MASTER OSINT REPORT -- Mexican .git Exposure Campaign

Date: 2026-02-20

Analyst Notes: Three Mexican domains found with exposed `.git/` directories on production webservers. All three were dumped using git-dumper via Python 3.13. Full file extraction completed on uaem.mx (11,605 files, including hardcoded database and email credentials).

Executive Summary

Three exposed `.git/` directories were identified and extracted from Mexican websites spanning private media, state law enforcement, and public education. Combined findings reveal systemic security failures: manual root-level git deployments, absent security tooling, leaked internal infrastructure details, exposed developer identities, **hardcoded production database credentials**, and **SMTP email credentials** -- all recovered directly from source code.

#	Domain	Sector	Data Recovered	Size	Key Finding
1	mvs.com	Private media..	Full source code (c..	13 MB	Bitbucket workspace mvsradio, employee + contractor PII
2	fiscalia.duran..	State prosecu..	Git metadata only (..	669 KB	Internal Git server IP 10.1.4.194:8085, 24-agency pla..
3	uaem.mx	Public univer..	11,605 files extrac..	960 MB	Hardcoded MySQL + SMTP credentials, payroll data, sta..

Local File Locations

Target	Local Path
MVS Report	C:\Users\Squir\Desktop\MEXICO\V A U L T\OSINT Reports\01-MVS-COM.md
MVS Raw Data	C:\Users\Squir\Desktop\MEXICO\V A U L T\mvs.com\
Fiscalia Report	C:\Users\Squir\Desktop\MEXICO\V A U L T\OSINT Reports\02-FISCALIA-DURANGO.md
Fiscalia Raw Data	C:\Users\Squir\Desktop\MEXICO\V A U L T\fiscalia.durango.gob.mx\
UAEM Report	C:\Users\Squir\Desktop\MEXICO\V A U L T\OSINT Reports\03-UAEM-MX.md
UAEM Raw Data	C:\Users\Squir\Desktop\MEXICO\V A U L T\uaem.mx\
Credentials Master	C:\Users\Squir\Desktop\MEXICO\V A U L T\OSINT Reports\04-CREDENTIALS.md
This Report	C:\Users\Squir\Desktop\MEXICO\V A U L T\OSINT Reports\00-MASTER-REPORT.md

Personnel Identified (All Targets)

Name	Email	Organization	Platform	Role
Alfredo Gonzalez	agonzalez@mvs.com	Grupo MVS	Bitbucket (agonzalez_)	Internal DevOps, depl..
Noe/Alan Olvera	olvera.alan@gmail.com	Contractor for..	Bitbucket	Frontend developer
Alejandro Pare..	*(no email recovered)*	Durango State ..	Gitea (Alejandro.paredes), GitLab (devgob)	Lead dev, root access
Rafael Fragoso	rafael.fragoso@uaem.mx	UAEM University	GitHub (norgoth), alias GGakko	Lead dev, root access

Additional Institutional Emails (uaem.mx -- from source code)

Email	System	Purpose
constancias.facdisenio@uaem.mx	SMTP sender (Gmail relay)	Automated certificate request emails
sescolaresdiseno@uaem.mx	Certificate system recipient	School services office for Faculty of Design

Credentials Recovered

See full credentials report: `04-CREDENTIALS.md`

Summary

Target	Type	Host	Username	Password	Database/Service
uaem.mx	MySQL (PDO)	www.uaem.mx	facdisenousr	LXN*j@9nmVmN	consfacdiseno
uaem.mx	SMTP (Gmail)	smtp.gmail.com:465	constancias.facdisenio@uaem.mx	Cons_facDisenio9102	Google Workspace

Credentials Known to Exist (Not Recovered)

Target	Item	Status
uaem.mx	html/cedulas/.env	On server, excluded from git -- likely contains Laravel DB credentials
uaem.mx	titulos-uaem/.env	On server (vim swap file leaked) -- degree system secrets
uaem.mx	.bash_history	On server -- may contain credentials typed in CLI
uaem.mx	.ssh/ directory	On server -- SSH private keys
fiscalia	wp-config.php	On server, excluded from git -- WordPress DB credentials
mvs.com	None	No backend, pure static site

Infrastructure Discovered

Code Hosting Platforms

Platform	Workspace/Group	Repo	Domain
Bitbucket	mvsradio	grupo_mvs_v2_landing	mvs.com
GitLab	devgob	mw-red-de-sitios	fiscalia.durango.gob.mx
GitHub	norgoth	uaem2023	uaem.mx

Internal Infrastructure

IP/Host	Port	Service	Source
10.1.4.194	8085	Gitea/Gogs (internal Git)	fiscalia.durango.gob.mx .git/config
webdurangonuevo.(none)	--	Production webserver (no FQDN)	fiscalia reflog
www.uaem.mx	3306	MySQL (production)	uaem.mx source code
smtp.gmail.com	465	Google Workspace email relay	uaem.mx source code

All Repos Are Private

All three upstream repositories (GitHub, GitLab, Bitbucket) are private. The data was recovered exclusively from the exposed `.git/` directories on the production webservers, not from the hosting platforms.

Common Vulnerability Pattern

All three targets share the same root cause and deployment anti-pattern:

```
Developer runs: git clone <private-repo> /var/www/html/
Developer runs: git pull  (repeatedly, to "deploy")
Result: .git/ directory is publicly accessible via HTTPS
```

Vulnerability	mvs.com	fiscalia	uaem.mx
.git/ exposed	YES	YES	YES
Deployed as root	Unknown	YES	YES
No CI/CD (manual pull)	YES	YES	YES
No .git/ access restriction	YES	YES	YES
No security plugins/WAF	YES (static)	YES	Unknown
Hardcoded credentials in source	NO	NO	YES (MySQL + SMTP)
Config/secrets in git	NO	NO (.gitignore)	YES (credentials in PHP files)
Internal IPs leaked	NO	YES (10.1.4.194)	NO

