OOSAPAT
ORGANISMO OPERADOR DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO DEL MUNICIPIO DE TEHUACÁN, PUEBLA.
Desarrollo y futuro

Avances en el Plan Maestro de Ciberseguridad

15 de Octubre de 2024

Prolongación Independencia Oriente no. 503,
San Diego Chalma, Tehuacán, Puebla.

238 382 50 00 y 38 245 72

www.oosapat.gob.mx
f: oosapat

Gobierno de Tehuacán
Desarrollo y futuro >
2021 - 2024

Organismo Operador de los Servicios de Agua Potable y Alcantarillado de Tehuacán, Pue.

Servicios públicos y Gubernamentales

OSAPAT

ORGANISMO OPERADOR DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO DEL MUNICIPIO DE TEHUACÁN, PUEBLA.

Desarrollo y futuro

Prolongación Independencia Oriente No.503

San Diego Chalma, Tehuacán, Puebla.

Problematic

The Organismo Operador de los Servicios de Agua Potable y Alcantarillado de Tehuacán (OOSAPAT), as a government entity providing public services, faces increasing exposure to cyber threats that could compromise the availability, integrity, and confidentiality of its information systems. The absence of a structured and up-to-date cybersecurity master plan has left the technological infrastructure vulnerable to attacks, such as ransomware, phishing, and other forms of cyberattacks that could disrupt critical services and impact the community.

Management Organization Chart

Leilani Naomi Robles Cavanzo

Team Lider

Supervisor of project activities, assignment of tasks, ensuring that the plan will adapt to the needs of OOSAPAT

Pedro Eduardo Moro Cruz

Incident Response Specialist

Identify the level of maturity of the organization in order to be able to carry out the cybersecurity plan

German Jesus Caballero Molina

Security Analyst

In charge of analyzing the networks that form the organization to create the topology of the network.

Rodrigo Jesus Hernandez Rosales

Cybersecurity Researcher

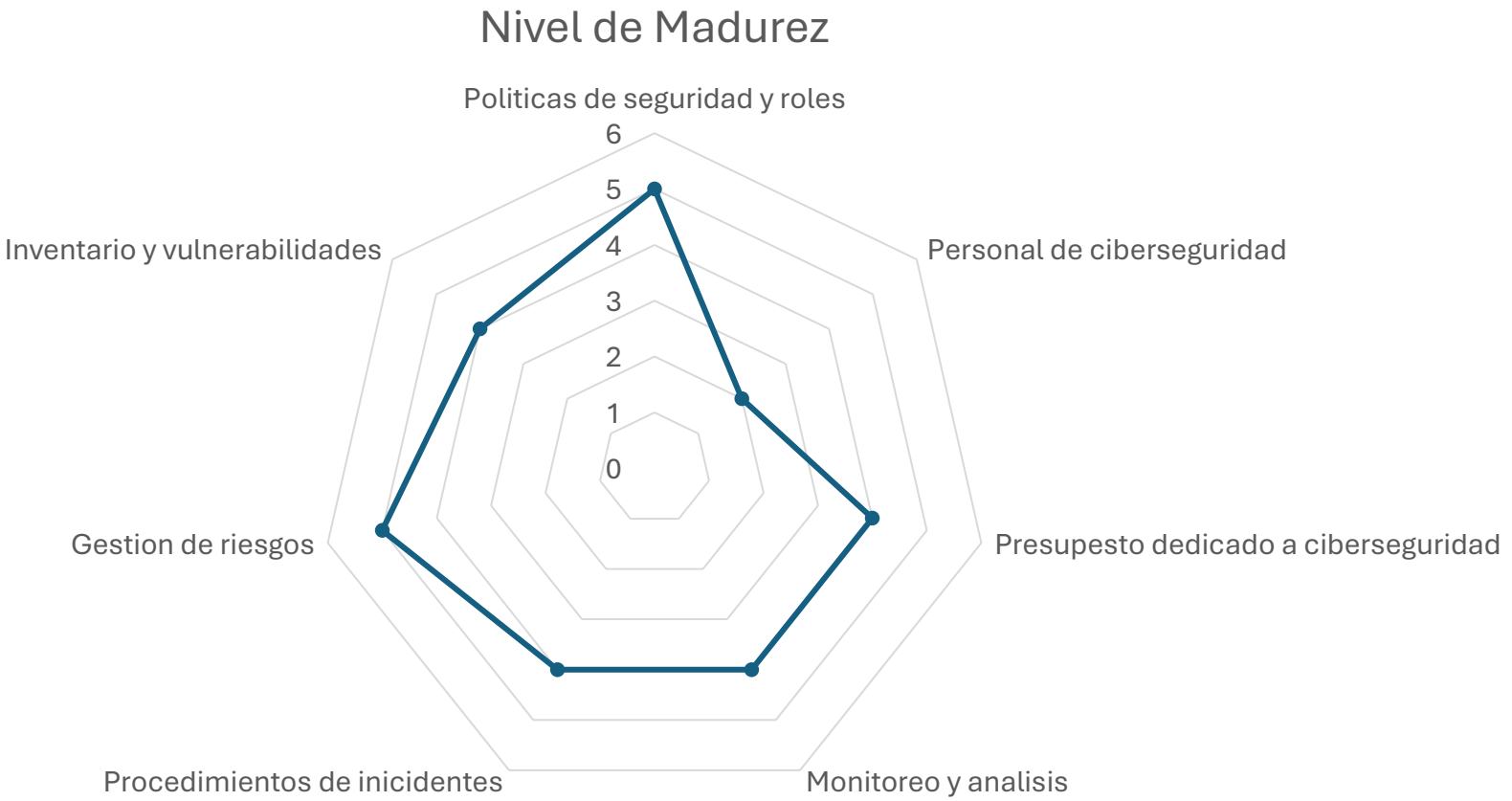
Investigate threats and vulnerabilities to assess organizational risks

