

Mecanismos para evitar SPAM

Oficina de Informática y Desarrollo Tecnológico
Bogotá DC

Fecha (2026-06-26)

CONTENIDO

	Página.
1. INTRODUCCIÓN	3
2. ALCANCE.....	3
3. DESCRIPCIÓN METODOLÓGICA	3
4. RESULTADOS.....	4
5. CONCLUSIONES	12
6. ANEXOS.....	12

1. INTRODUCCIÓN

El presente informe técnico tiene como propósito estructurar, documentar y validar las estrategias implementadas por Instituto Nacional de Metrología para robustecer la seguridad del canal de comunicación oficial por correo electrónico. Específicamente, se enfoca en el desarrollo y despliegue de mecanismos avanzados de control destinados a mitigar la recepción e impacto de correos electrónicos masivos, automatizados o maliciosos, comúnmente categorizados como correo no deseado (SPAM).

En el entorno operativo actual, el correo electrónico representa el vector de comunicación primario con la ciudadanía y otras instituciones, pero al mismo tiempo constituye la principal superficie de ataque para amenazas de ciberseguridad como el phishing, el malware y la saturación de infraestructura. Garantizar la disponibilidad, integridad y confidencialidad de este servicio mediante políticas estrictas de filtrado no solo protege los activos de información de la entidad, sino que asegura el cumplimiento de las directivas de Gobierno Digital y las normativas vigentes en materia de seguridad de la información.

2. ALCANCE

El alcance de este documento y de los mecanismos evaluados abarca la totalidad de la infraestructura de correo electrónico institucional (tanto para el flujo de mensajes entrantes como salientes) administrada por la Oficina de Informática y Desarrollo Tecnológico.

