Protección del Correo Empresarial contra Phishing y Spam en Codearts Solutions

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

- **SPF configurado** en el registro DNS para permitir solo a los servidores autorizados enviar correos con el dominio de la empresa.
- **DKIM habilitado**, generando claves pública y privada para firmar los correos salientes.
- **DMARC activo** con política quarantine y generación de reportes.
- **SpamAssassin instalado** como filtro antispam, configurado con políticas adaptadas a la organización.
- **Habilitados logs y alertas** en el servidor Postfix para detectar intentos de spoofing o envío masivo anómalo.

Errores comunes:

Error	Causa probable	Solución
SPF fallido	Registro mal formado	Verificar sintaxis: v=spf1 ip4:x.x.x.x -all
DKIM sin firmar	Claves mal ubicadas o permisos incorrectos	Revisar /etc/opendkim/, asegurar que postfix tenga acceso
DMARC sin reportes	Falta de rua o ruf	Asegurar que los campos de email de reporte estén presentes

🔹 Fase 2: Simulación y detección de ataques de phishing

- Se diseñó un **correo falso de phishing** imitando un aviso bancario con enlace malicioso.
- Se envió a **10 empleados** para medir su respuesta.
- Se utilizó un **servidor de pruebas** para redirigir los clics a una página de captura sin comprometer datos reales.
- Se generó un **informe anónimo** con tasas de clics y errores cometidos.

Errores comunes:

Error	Causa	Solución
El correo se va a SPAM	Falta de autenticación DKIM o SPF	Revisar encabezados y reputación del dominio
No se registran los clics	URL mal configurada o redirección bloqueada	Revisar reglas de firewall y configuración del servidor de phishing

🔹 Fase 3: Configuración de seguridad en clientes de correo

- Activada la **autenticación 2FA** en cuentas corporativas de Gmail y Office 365.
- Configurados filtros antiphishing en **Outlook**, **Thunderbird** y **Gmail**.
- Distribuida **guía visual** con ejemplos de phishing, encabezados falsos, URLs sospechosas, y remitentes maliciosos.

Errores comunes:

Error	Causa	Solución
Outlook no aplica filtro	Reglas mal ordenadas o sin aplicar	Reorganizar reglas, activar opción de ejecución automática
Fallos en 2FA	Usuario no configuró app	Habilitar Google Authenticator o Microsoft Authenticator correctamente

🔹 Fase 4: Implementación de políticas de seguridad y monitoreo

- Añadidas **listas negras** personalizadas en el servidor antispam.
- Activado análisis automático de **enlaces y adjuntos** sospechosos.
- Se configuró **DMARC Analyzer** para generar informes diarios y estadísticas de fallos de autenticación.

Errores comunes:

Error	Causa	Solución
DMARC Analyzer no muestra datos	Falta de envío de reportes por DNS	Verificar rua=mailto:seguridad@empresa.com
Archivos adjuntos peligrosos pasan	Umbral de SpamScore bajo	Ajustar puntuación de detección en SpamAssassin