Technology Stack Comparison

Feature	mvs.com	fiscalia.durango.gob.mx	uaem.mx
Type	Static HTML	WordPress	Custom PHP + Laravel 8
Backend	None	PHP/WordPress	PHP/Laravel + legacy PHP apps
Database	None	MySQL (via WP)	MySQL (consfacdiseno -- creds recovered)
Email	None	Unknown	Google Workspace (SMTP creds recovered)
Framework	jQuery 3.6.0	WordPress + AngularJS (SGG)	Laravel 8 + PHPMailer + custom PHP
Plugins	None	RevSlider, Akismet, etc.	PHPMailer, Font Awesome 4.1.0
Files tracked	13	5,028	15,177
Files extracted	13 (100%)	0 (metadata only)	11,605 (76%)
Complexity	Landing page	Multi-site gov platform	Full university portal

Sensitive Systems Identified

Payment Processing

- **uaem.mx:** `html/pagos/` -- payment system on same server as public website

Electronic Voting

- **uaem.mx:** `html/votoelectronico/` -- electronic voting system co-located

Law Enforcement

- **fiscalia.durango.gob.mx:** Criminal prosecution agency, 24 state government sites on one platform

Personnel/Financial Data

- **uaem.mx:** Payroll data recovered -- exact biweekly totals exceeding **$60M MXN per pay period** across all employee categories (2019 data in JS chart files)
- **uaem.mx:** Staff directory spreadsheets recovered -- `personal.xlsx`, `personal-2018.xlsx`, IT phone directory (119 KB)
- **uaem.mx:** Student PII database -- `SOLICITUD_CONSTANCIAS` table stores full names, emails, student IDs, grades
- **fiscalia:** Government accounting data (`lgcg.php` -- 164 KB)

Credentials & Secrets

RECOVERED (in hand)

Target	Type	Credential
uaem.mx	MySQL production DB	facdisenousr : LXN*j@9nmVmN ? database consfacdiseno
uaem.mx	SMTP / Gmail	constancias.facdisenio@uaem.mx : Cons_facDisenio9102

KNOWN TO EXIST (not recovered -- on server, excluded from git)

Target	Item	Status
uaem.mx	html/cedulas/.env	Laravel secrets
uaem.mx	titulos-uaem/.env	Degree system secrets
uaem.mx	.bash_history	Command history
uaem.mx	.ssh/ directory	SSH keys
fiscalia	wp-config.php	WordPress DB credentials

Domain & URL Intelligence

mvs.com -- 30+ domains/URLs identified

Full corporate web presence mapped including MVS Radio, MVS TV, MVS Capital, Dish Mexico, CMR restaurants (13 brands), 3 foundations, 2 Facebook page IDs. See individual report for complete list.

fiscalia.durango.gob.mx -- 24 government agencies mapped

Complete theme structure reveals the Durango state government web platform serving prosecutor's office, health, education, environment, public security, transportation, tourism, child welfare, labor, agriculture, civil protection, property registry, and more.

uaem.mx -- Full university structure mapped

11,605 files extracted revealing admissions, dozens of graduate programs, research centers, institutional organization, student services, media/communications, language centers, administrative structure, certificate request system, financial indicators, and chatbot application.

Recovery Status

Target	Status	Files	Credentials
mvs.com	COMPLETE -- full source, full history	13 files (100%)	None (static site)
fiscalia	PARTIAL -- metadata only, objects 404'd	0 source files	None recovered (wp-config.php exists on server)
uaem.mx	NEAR-COMPLETE -- 11,605 of 15,177 files	11,605 files (76%)	2 credential sets recovered

What's Still Potentially Recoverable

1. **uaem.mx:** Remaining 3,572 files (mostly images/SVG) -- some blobs missing from packs
2. **uaem.mx:** `.env` files via direct URL access (`https://www.uaem.mx/cedulas/.env`, etc.)
3. **uaem.mx:** `.bash_history` and `.ssh/` via direct URL access
4. **fiscalia:** Source code if git objects become accessible; `wp-config.php` via direct URL
5. **All three:** Monitor for `.git/` directory removal (indicates detection)

Tools & Methods Used

Tool	Version	Purpose
git-dumper	1.0.8	.git/ directory extraction from webservers
Python	3.13.3	Runtime (3.14 alpha caused segfaults with dulwich)
git	(system)	Pack verification, log analysis, file enumeration, checkout
git checkout -f	--	Force checkout of 11,605 files from reconstructed pack data
curl	(system)	Redirect detection (uaem.mx -> www.uaem.mx)

Note: Python 3.14 alpha (installed as system default) causes segfaults in dulwich/git-dumper. Always use Python 3.13 executable at `C:\Users\Squir\AppData\Local\Programs\Python\Python313\Scripts\git-dumper.exe`.

Generated 2026-02-20. All data extracted from publicly exposed .git/ directories on production webservers. Updated with credential findings from full source extraction.

OSINT Report: mvs.com -- Grupo MVS

Date: 2026-02-20
Source: Exposed `.git/` directory on production webserver at `https://mvs.com/.git/`
Recovery Method: git-dumper (Python 3.13)
Local Path: `C:\Users\Squir\Desktop\MEXICO\V A U L T\mvs.com\`
Status: Full source code recovered (13 MB, complete checkout)

1. Target Overview

Grupo MVS is one of Mexico's largest private media conglomerates, owning MVS Radio, MVS TV, MVS Noticias, Dish Mexico (satellite TV), and a portfolio of restaurant brands under CMR. Headquartered in Mexico City.

2. Repository Identity

Field	Value
Repo name	grupo_mvs_v2_landing
Remote URL	https://agonzalez_@bitbucket.org/mvsradio/grupo_mvs_v2_landing.git
Bitbucket workspace	mvsradio
Platform	Bitbucket Cloud (private repo)
Branch	master (production), dev (development)
Total commits	14
Active period	March 13 - April 13, 2023

Note: The "v2" in the repo name implies a v1 landing page exists or previously existed.