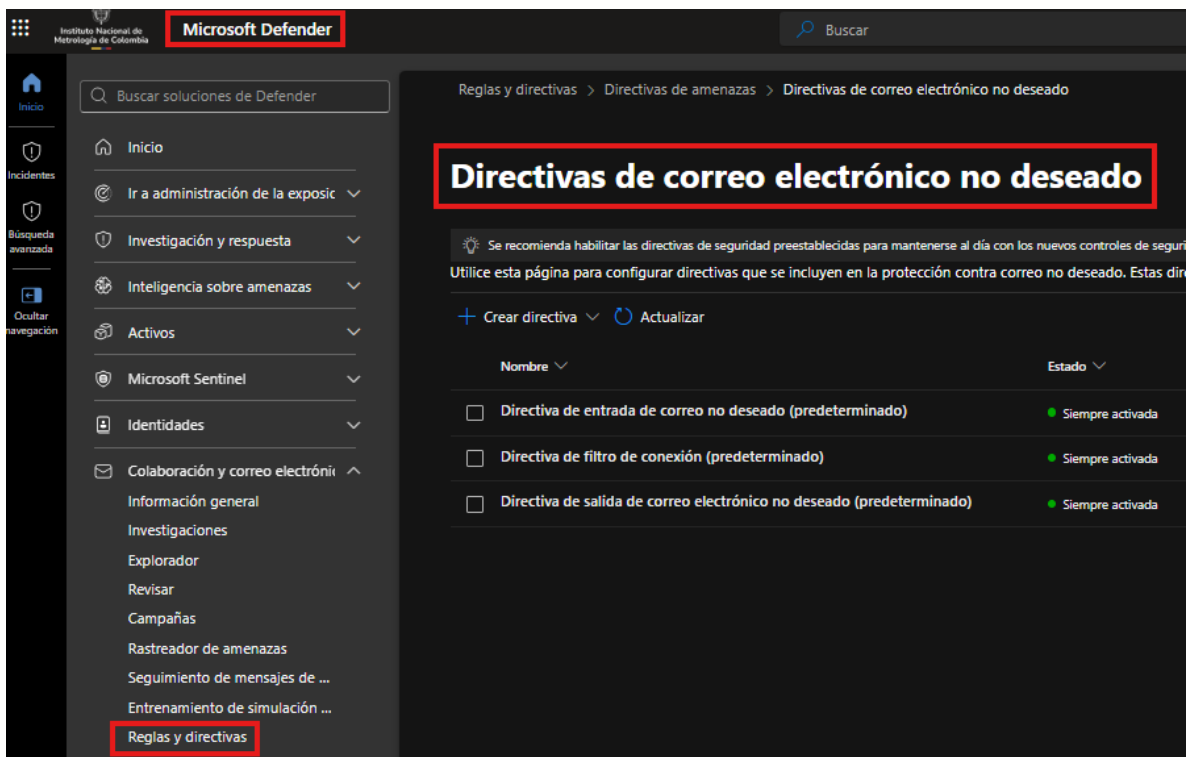
3. DESCRIPCIÓN METODOLÓGICA

Para el desarrollo y la ejecución de los mecanismos destinados a evitar la recepción de correos automatizados no deseados, se adoptó un enfoque metodológico basado en las siguientes fases operativas:

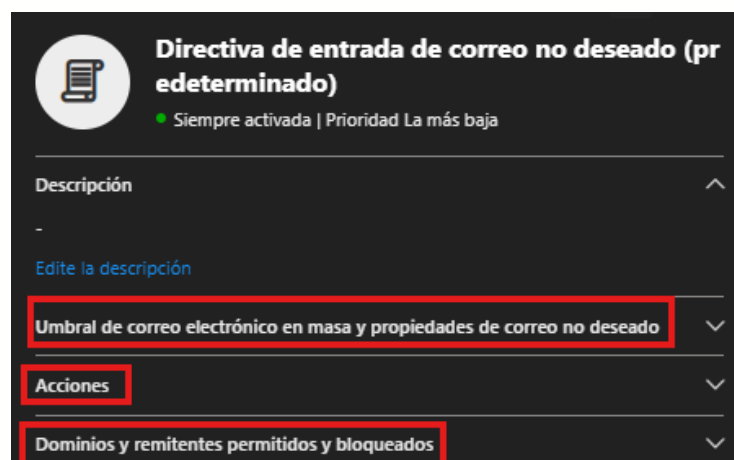
- ❖ Políticas Anti-Spam
- ❖ Políticas Anti-Phishing
- ❖ Safe Links
- ❖ Configuración SPF, DKIM y DMARC
- ❖ Reportes de amenazas bloqueadas
- ❖ Cuarentena de correo
- ❖ Configuración de autenticación

4. RESULTADOS

- Se realiza la revisión de las políticas Anti-Spam en el portal de Microsoft Defender.



Al evaluar la directiva de entrada del correo no deseado se determinan los siguientes parámetros:



- ❖ Umbral de correo electrónico en masa y propiedades de correo no deseado.
- ❖ Acciones por implementar.
- ❖ Dominios y remitentes permitidos y bloqueados.

**Directiva de entrada de correo no deseado
(predeterminado)**
● Siempre activada | Prioridad La más baja
[Edite la descripción](#)

Umbral de correo electrónico en masa y propiedades de correo no deseado

Acciones

Acción de mensaje de correo electrónico no deseado
Mover el mensaje a la carpeta Correo electrónico no deseado

Acción de mensaje de correo no deseado de confianza alta
Mover el mensaje a la carpeta Correo electrónico no deseado

Acción de mensaje de phishing
Mover el mensaje a la carpeta Correo electrónico no deseado

Acción de mensaje de phishing de confianza alta
Mensaje en cuarentena

Aplicar la siguiente directiva de cuarentena:
AdminOnlyAccessPolicy

Acción de mensaje en masa
Mover el mensaje a la carpeta Correo electrónico no deseado

Mensajes dentro de la organización sobre los que tomar medidas
Predeterminado

Habilitar sugerencias de seguridad para el spam
● Activado

Habilitar para mensajes de correo no deseado
● Activado

Habilitar para mensajes de suplantación de identidad (phishing)
● Activado

Conservar el spam en cuarentena durante esta cantidad de días
15

Al evaluar la directiva de salida del correo no deseado se determina el parámetro de configuración de protección:

