Protección del Correo Empresarial contra Phishing y Spam en Codearts Solutions

🔹 Fase 1: Implementación de medidas de seguridad en el servidor de correo

```
# SPF (registro DNS)
"v=spf1 ip4:TU.IP.PUBLICA -all"

# DKIM (OpenDKIM)
sudo apt install opendkim opendkim-tools
opendkim-genkey -s mail -d empresa.com
cat mail.txt  # copiar a DNS

# DMARC (registro DNS)
"v=DMARC1; p=quarantine; rua=mailto:seguridad@empresa.com"

# SpamAssassin
sudo apt install spamassassin
sudo systemctl enable --now spamassassin
```

🔹 Fase 2: Simulación y detección de ataques de phishing

```
# GoPhish (simulación)
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
unzip gophish*.zip && cd gophish
./gophish
```

🔹 Fase 3: Configuración de seguridad en clientes de correo

2FA (interfaz web)

Gmail: https://myaccount.google.com/security

Outlook: Seguridad > Verificación en dos pasos

Filtros: Configurados desde la interfaz (Outlook, Gmail, Thunderbird)

🔹 Fase 4: Implementación de políticas de seguridad y monitoreo

Listas negras en SpamAssassin

echo "blacklist_from *@phish.com" >> /etc/spamassassin/local.cf

Activar DMARC Analyzer (web):

https://dmarcian.com / https://dmarc.postmarkapp.com