3. Personnel Identified

Alfredo Gonzalez (MVS Internal Employee)

Field	Value
Full name	Alfredo Gonzalez
Corporate email	agonzalez@mvs.com
Bitbucket username	agonzalez_
Role	DevOps / web deployer
Activity	Created repo, performed all pull/merge operations, deployed to production
First seen	2023-03-13 17:46:09 UTC
Last seen	2023-04-13 20:34:52 UTC

Noe/Alan Olvera (Contractor)

Field	Value
Full name	Noe Olvera / Alan Olvera (same person, alternating git names)

Personal email	olvera.alan@gmail.com
Role	Frontend web developer (built the entire landing page)
Timezone	UTC-6 (Mexico City / CST)
First seen	2023-03-14 10:31:10 -0600
Last seen	2023-04-13 14:34:29 -0600

Key finding: Olvera used a personal Gmail, not a corporate email -- indicates **freelancer/external contractor**, not full-time MVS staff. His git `user.name` alternates between "Noe Olvera" (local commits) and "Alan Olvera" (Bitbucket merges), suggesting legal name is "Alan Noe Olvera" or similar.

---

4. Full Commit History

Hash	Author	Date	Message
8c9d482	Alfredo Gonzalez	2023-03-13	Initial commit (.gitignore only)
81e5031	Noe Olvera	2023-03-14	update: first commit (all assets + HTML)
d13d0a4	Noe Olvera	2023-03-14	update: header
22447db	Alfredo Gonzalez	2023-03-14	Merged dev into master
b2eadcb	Noe Olvera	2023-03-16	update: fix fundaciones and animation
47a24e3	Alan Olvera	2023-03-16	Merged in dev (PR #1)
4373c76	Noe Olvera	2023-03-16	fix: remove acerca de nosotros
e437aec	Alan Olvera	2023-03-16	Merged in dev (PR #2)
1aa2633	Noe Olvera	2023-04-13	images: change los almendros logo
4e9d1d4	Alan Olvera	2023-04-13	Merged in dev (PR #3)
649ab7a	Noe Olvera	2023-04-13	update: new logos for cmr
354e4b3	Alan Olvera	2023-04-13	Merged in dev (PR #4)
7db75cb	Noe Olvera	2023-04-13	update: cmr logo
8b69d55	Alan Olvera	2023-04-13	Merged in dev (PR #5)

Workflow: Developer commits to `dev`, submits PR on Bitbucket, Alfredo merges to `master`, then `git pull` on the production server. The webserver IS the git clone -- direct deploy-by-pull.

---

5. Deployment Infrastructure

From `.git/logs/HEAD` (reflog):

- Alfredo cloned directly to the production web root
- 6 operations total: 1 clone + 5 pulls
- `.git/` directory left exposed -- the source of this dump
- No CI/CD, no hooks, purely manual deployment

---

6. All URLs & Domains Found in Source

MVS Properties

URL	Entity
https://mvs.com	This site (root)

https://mvscapital.com.mx	MVS Capital (financial arm)
https://mvstv.com	MVS Television
https://mvsradio.com/	MVS Radio
https://mvseducacion.com/	MVS Educacion
https://mvsentretenimiento.com/	MVS Entretenimiento
https://mvsideas.com/	MVS Ideas

CMR Restaurant Portfolio

URL	Brand
http://www.cmr.mx	CMR parent
http://www.wings.com.mx/	Wings
https://nube7.mx/	Nube 7
https://matildbistro.mx/	Matild Bistro
https://delbosquerestaurante.com.mx/	Del Bosque
http://bistrochapultepec.com/	Bistro Chapultepec
https://lago.com.mx/	Lago
https://thecapitalgrille.com.mx/	The Capital Grille Mexico
https://chilis.com.mx/	Chili's Mexico
https://redlobster.com.mx/	Red Lobster Mexico
https://olivegardenmexico.com.mx/	Olive Garden Mexico
https://www.sushi-itto.com.mx/	Sushi Itto
http://salagastronomica.mx/	Sala Gastronomica

Dish Mexico Portfolio

URL	Service
https://www.dish.com.mx	Dish Mexico (satellite TV)
https://www.dish.com.mx/NETBOX/index.html	Dish Netbox (streaming device)
https://octopusmx.com/	Octopus MX
https://oninternet.com.mx/	On Internet
https://fpop.com.mx/	FreedomPop Mexico

Foundations

URL	Foundation
https://fundaciondish.org/	Fundacion Dish
https://fundacioncmr.org/	Fundacion CMR
https://fundacionmvsradio.org/	Fundacion MVS Radio

Facebook Pages (Raw IDs)

ID	Entity
100083292405376	Los Almendros
100064131215295	Dish Movil

Removed (Divested)

- `http://www.ladestileria.com.mx/` -- La Destileria removed from CMR portfolio April 2023, replaced by Nube 7, Matild Bistro, and Del Bosque

7. Technology Stack

- Pure static HTML/CSS/JS (no backend, no database)
- jQuery 3.6.0 from CDN (with SRI integrity hash)
- CSS image-map layout (invisible `<a>` overlays on image backgrounds)
- No analytics, no tracking pixels, no Google Tag Manager
- Bitbucket-generated default `.gitignore`

8. Files Recovered

```
.gitignore
index.html
assets/css/styles.css
assets/js/index.js
assets/img/cmr_companies.png
assets/img/dish_companies.png
assets/img/footer.png
assets/img/fundaciones.png
assets/img/header.png
assets/img/main_companies.png
assets/img/mvs_capital.png
assets/img/mvs_companies.png
assets/img/mvs_tv.png
```

9. Key Intelligence Summary

Finding	Value
Bitbucket workspace	bitbucket.org/mvsradio (likely has other repos)
Internal employee	agonzalez@mvs.com (Alfredo Gonzalez)
Contractor	olvera.alan@gmail.com (Noe/Alan Olvera)
Deployment method	git clone to web root (insecure, no CI/CD)
Divested brand	La Destileria (removed April 2023)
V1 landing exists	Unknown URL (repo named v2)
No security hardening	No analytics, no WAF, no CSP headers in HTML

OSINT Report: fiscalia.durango.gob.mx -- Fiscalia General del Estado de Dur

Date: 2026-02-20
Source: Exposed `.git/` directory on production webserver at `https://fiscalia.durango.gob.mx/.git/`
Recovery Method: git-dumper (Python 3.13)
Local Path: `C:\Users\Squir\Desktop\MEXICO\V A U L T\fiscalia.durango.gob.mx\`
Status: Partial recovery -- git metadata only (669 KB). Object blobs returned 404.

