn.edu.ar` reportando (`p=none`) - ✅ Periodo de calentamiento superado. Correos validados sin ser marcados como SPAM.

Triada de autenticación COMPLETA: SPF + DKIM + DMARC

Comandos de verificación:

Verificar propagación CNAME

```
dig selector1._domainkey.frrl.utn.edu.ar CNAME +short
```

```
dig selector2._domainkey.frrl.utn.edu.ar CNAME +short
```

```
# Debería responder:
# selector1-frlr-utn-edu-
  ar._domainkey.o365frlrutneduar.onmicrosoft.com.
# selector2-frlr-utn-edu-
  ar._domainkey.o365frlrutneduar.onmicrosoft.com.
```

Headers a verificar en Gmail:

Authentication-Results: ...
dkim=pass header.i=@frlr.utn.edu.ar ...

Criterios de Éxito

Criterio	Verificación
Registros CNAME publicados	dig responde ambos selectores
DKIM habilitado en M365	Interruptor en azul (Enabled)
Correos sin spam en Gmail	Email de prueba llega a bandeja principal
Headers de autenticación OK	dkim=pass en Authentication-Results

Notas Técnicas

¿Por qué DKIM es importante?

DKIM (DomainKeys Identified Mail) es un mecanismo de autenticación que: 1. **Firma digitalmente** los correos salientes 2. **Verifica** que el correo no fue alterado en tránsito 3. **Demuestra** que el correo proviene del dominio legítimo

Sin DKIM, Gmail y otros proveedores: - Marcan correos como spam - Rechazan la entrega directamente - No pueden verificar la legitimidad del remitente

Diferencia entre SPF, DKIM y DMARC

Mecanismo	Función	Registro DNS
SPF	Lista de servidores autorizados a enviar	TXT (v=spf1 ...)
DKIM	Firma digital del correo	CNAME (selectores) + TXT (clave pública)
DMARC	Política de qué hacer si falla SPF/DKIM	TXT (_dmarc, v=DMARC1 ...)

Configuración Actual (para referencia)

SPF actual:

```
frrlr.utn.edu.ar. IN TXT "v=spf1 mx ip4:190.114.205.2
include:spf.protection.outlook.com -all"
```

DKIM local (no usado por M365):

```
mail._domainkey.frrlr.utn.edu.ar. IN TXT "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOMtst0Un3kUnMr+azAfJ1zho2..."
```

Tiempo de Propagación

- **Estimado oficial:** 4 días (Microsoft)
- **Típico real:** 15-30 minutos
- **Recomendación:** Intentar habilitar DKIM después de 30 minutos, si falla esperar 24h



Armonía Integral

Documento	Estado	Notas
A07_dtic-DNS.md	✓ Actualizado	Ámbito operativo
A07.P001_Deteccion-Conexion-DNS.md	✓ Completado	Plan anterior
A07.P002_Resolver-DKIM-Gmail.md	✓ Completado	Este plan
docs/contexto/IA.md	⌚ Pendiente	Actualizar post-resolución

Referencias

- **Microsoft DKIM Guide:** <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/use-dkim-to-validate-outbound-email>
- **DKIM Validator:** <https://dkimvalidator.com/>
- **MX Toolbox:** <https://mxtoolbox.com/dkim.aspx>
- **Bitácoras:** `./adn/tools/run db evento:listar --ambito dtic-DNS`