**Directiva de salida de correo electrónico no deseado (predeterminado)**
● Siempre activada | Prioridad La más baja

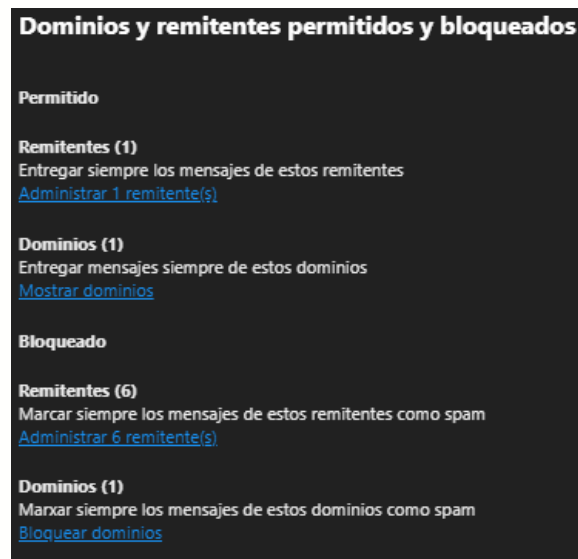
Descripción 

-

[Edite la descripción](#)

Configuración de protección 

- Se realiza la revisión de las políticas en Microsoft Defender validando los usuarios y dominios permitidos, así como los bloqueados.



- Se realiza revisión de la directiva de filtro de conexión para enlaces seguros (Safe Links).



- Configuración de SPF (Sender Policy Framework)

Definición del registro SPF que especifica los servidores autorizados para enviar correos en nombre del dominio inm.gov.co.

inm.gov.co

Administrador en Azure - Dominio predeterminado

 Quitar dominio  Actualizar

Información general **Registros de DNS** Usuarios Teams y grupos Aplicaciones

Para administrar registros de DNS para inm.gov.co, vaya a su proveedor de host DNS: [Azure](#).

Agregue los registros DNS en el registrador de dominios o proveedor de host DNS para conectar sus servicios a su dominio. Seleccione un registro para ver todos los detalles y copie y pegue los valores esperados en el registrador. [Más información sobre DNS y los tipos de registro](#).

 Comprobar estado  Administrar DNS  Descargar archivo .csv  Descargar archivo de zona  Imprimir

Microsoft Exchange

Tipo	Estado	Nombre	Valor	TTL
☐ MX	 Aceptar	@	inm-gov-co.mail.protection.outlook.com	1 hora
☐ TXT	 Aceptar	@	v=spf1 include:spf.protection.outlook.com -all	1 hora
☐ CNAME	 Aceptar	autodiscover	autodiscover.outlook.com	1 hora

Publicación en DNS: Se añade el registro SPF al sistema de nombres de dominio (DNS) del dominio inm.gov.co.

 inm.gov.co

 Usuarios

Nombre

@inm.gov.co

Tipo

TXT

TTL *

1

Unidad de TTL

Horas

Valor

MS=ms69815736

google-site-verification=76lzrevtf3kECdjZhtGdtPn30cXQ0t6pF9mW78ANS4

v=spf1 include:spf.protection.outlook.com -all

Verificación: Se utilizan herramientas de validación de SPF para asegurar que el registro está configurado correctamente y es funcional.