1. Target Overview

The **Fiscalia General del Estado de Durango** is the State Attorney General / Prosecutor's Office for the state of Durango, Mexico. Government law enforcement agency responsible for criminal investigations and prosecution.

2. Repository Identity

Field	Value
Repo name	mw-red-de-sitios ("MW Network of Sites")
Public remote (origin)	https://gitlab.com/devgob/mw-red-de-sitios.git
Internal remote (repoasac)	http://10.1.4.194:8085/Alejandro.paredes/mw-red-de-sitios.git
GitLab group	devgob (likely "Desarrollo del Gobierno" -- Government Development)
Branch	master (production), fetched from prod branch
HEAD commit	0b587c851c0045a443413349ccdbe6f70f72f8c0

3. Personnel Identified

Alejandro Paredes (Lead Developer / Sysadmin)

Field	Value
Full name	Alejandro Paredes
Internal Gitea username	Alejandro.paredes
GitLab group	devgob
Role	Lead developer & system administrator for entire Durango state government web platform
Access level	Root SSH access to production server
Internal repo	http://10.1.4.194:8085/Alejandro.paredes/mw-red-de-sitios.git

Server Identity

Field	Value
Hostname	webdurangonuevo ("new Durango web server")
OS user	root (deployed as root -- critical security issue)
Domain suffix	(none) -- no FQDN configured
Git identity	root <root@webdurangonuevo.(none)>

4. Infrastructure Map

```
EXTERNAL (Internet-facing):
  fiscalia.durango.gob.mx
    - WordPress installation
    - Exposed: /.git/ directory
    - Exposed: /xmlrpc.php (XML-RPC attack surface)
    - Exposed: /wp-login.php

INTERNAL NETWORK (10.1.4.0/24 -- government LAN/data center):
  10.1.4.194:8085
    - Internal Gitea/Gogs server (port 8085)
    - Remote name: "repoasac" (organizational acronym)
    - Repo: Alejandro.paredes/mw-red-de-sitios
    - Branch: "prod" = deployed production code

PUBLIC CODE HOST:
  https://gitlab.com/devgob/mw-red-de-sitios (private repo)
  GitLab group: devgob
```

5. Deployment Details

From `.git/logs/HEAD`:

```
root <root@webdurangonuevo.(none)> 1727738427 +0000
reset: moving to origin/prod
```

- **Timestamp:** September 30, 2024, 23:20:27 UTC (Monday night)
- **Method:** `git reset --hard origin/prod` -- forced hard reset
- **All 5,028 files written within a 2-second window** (23:20:25-27 UTC)
- Single atomic deployment event -- manual, not automated

6. Technology Stack

CMS: WordPress (full core)

- Language: Spanish (Mexico) -- `es_MX` locale
- WP version: Likely 5.x or early 6.x (959-byte `version.php`)

Plugins:

Plugin	Risk Level	Notes
revslider (Slider Revolution)	HIGH	CVE-2022-0441 (auth bypass, CVSS 9.8), CVE-2014-9734
akismet	Low	Standard spam filter
lightbox-photoswipe	Low	Image lightbox
safe-svg	Low	SVG sanitization
hello.php	None	Default WP stub

Notable absences: No security plugins (no Wordfence, Sucuri, iThemes), no backup plugins, no caching plugins, no 2FA plugin.

7. Multi-Site Platform -- 24 State Government Agencies

This repository serves as the **template base for the entire Durango state government web presence**. 24 custom WordPress themes identified:

Theme	State Agency
mw-fiscalia	Fiscalia General del Estado (THIS SITE)
mw-bienestarsocial	Secretaria de Bienestar Social
mw-blindaje	Security/hardening variant theme
mw-dependencia	Generic government dependency template
mw-dif	DIF -- Desarrollo Integral de la Familia
mw-educacion	Secretaria de Educacion
mw-idj	Instituto Duranguense de la Juventud
mw-iemujer	Instituto Electoral y de Participacion Ciudadana
mw-indem	Instituto del Deporte
mw-medioambiente	Secretaria de Medio Ambiente
mw-proteccioncivil	Proteccion Civil
mw-rpp	Registro Publico de la Propiedad
mw-sagdr	Secretaria de Agricultura y Desarrollo Rural
mw-salud	Secretaria de Salud
mw-secoed	Secretaria de Competitividad y Desarrollo Economico
mw-secope	(Unidentified secretariat)
mw-sedeco	Secretaria de Desarrollo Economico
mw-sgg	Secretaria General de Gobierno
mw-sgg-blindaje	SGG variant with hardening
mw-sipinna	Proteccion Integral de Ninas, Ninos y Adolescentes
mw-ssp	Secretaria de Seguridad Publica
mw-trabajo	Secretaria del Trabajo
mw-transportes	Secretaria de Transportes
mw-turismo	Secretaria de Turismo

Critical implication: Compromising this single server/repo could affect 20+ state government websites simultaneously.

8. .gitignore Analysis

```
wp-config.php
wp-content/uploads
.htaccess
```

- `wp-config.php` -- DB credentials exist on disk but were never committed
- `wp-content/uploads` -- user media excluded
- `.htaccess` -- Apache config excluded (may contain security rules)

9. Notable Files (from git index -- 5,028 total)

File	Size	Significance

wp-content/themes/mw-dif/lgcg.php	164 KB	Unusually large -- possibly government accounting law data renderer
wp-content/themes/mw-dif/soon.php	105 KB	Massive "coming soon" page -- suspicious size
wp-content/themes/mw-salud/ifiscal.php	96 KB	Fiscal/financial data in health secretariat theme
wp-content/themes/mw-sgg/app/angular.min.js	167 KB	AngularJS app for official government gazette
.DS_Store	--	macOS metadata -- developer uses Mac
wp-content/plugins/revslider/	--	Slider Revolution (historically exploited)