Análisis de Situación

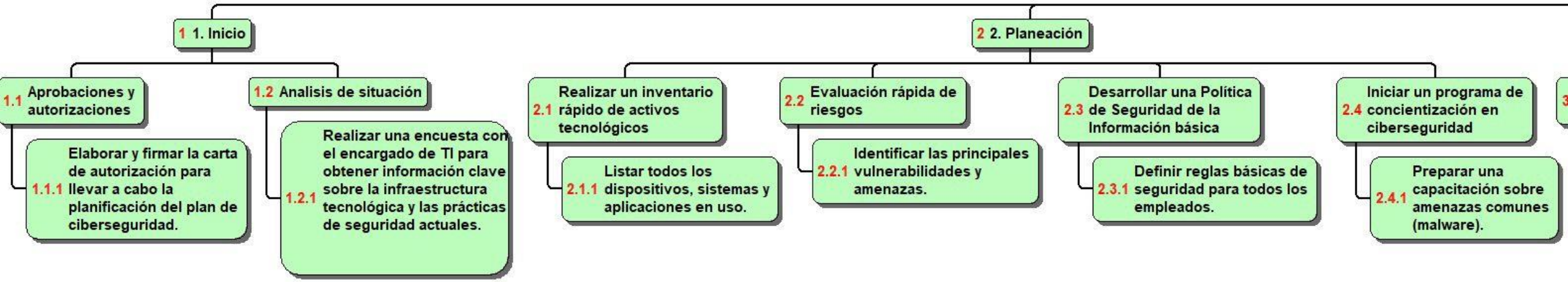
Sistema CMMI (Capability Maturuty Model Integration) basado en 5 niveles:

1. Inicial (Ad-hoc): La ciberseguridad se maneja de manera reactiva sin procesos definidos.
2. Repetible: Existen procesos básicos, pero no son formalizados ni revisados regularmente.
3. Definido: La organización tiene políticas y procedimientos formales para ciberseguridad.
4. Gestionado: Se mide el rendimiento de los procesos de ciberseguridad y se gestionan con métricas claras.
5. Optimizado: La organización mejora continuamente sus procesos de ciberseguridad con un enfoque proactivo.

Análisis del grado de madurez en Ciberseguridad de OOSAPAT



Realización de WBS



Inventarios de Activos Tecnológicos

Software libre

OOSAPAT
ORGANISMO OPERADOR DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO DEL MUNICIPIO DE TEHUACÁN, PUEBLA.
Desarrollo y futuro

Nombre del Sistema/Aplicación	Descripción
Sistema de Almacén	Software para gestionar inventarios y operaciones diarias.
Aplicación OOSAPAT	App móvil para pagos de servicios en Android (software libre) e iOS (licencia adquirida).
Sistema de Obra Pública	Gestión de materiales y productos en obras públicas.
Sistema de Evidencia Fotográfica	Agregar fotos de trabajos antes, durante y después, exportando reportes en PDF.
Servidor Web Services	Enlace entre la app de pagos y el sistema SIAC.
Servidor de Telefonía IP	Sistema para enlazar llamadas telefónicas internas y externas.
Sistema de Indicadores	Medición de ingresos, contratos y eficiencia de departamentos.
Sistema de Pagos	Monitorea pagos realizados en la aplicación y cajeros automáticos.
TrueNAS	Sistema operativo para almacenamiento en red.
Nextcloud	Servidor de almacenamiento en la nube
Kali	Sistema operativo para auditorios de seguridad y análisis forense