SuperTool Beta7

inm.gov.co

SPF Record Lookup

spf:inm.gov.co

Find Problems

Solve Email Delivery Problems

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

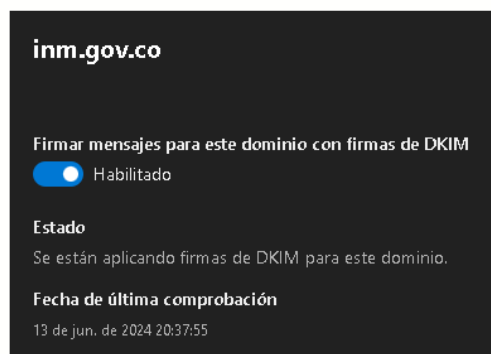
```
v=spf1 include:spf.protection.outlook.com -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

	Test	Result
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found
✓	SPF Void Lookups	Number of void lookups is OK
✓	SPF MX Resource Records	Number of MX Resource Records is OK
✓	SPF Record Null Value	No Null DNS Lookups found

❖ Configurar de DKIM (DomainKeys Identified Mail)

Activación de DKIM en Office 365: Habilitar DKIM en la configuración de Office 365 para el dominio inm.gov.co.



Generación de Claves DKIM: Se generan las claves públicas y privadas DKIM necesarias para firma digital de los correos electrónicos.

Publicación de Claves en DNS: Se publica la clave pública DKIM en el DNS del dominio inm.gov.co.

inm.gov.co | Registros ☆ ...
Zona DNS

Buscar « + Agregar Actualizar Eliminar

Información general
Registro de actividad
Control de acceso (IAM)
Etiquetas
Diagnosticar y solucionar problemas
Configuración
Propiedades
Bloqueos

Un conjunto de registros es una colección de registros de una zona que tienen el mismo nombre y son del mismo tipo. Puede buscar conjuntos de registros cargados en esta página. Si no ve lo que busca, puede intentar desplazarse para permitir que se carguen más conjuntos de registros. [Más información](#)

Buscar

Se capturaron 36 conjuntos de registros.

selector1_domainkey	CNAME	3600	selector1-inm-gov-co_domainkey.metrologiainm.onmicrosoft.com
selector2_domainkey	CNAME	3600	selector2-inm-gov-co_domainkey.metrologiainm.onmicrosoft.com

Verificación: Se hacen pruebas de envíos de correos de prueba para verificar que están siendo firmados correctamente mediante herramientas de verificación de DKIM.