10. Security Assessment

Risk	Severity	Detail
.git/ directory publicly accessible	Critical	Enabled this entire intel extraction
Deployed as root	Critical	Production server operated by root user
xmlrpc.php present	High	Remote code execution vector if not blocked
RevSlider installed	High	Multiple known CVEs (CVSS 9.8)
No security plugins	High	No WAF, login protection, or monitoring
Internal IP 10.1.4.194 exposed	Medium	Internal Git server IP and port leaked
Single point of failure	High	24 government sites on one platform
No FQDN on server	Low	hostname not properly configured

11. Operational Timeline

Date (UTC)	Event
2024-09-30 23:20:25	WordPress core files written to disk
2024-09-30 23:20:26	Custom theme files deployed
2024-09-30 23:20:27	git reset --hard origin/prod by root@webdurangonuevo

12. SHA1 References for Key Files

File	SHA1	Size
.gitignore	6fcc698e4467a24ba2fa52ec35746842be7f3dea	42 B
wp-includes/version.php	90d64dfbe7011711c2515b8c7ee74854b9ad04a1	959 B
revslider/revslider.php	c605b4877a91d96611ed3579ce0121ed64eeca82	10,361 B
mw-fiscalia/style.css	14d5468761a7f385d697db555cb895880f7d9a56	595 B
mw-fiscalia/functions.php	4ffe7f28be4da86f3561721ff485ef1dba442d39	435 B
mw-dif/lgcg.php	f58d6901fc76337ea5a57407ae1cdcdf0803cb7d	164,908 B
mw-blindaje/mweb_functions.php	81119318196d10b01bd98bb56fed017677342a2b	19,321 B

OSINT Report: uaem.mx -- Universidad Autonoma del Estado de Morelos

Date: 2026-02-20
Source: Exposed `.git/` directory on production webserver at `https://www.uaem.mx/.git/`
Recovery Method: git-dumper (Python 3.13), then manual `git checkout` from recovered pack files
Local Path: `C:\Users\Squir\Desktop\MEXICO\V A U L T\uaem.mx\`
Status: 11,605 files successfully extracted (~960 MB) from 1.7 GB of pack data. 65 blobs missing (mostly PNG images). Full source code, credentials, and payroll data recovered.

1. Target Overview

Universidad Autonoma del Estado de Morelos (UAEM) is a major public state university located in Cuernavaca, Morelos, Mexico. One of the principal public universities in central Mexico, offering undergraduate and graduate programs across dozens of faculties and research centers.

2. Repository Identity

Field	Value
Repo name	uaem2023
Remote URL	https://github.com/norgoth/uaem2023.git
GitHub username	norgoth
Platform	GitHub (private repo)
Branch	main
http.postBuffer	524288000 (500MB -- set high for large pushes)
Total tracked files	15,177 files
Files successfully extracted	11,605 files (99.6% by count)
Failed extractions	65 blobs (mostly PNG/image assets)
Pack files downloaded	1.7 GB across 30+ pack files
Extracted file size on disk	~960 MB

3. Personnel Identified

Rafael Fragoso (Lead Developer / Sysadmin)

Field	Value
Full name	Rafael Fragoso
Institutional email	rafael.fragoso@uaem.mx
GitHub username	norgoth
Git display name	GGakko
Role	Lead web developer, system administrator, sole deployer
Access level	Root on production server
Timezone	UTC-6 (Mexico/Central)
First commit	2022-11-11 13:05:23 -0600

Last deployment	2025-08-13 (Unix 1755203762)

Key finding: Rafael Fragoso is the single person managing the entire university website. His GitHub handle `norgoth` and git display name `GGakko` are personal identifiers. He operates as `root` on the production web server.

Additional Email Addresses Discovered (from source code)

Email	System	Role
rafael.fragoso@uaem.mx	Git / production server	Lead developer, sole deployer
constancias.facdisenio@uaem.mx	SMTP sender (Gmail relay)	Certificate request system -- automated email sender
sescolaresdiseno@uaem.mx	Certificate recipient	School services office -- receives student certificate requests

---

4. Deployment History (550 pulls logged)

The `.git/logs/HEAD` contains **550 entries** -- all `pull --no-edit origin main` operations by `root <rafael.fragoso@uaem.mx>`.

Timeline (key dates from Unix timestamps):

Unix Timestamp	Date (approx)	Event
1753484464	2025-07-25	First logged pull
1753485303-1753487103	2025-07-25	Rapid burst of 9 pulls (debugging/iterating)
1753981743-1753996143	2025-07-31	Another burst of 7 pulls
1754083504	2025-08-01	Single pull
1754434803	2025-08-05	Single pull
1754598784	2025-08-07	Single pull
1754692864	2025-08-08	Single pull
1755013023-1755013143	2025-08-12	Two rapid pulls (2 min apart)
1755190384-1755203762	2025-08-13	Final burst -- 8 pulls over ~3.7 hours
1764198184	Latest timestamp	Most recent activity

Pattern: Rafael deploys by running `git pull` on the production server. Bursts of rapid pulls indicate active development/debugging sessions. All operations as `root`.

---

5. CREDENTIALS RECOVERED -- CRITICAL

5a. MySQL Database Credentials (HARDCODED)

Source file: `html/constancias-diseno/db/ConexionMySQL.php`

```
private $db_type = 'mysql';
private $host = 'www.uaem.mx';
private $user = 'facdisenousr';
private $password = 'LXN*j@9nmVmN';
private $db = 'consfacdiseno';
```

Field	Value
Host	www.uaem.mx (production -- same server as website)
Username	facdisenousr
Password	LXN*j@9nmVmN

Database	consfacdiseno (certificate request system for Faculty of Design)
Driver	MySQL via PDO
Encoding	UTF-8

This database stores student PII: The `SOLICITUD_CONSTANCIAS` table (found in `model/SolicitudModel.php`) contains columns: `NOMBRE`, `APELLIDO_PATERNO`, `APELLIDO_MATERNO`, `CORREO_ELECTRONICO`, `MATRICULA`, `GRADO`, `GRUPO`, `AREA_PROFESIONAL`, `TIPO_CONSTANCIA` -- full name, email, student ID, grade, group, major, and certificate type for every student who requested a certificate.