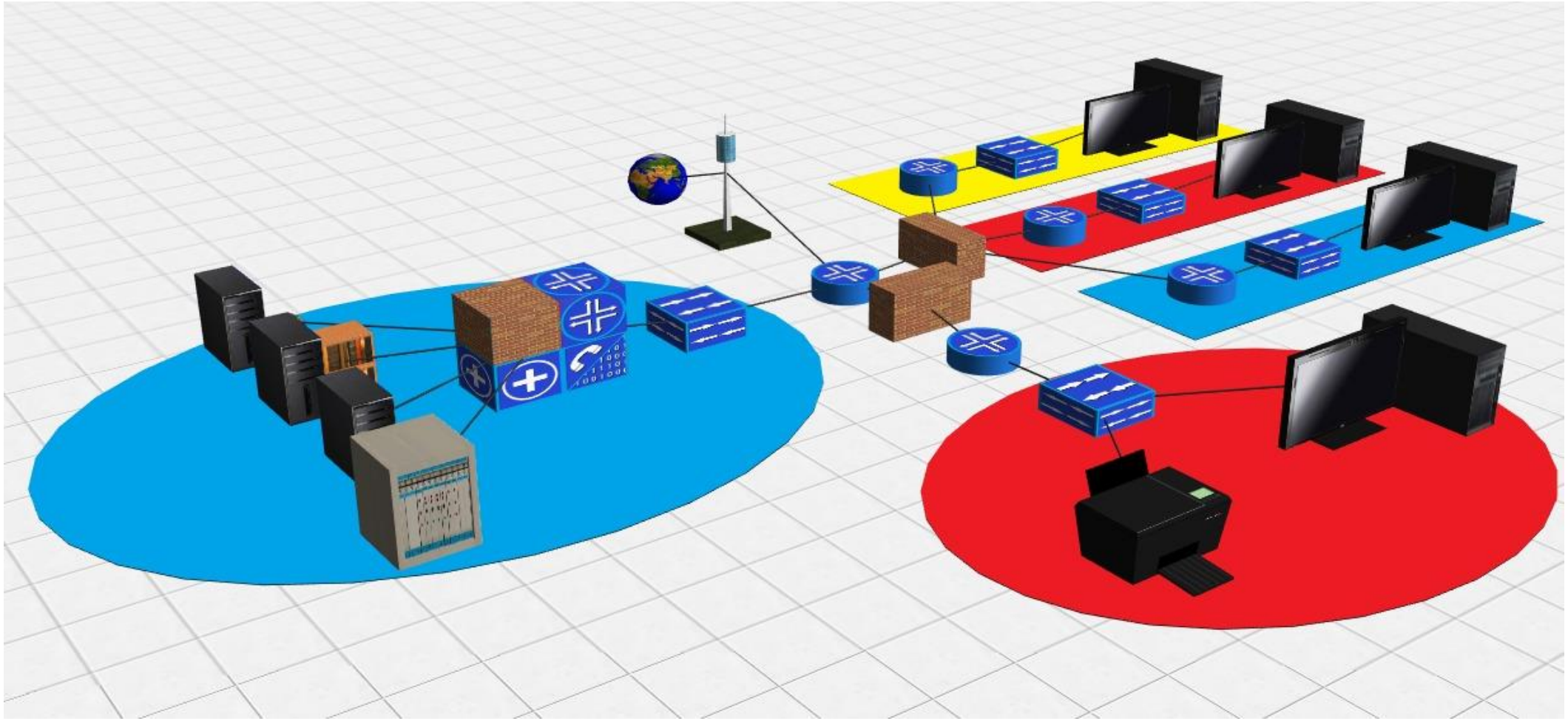
Inventarios de Activos Tecnológicos

Licencia adquirida

OOSAPAT
ORGANISMO OPERADOR DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO DEL MUNICIPIO DE TEHUACÁN, PUEBLA.
Desarrollo y futuro

Nombre del Sistema/Aplicación	Descripción
Servidor de Seguridad Perimetral	Software para gestionar inventarios y operaciones diarias.
Sistema de Cajeros Automáticos	App móvil para pagos de servicios en Android (software libre) e iOS (licencia adquirida).
Sistema Contable NSARC II	Gestión de materiales y productos en obras públicas.
SIAC	Agregar fotos de trabajos antes, durante y después, exportando reportes en PDF.
CONTPAQI Nominas	Enlace entre la app de pagos y el sistema SIAC.
Kaspersky Small Office	Sistema para enlazar llamadas telefónicas internas y externas.
Crystal Reports XI	Medición de ingresos, contratos y eficiencia de departamentos.
CONTPAQI Facturación-E	Monitorea pagos realizados en la aplicación y cajeros automáticos.