```
ARC-Authentication-Results: i=2; mx.google.com;
dkim=pass header.i=@inm.gov.co header.s=selector1 header.b=Oh7ymo1E;
arc=pass (i=1 spf=pass spfdomain=inm.gov.co dkim=pass dkdomain=inm.gov.co dmarc=pass fromdomain=inm.gov.co);
spf=pass (google.com: domain of jatorres@inm.gov.co designates 2a01:111:f403:200a::72f as permitted sender) smtp.mailfrom=jatorres@inm.gov.co;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=inm.gov.co
Return-Path: <jatorres@inm.gov.co>
Received: from NAM12-MW2-obe.outbound.protection.outlook.com (mail-mw2nam12on2072f.outbound.protection.outlook.com. [2a01:111:f403:200a::72f])
by mx.google.com with ESMTPS id ca18e2360f4ac-7ebdbad65d2si178730439f.86.2024.06.13.20.01.54
for <ingjhontorres@gmail.com>
(version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
Thu, 13 Jun 2024 20:01:54 -0700 (PDT)
```

Dominio

inm.gov.co

Por favor, introduzca un nombre de dominio válido, sin el prefijo http://

Selector

auto

Introduzca los selectores de registro DKIM

Selector de detección automática  

Buscar en

Estado de DKIM

selector: **selector1**

✓ This record has been correctly setup

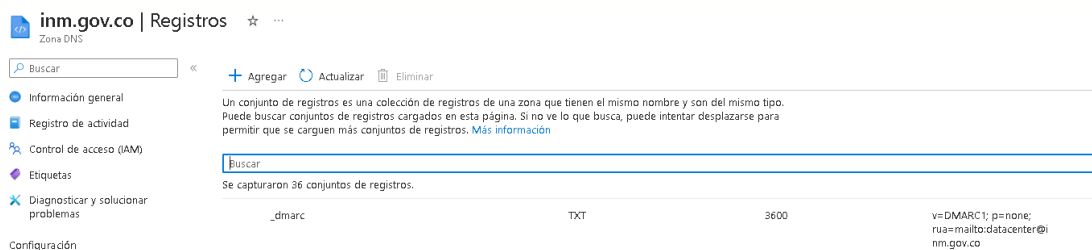
```
v=DKIM1; k=rsa;
p=MIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArXRSyB4yLjVVOF1CMeeAT1yX/G3xACNeyU31BID8FL+8rDZgchi
PwBCmVeB7d2NTyLK/5Cph9YcajSW+oM9AjAZKJNsAK+xKn0GoIQIKI5g+9LKlvoa4WploixwnTW99RF1+U/1YoHtw3DEzqC/3K6
PE+WTm87sCBVtNYN6Gq0zRTbXJYZvka0yIFnwbfS1Lsm7GjahSbmra9TGdd1f8r4LmoNOuTT9S3lsom72DE/Qo395Vw9zaMT
m102yHlGmZ1nF8kScQnnouSTdnXB7n4m7wppnC Md16iHf5YlXb0iJfnYW7L sW5kftYnvc3aAGoDDh0kcpnosKQmIDAOAR;
```

❖ **Configuración de DMARC (Domain-based Message Authentication, Reporting & Conformance)**

Creación del Registro DMARC: Se definen las políticas de DMARC que especifiquen cómo deben manejarse los correos electrónicos que no pasen las verificaciones de SPF y DKIM.

v=DMARC1; p=none; rua=mailto:datacenter@inm.gov.co. Se define el comportamiento de bloqueo para los orígenes (dominios externos) hacia inm.gov.co como NONE=Ninguno, para iniciar con el monitoreo de los buzones sospechosos, sin embargo, se enviarán reportes periódicos al buzón datacenter@inm.gov.co (administrado por la OIDT) para estudio. Posteriormente se definirá si es conveniente iniciar con rechazo de correos que no pasen la comprobación de seguridad.

Publicación en DNS: Añadir el registro DMARC al DNS del dominio inm.gov.co

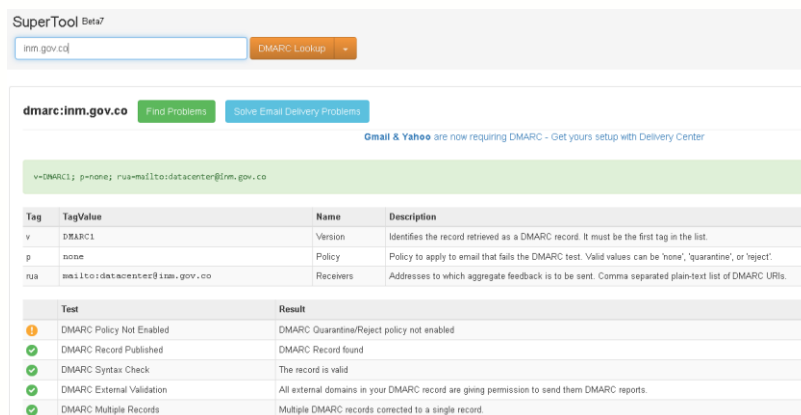


The screenshot shows the 'Registros' (Records) section of the inm.gov.co DNS management interface. A search bar is at the top. On the left, there are navigation links: 'Información general', 'Registro de actividad', 'Control de acceso (IAM)', 'Etiquetas', and 'Diagnosticar y solucionar problemas'. The main area displays a table of DNS records. One record is shown with the following details:

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'.
rua	mailto:datacenter@inm.gov.co	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

Configuración de Reportes: Se establecen direcciones de correo para recibir informes de DMARC sobre intentos de suplantación y otros incidentes.

rua=mailto:datacenter@inm.gov.co



The screenshot shows the 'SuperTool DMARC Lookup' interface. At the top, there is a search bar with 'inm.gov.co' entered and a 'DMARC Lookup' button. Below the search bar, there are links for 'Find Problems' and 'Solve Email Delivery Problems'. A message states: 'Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center'. The main area displays the DMARC record configuration for inm.gov.co:

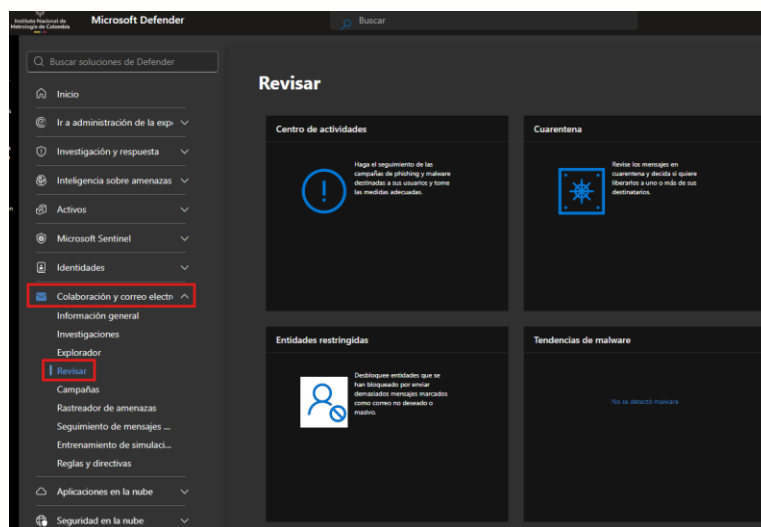
v=DMARC1; p=none; rua=mailto:datacenter@inm.gov.co

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'.
rua	mailto:datacenter@inm.gov.co	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.

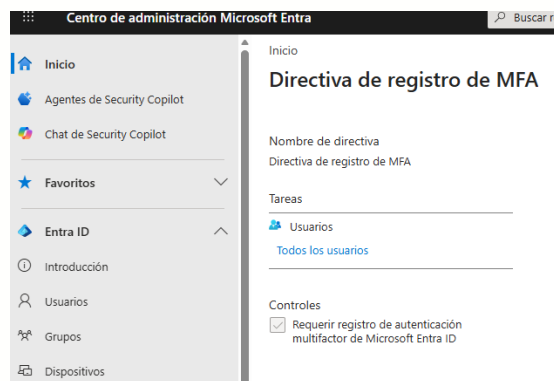
Test	Result
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled
DMARC Record Published	DMARC Record found
DMARC Syntax Check	The record is valid
DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
DMARC Multiple Records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

Al haber realizado esta implementación con éxito de los estándares de seguridad DKIM, DMARC y SPF en Office 365 para el dominio inm.gov.co. Estos protocolos están activos y configurados correctamente.

- Se realiza la revisión de reportes de amenazas en Microsoft Defender, incluyendo:
 - Centro de actividades (seguimiento de campañas de phishing y malware).
 - Mensajes en Cuarentena.
 - Entidades Restringidas
 - Tendencias de malware.



- Se realiza revisión desde el centro de administración de Microsoft 365 la configuración del doble factor de autenticación (MFA).



5. CONCLUSIONES

- ❖ La implementación de los estándares de seguridad DKIM, DMARC y SPF en Office 365 para el dominio inm.gov.co se llevó a cabo para fortalecer significativamente la seguridad del correo electrónico del INM. Estos protocolos mejoraran la autenticidad y la integridad de las comunicaciones, reduciendo el riesgo de suplantación de identidad y ataques de phishing.
- ❖ Con la correcta configuración y activación de estos métodos de seguridad se asegura que los correos electrónicos enviados y recibidos por el dominio inm.gov.co son legítimos y de confianza para los destinatarios.
- ❖ El Tenant de Microsoft cuenta con controles preventivos y correctivos para la protección del correo electrónico institucional.

6. ANEXOS

NA.

Firma de la persona que elaboró

Firma de la persona que aprobó

Elaboró:

Juan Camilo Trujillo Soto
Profesional Universitario
Oficina de Informática y Desarrollo Tecnológico

Aprobó:

Jhon Alexander Torres Galindo
Profesional Especializado
Oficina de Informática y Desarrollo Tecnológico