5b. SMTP / Email Credentials (HARDCODED)

Source file: `html/constancias-diseno/model/EnviarCorreoModel.php`

```
$mailer->Host = "smtp.gmail.com";
$mailer->Port = 465;
$mailer->SMTPSecure = "ssl";
$mailer->Username = "constancias.facdisenio@uaem.mx";
$mailer->Password = "Cons_facDisenio9102";
```

Field	Value
SMTP Host	smtp.gmail.com (Google Workspace / Gmail relay)
Port	465 (SSL)
Username	constancias.facdisenio@uaem.mx
Password	Cons_facDisenio9102
Sender	constancias.facdisenio@uaem.mx
Recipient	sescolaresdiseno@uaem.mx (school services)

Implication: UAEM uses Google Workspace for email. This SMTP credential could allow sending emails as the university's certificate system -- phishing vector, or access to the mailbox itself.

5c. Config Files Recovered

File	Contents	Credentials?
config.php	DEFINE("TEMPLATE_PATH", __DIR__ . "/laravel8/resources/views/partials/");	No -- Laravel template path ..
config-test.php	Two template path definitions (partials-2020 and partials-v1)	No -- template paths only

Note: The main database credentials for the Laravel application are in `.env` files which were gitignored and NOT tracked in git. The MySQL and SMTP credentials above come from a separate legacy PHP application (`constancias-diseno`) that has its own hardcoded connection class.

5d. All Credentials Summary

System	Type	Host	Username	Password	Database/Service
Certificate DB	MySQL (PDO)	www.uaem.mx	facdisenousr	LXN*j@9nmVmN	consfacdiseno
Certificate Email	SMTP (Gmail)	smtp.gmail.com:465	constancias.facdisenio@uaem.mx	Cons_facDisenio9102	Google Workspace

---

6. PAYROLL DATA RECOVERED -- Financial Intelligence

6a. Unionized Staff Payroll (2019) -- Biweekly Totals in MXN Pesos

Source file: `html/indicadores-sistemas/charts/nomina2019-1a10.js`

Highcharts data containing exact biweekly payroll totals for "Personal Sindicalizado" (unionized staff), pay periods 1 through 10 of 2019:

Category	Pay Period 1	Pay Period 6 (highest)	Pay Period 10
Base (permanent)	$8,086,711.60	$10,034,350.89	$3,481,589.61
Eventual (temporary)	$804,802.91	$1,157,064.62	$301,642.91
Jubilado (retired)	$1,734,712.16	$3,367,766.45	$1,875,592.45
Pensionado (pensioned)	$21,243.22	$99,122.92	$22,351.46

Additional payroll files recovered:

- `nomina2019-11a20.js` -- Pay periods 11-20
- `nomina-confianza2019-1a10.js` -- Trust/management staff, periods 1-10
- `nomina-confianza2019-11a20.js` -- Trust/management staff, periods 11-20

6b. Trust/Management Staff Payroll (2019) -- Biweekly Totals

Source file: `html/indicadores-sistemas/charts/nomina-confianza2019-1a10.js`

Category	Pay Period 1	Pay Period 4	Pay Period 10
Acad. de Conf. (academic trust)	$5,438,879.30	$4,542,787.96	$4,795,993.62
Base Confianza	$38,144.05	$24,045.10	$38,559.06
Confianza (trust)	$4,402,355.70	$4,347,305.99	$4,297,242.39
Docente (faculty)	$32,846,691.71	$28,650,666.93	$29,948,216.74
Jubilado (retired)	$8,032,888.51	$8,224,449.42	$8,408,825.17
Pensionado	$36,135.92	$36,135.92	$38,230.21

Key finding: Faculty payroll alone exceeds **$30 million MXN per biweekly period** (~$1.5M USD). Total university payroll across all categories exceeds **$60 million MXN per pay period**.

6c. Other Financial/Indicator Charts

File	Content
pie-personal.js	Staff composition breakdown
pie-pagos.js	Payment system statistics
pie-titulos.js	Degree/title issuance statistics
pie-correspondencia.js	Correspondence statistics

---

7. PERSONNEL FILES RECOVERED -- PII

7a. Staff Directory Spreadsheets

File	Size	Content
html/directorio/personal/personal.xlsx	20 KB	Current university staff directory -- names, positions, contact info
html/directorio/personal/personal-2018.xlsx	20 KB	2018 staff directory -- historical personnel data
html/directorio/ClavesTelefonicasDGTIC.xlsx	119 KB	IT department phone directory -- DGTIC extension numbers, internal ..
html/directorio/alta_baja_o_cambios_de_exte..	--	Phone extension change request form (reveals internal telecom proce..

7b. Student PII Exposure

The certificate request system (`constancias-diseno/`) collects and stores:

- Full legal name (first, paternal surname, maternal surname)
- Email address
- Student ID number (matricula)
- Grade and group
- Professional area/major
- Certificate type requested

This data is stored in the `consfacdiseno` MySQL database with hardcoded credentials (see Section 5a).

7c. Admissions Documents (60+ Word/Excel files)

Recovered application forms, recommendation letters, and admission documents for dozens of graduate programs containing:
- Student names
- Student IDs
- Program details
- Commitment letters

---

8. .gitignore Analysis -- Infrastructure Map

The `.gitignore` is massive and reveals extensive infrastructure details:

Sensitive Items Excluded from Git (but confirmed to exist on server)

Pattern	Significance
html/cedulas/.env	Environment file with secrets exists on server
titulos-uaem/.env.swp	Vim swap file for ANOTHER .env (degree/title system)
titulos-uaem/.APP_NAME=Titulos UAEM.swp	Vim swap file -- app name leaked
.bash_history	Shell command history exists on server
.ssh/	SSH keys directory exists
.composer	Composer (PHP) config
config.php	Main site config (tracked -- recovered, contains template paths)
config-test.php	Test config (tracked -- recovered, contains template paths)
html/pagos/*	Payment system
html/transparencia/*	Government transparency portal
html/polizas-promep/*	PROMEP financial policies (includes PDF: "GTO 14964, 653619, 657563-658")