Topología de Red



Evaluación de Riesgos

OSAPAT
ORGANISMO OPERADOR DE LOS SERVICIOS DE AGUA POTABLE Y ALCANTARILLADO DEL MUNICIPIO DE TEHUACÁN, PUEBLA.
Desarrollo y futuro

Amenazas y Vulnerabilidades	Descripción	Acción de Mitigación
Ataques de ransomware	Malware que cifra los datos y solicita un rescate para restablecer el acceso a la información.	Implementar autenticación multifactor, actualizar el software y realizar copias de seguridad más frecuentes.
Phishing	Correos electrónicos o mensajes fraudulentos que buscan engañar a los empleados para obtener credenciales.	Realizar campañas de concientización sobre phishing y mejorar los filtros de correo electrónico.
Falta de capacitación del personal	El personal no cuenta con el conocimiento suficiente para identificar amenazas o actuar ante incidentes.	Programar capacitaciones regulares en ciberseguridad y protocolos de respuesta ante incidentes.
Exposición de información sensible	Divulgación accidental o no autorizada de datos confidenciales.	Fortalecer el monitoreo de acceso a datos sensibles y aplicar cifrado avanzado en toda la información crítica.

Políticas de Seguridad Básica

POLITICAS DE CUENTAS

Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.

1. Sean trabajadores vigentes del Organismo.
2. Tengan la autorización del jefe del área.
3. Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.
4. La asignación de cuentas la hará el administrador del servidor del área en cuestión y al usuario
5. El administrador podrá deshabilitar las cuentas que no sean vigentes.
6. La cuenta y contraseña personales son intransferibles.

Políticas de Seguridad Básica

POLÍTICAS DE CONTROL DE ACCESO

Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

1. Todos los administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
2. Todos los usuarios deberán autentificarse con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.
3. Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
4. Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
5. Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta, hacer la conexión a la computadora deseada.

Políticas de Seguridad Básica

POLÍTICAS DE CONTRASEÑAS

1. El administrador del servidor será el responsable de asignar las contraseñas.
2. El administrador deberá contar con herramientas de detección de contraseña débiles
3. La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador/usuario. Todas las contraseñas deberán contar con al menos 16 caracteres.
4. Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
5. Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
6. No se podrán informar contraseñas por vía telefónica.
7. La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.

Programa de concientización

El programa se enfocará en la entrega de conocimientos prácticos mediante presentaciones, actividades interactivas, estudios de casos, y simulaciones para fortalecer la comprensión y aplicación de las mejores prácticas de ciberseguridad.

Resultados Esperados

1. Mejora del conocimiento general sobre ciberseguridad
2. Reducción de incidentes por errores humanos
3. Fortalecimiento de la cultura de ciberseguridad en la empresa

Plan de Capacitación

Objetivos

1. Capacitar a los empleados sobre las mejores prácticas de ciberseguridad.
2. Informar sobre las amenazas más comunes, con un enfoque específico en Malware.
3. Proporcionar procedimientos básicos para la respuesta a incidentes de seguridad.
4. Promover una cultura de ciberseguridad en la empresa.

Agenda del Programa de Capacitación

1. Sesión 1 – Introducción a la ciberseguridad
2. Sesión 2 – Malware (Tipos y Prevención)
3. Sesión 3 – Buenas prácticas de seguridad en la red
4. Sesión 4 – Respuesta a incidentes de seguridad

Controles de Acceso

Políticas de contraseñas robustas

- Pasos para Implementar la Política de Contraseñas Robusta

  Definición de Requisitos de Contraseña

1. Longitud mínima:12 caracteres.
2. Complejidad: Incluir mayúsculas, minúsculas, números y caracteres especiales.
3. No reutilización: Prohibir el uso de contraseñas anteriores.
4. Expiración: Cambios obligatorios cada 90 días.
5. Bloqueo de cuenta: Después de 5 intentos fallidos.

Controles de Acceso

Autenticación de Dos Factores

Pasos para Implementar la Autenticación de Dos Factores

Selección del Método de 2FA

Tipos comunes:

- Aplicaciones de autenticación: Google Authenticator, Microsoft Authenticator.
- Mensajes SMS: Envío de códigos vía SMS.
- Tokens de hardware: Dispositivos físicos como YubiKey.
- Correo electrónico: Envío de códigos a correo corporativo.