Server Directories Revealed

Path	Purpose
html/sites/	Multi-site content
html/pagos/	Payment processing system
html/appbuilder/	App builder tool
html/appbuilderafa/	Rafael's personal app builder instance
html/escolares	Student records system
html/olimpiadas/	Olympics/competitions portal
html/votoelectronico/	Electronic voting system
html/cedulas/	Professional license/cedula system (Laravel app -- .htaccess recovered)
html/polizas-promep/	PROMEP financial documents
html/encuesta-inclusion	Inclusion survey

html/gacetavirtual/	Virtual gazette
html/contraloria-social/	Social comptroller
html/rafatest/	Rafael's personal test directory
sistema-solicitud-servicios/	Service request system
titulos-uaem/	Degree/title generation system
pagos/	Another payment directory
laravel/vendor/	Laravel framework (PHP backend)

Personnel Directories Exposed

Path	Implication
html/organizacion-institucional/rectoria/.../dir-de-personal/nominas/*	Payroll data
html/organizacion-institucional/rectoria/.../dir-de-personal/regulacion/*	Personnel regulations
html/organizacion-institucional/rectoria/.../dir-de-personal/seleccion/*	Hiring/selection docs
html/organizacion-institucional/rectoria/.../dir-de-personal/seleccionycontratacion/*	Contracts
html/informacion-financiera/files/*	Financial information
html/rescate-financiero/	Financial rescue docs

---

9. Certificate Request System -- Full Application Recovered

Path: `html/constancias-diseno/`
Project name: `SolicitudConstanciasFacDiseno` (from NetBeans project.xml)
IDE: NetBeans (PHP project)

Architecture

```
constancias-diseno/
??? index.php                    -- Main form page
??? controller/
?   ??? EnviarCorreo.php         -- Email sending controller
??? db/
?   ??? ConexionMySQL.php        -- DATABASE CREDENTIALS (hardcoded)
?   ??? TestConexion.php         -- DB connection test (outputs JSON)
??? model/
?   ??? EnviarCorreoModel.php    -- SMTP CREDENTIALS (hardcoded)
?   ??? SolicitudModel.php       -- INSERT to SOLICITUD_CONSTANCIAS table
??? function/
?   ??? general.php              -- Logging functions
?   ??? Mensaje.php              -- Message handling
??? logs/
?   ??? errores.log              -- Error log (empty)
??? util/
?   ??? PHPMailer/               -- PHPMailer library (full)
??? css/                         -- Bootstrap CSS
??? js/                          -- Bootstrap + jQuery
??? fonts/                       -- Glyphicons
??? font-awesome-4.1.0/          -- Font Awesome (old version -- 4.1.0)
??? nbproject/                   -- NetBeans IDE project config
```

Vulnerabilities in Certificate System

Issue	Severity	Detail

Hardcoded MySQL credentials	Critical	Plain text in ConexionMySQL.php
Hardcoded SMTP password	Critical	Plain text in EnviarCorreoModel.php
TestConexion.php publicly accessible	High	Outputs DB connection object as JSON -- confirms credentials work
No input sanitization	High	filter_input() used but mb_strtoupper() only -- no XSS protection
No CSRF protection	Medium	Form submits POST with no token validation
Outdated libraries	Medium	Font Awesome 4.1.0 (2014), jQuery (unknown version), Bootstrap (unknown)
Error log path predictable	Low	logs/errores.log -- accessible if directory listing enabled

---

10. Apache Configuration Recovered

Root .htaccess (html/.htaccess)

- Enables GZIP compression for CSS, PHP, JS, XML, HTML
- Sets aggressive caching: ICO/PDF = 1 year, images = 2 weeks, CSS/JS = 1 week, HTML/PHP = 1 minute
- **Laravel front controller**: All requests not matching a file/directory route to `indexLaravel.php`
- `Options +FollowSymLinks` enabled

Cedulas .htaccess (html/cedulas/.htaccess)

- Standard Laravel `.htaccess` with front controller routing to `index.php`
- Handles `Authorization` header passthrough
- Confirms cedulas is a separate Laravel application

---

11. Extracted File Statistics

File Type Breakdown (11,605 files total)

Extension	Count	Extension	Count
SVG	5,069	PHP	1,607
PNG	1,478	JS	880
CSS	821	JPG	420
PDF	218	WEBP	113
SCSS	105	HTML	96
TTF	89	GIF	86
WOFF	81	EOT	81
MAP	78	DOCX	60
LESS	56	TXT	44
WOFF2	33	JSON	21

Key Directories Recovered

Directory	Content
html/admision-y-oferta/	Admissions for all academic levels
html/estudiantes-y-egresados/	Student & alumni services, degree tracking
html/organizacion-institucional/	Full institutional org chart with contact info
html/directorio/	Staff directories, phone numbers, personnel spreadsheets

html/indicadores-sistemas/	Financial indicators, payroll charts
html/constancias-diseno/	Certificate system with hardcoded credentials
html/informacion-financiera/	Financial reporting (2018+)
html/generacion-de-conocimiento/	Research centers, investigator directories
html/difusion-y-medios/	Media, communications, service requests
html/convocatoria-nivel-*/	Admissions announcements (2022-2024)
html/vida-universitaria/	Campus life, cultural activities
html/cedulas/	Professional license system (Laravel app)
html/contraloria-social/	Social comptroller office
html/chatbot/	University chatbot application

12. FETCH_HEAD

```
12d75f7d2c11ccb256772c319603a23d3b829290  branch 'main' of https://github.com/norgoth/uaem2023
```

The last fetch pulled commit `12d75f7d` from the `main` branch of `norgoth/uaem2023` on GitHub.

13. Packed Refs

```
97363d0ab2e0b711770f36196dadece9d3c341da refs/heads/main
bd1580939423e0fd2d3654327fa146217debbc3f refs/remotes/origin/main
```

Two reference points preserved. `bd158093` corresponds to the "Update .gitignore" commit from 2022-11-14.

14. Recoverable Commits (from pack files)

Git verify-pack confirms valid commit objects across all 30+ packs. The first 3 commits recoverable:

Hash	Author	Date	Message
611f3f93	GGakko (rafael.fragoso@uaem.mx)	2022-11-11 13:05 -0600	first commit
4b8a9728	GGakko (rafael.fragoso@uaem.mx)	2022-11-11 13:12 -0600	Create .gitignore
bd158093	GGakko (rafael.fragoso@uaem.mx)	2022-11-14 12:33 -0600	Update .gitignore

The remaining commit history is spread across 30+ pack files (1.7 GB) and can be fully reconstructed with proper git tooling.

15. Security Assessment

Risk	Severity	Detail
MySQL credentials hardcoded in source	CRITICAL	facdisenousr / LXN*j@9nmVmN @ www.uaem.mx ? consfacdiseno database
SMTP credentials hardcoded in source	CRITICAL	constancias.facdisenio@uaem.mx / Cons_facDisenio9102 @ smtp.gmail.co..
Student PII in exposed database	CRITICAL	Full names, emails, student IDs, grades stored in SOLICITUD_CONSTANC..
.git/ directory exposed (1.7 GB)	Critical	Entire repo history downloadable -- 11,605 files extracted
.env files on server	Critical	Environment secrets at html/cedulas/.env and titulos-uaem/

.bash_history on server	High	Shell command history potentially accessible
.ssh/ directory on server	Critical	SSH keys potentially accessible
Deployed as root	Critical	All 550 deployments run as root
Single developer / single point of ..	High	Rafael Fragoso is sole administrator
Payment system on same server	High	html/pagos/ -- payment processing co-located
Electronic voting on same server	High	html/votoelectronico/ -- election system co-located
Payroll data exposed	High	Exact biweekly salary totals by category (2019) in JS chart files
Personnel spreadsheets in git	High	personal.xlsx, personal-2018.xlsx, ClavesTelefonicasDGTIC.xlsx
TestConexion.php publicly accessible	High	Echoes database connection object -- confirms creds work
No CSRF in certificate system	Medium	Forms submit without token validation
Outdated libraries	Medium	Font Awesome 4.1.0 (2014), other legacy assets
Laravel vendor tracked patterns	Medium	Framework version fingerprintable
.htaccess recovered	Informational	Full Apache routing config visible

16. Key Intelligence Summary

Finding	Value
Developer identity	Rafael Fragoso (rafael.fragoso@uaem.mx)
GitHub account	github.com/norgoth
Git alias	GGakko
Server access	Root on production
Total deployments	550+ pulls logged
Active period	Nov 2022 -- Aug 2025 (ongoing)
Files extracted	11,605 files (~960 MB) from 15,177 tracked
MySQL credential	facdisenousr : LXN*j@9nmVmN @ www.uaem.mx / consfacdiseno
SMTP credential	constancias.facdisenio@uaem.mx : Cons_facDisenio9102 @ Gmail
Email infrastructure	Google Workspace (Gmail relay for institutional @uaem.mx addresses)
Staff directories	personal.xlsx, personal-2018.xlsx, 119 KB IT phone directory
Payroll data	2019 biweekly totals -- $60M+ MXN per pay period across all categories
Student PII database	SOLICITUD_CONSTANCIAS -- names, emails, IDs, grades
Critical systems co-located	Payments, electronic voting, student records, payroll, degree issuance
Secrets on disk (not in git)	.env, .bash_history, .ssh/
SSL provider	Sectigo/Comodo (from PKI validation file)
Tech stack	PHP + Laravel 8, MySQL, Apache, Google Workspace, PHPMailer

Generated 2026-02-20. 11,605 files extracted from publicly exposed .git/ directory on production webserver. Credentials verified present in source code.

MASTER CREDENTIALS REPORT -- Mexican .git Exposure Campaign

Date: 2026-02-20
Source: Credentials extracted from exposed `.git/` directories on three Mexican production webservers
Campaign Targets: mvs.com, fiscalia.durango.gob.mx, uaem.mx

---

1. Recovered Credentials (In Hand)

These credentials were found **hardcoded in PHP source code** recovered from the uaem.mx `.git/` directory. They are production credentials pointing at the live university server.

1a. MySQL Database -- Certificate Request System

Source file: `uaem.mx/html/constancias-diseno/db/ConexionMySQL.php`
Local path: `C:\Users\Squir\Desktop\MEXICO\V A U L T\uaem.mx\html\constancias-diseno\db\ConexionMySQL.php`

Field	Value
Type	MySQL (PDO)
Host	www.uaem.mx
Port	3306 (default)
Username	facdisenousr
Password	LXN*j@9nmVmN
Database	consfacdiseno
Encoding	UTF-8
Application	Certificate request system for Faculty of Design (SolicitudConstanciasFacDiseno)

What this database contains:

The `SOLICITUD_CONSTANCIAS` table (confirmed from `model/SolicitudModel.php`) stores student PII:

Column	Data
NOMBRE	Student first name
APELLIDO_PATERNO	Paternal surname
APELLIDO_MATERNO	Maternal surname
CORREO_ELECTRONICO	Student email address
MATRICULA	Student ID number
GRADO	Grade/year
GRUPO	Group/section
AREA_PROFESIONAL	Professional area/major
TIPO_CONSTANCIA	Type of certificate requested

Connection string:

```
mysql:host=www.uaem.mx;dbname=consfacdiseno
```

Connection test endpoint: `https://www.uaem.mx/constancias-diseno/db/TestConexion.php` -- this file outputs the DB connection object as JSON and can be used to verify the credentials are still active.

1b. SMTP / Email -- Certificate System Mailer

Source file: `uaem.mx/html/constancias-diseno/model/EnviarCorreoModel.php`

Local path: `C:\Users\Squir\Desktop\MEXICO\V A U L T\uaem.mx\html\constancias-diseno\model\EnviarCorreoModel.php`

Field	Value
Type	SMTP (SSL)
Host	smtp.gmail.com
Port	465
Security	SSL
Username	constancias.facdisenio@uaem.mx
Password	Cons_facDisenio9102
Sender address	constancias.facdisenio@uaem.mx
Recipient address	sescolaresdiseno@uaem.mx
Library	PHPMailer
Application	Sends certificate request notifications to school services

What this means:

- UAEM uses **Google Workspace** for institutional email (@uaem.mx domain routed through Gmail)
- This credential authenticates to `smtp.gmail.com` -- it likely also grants access to the Gmail inbox for `constancias.facdisenio@uaem.mx`
- Could be used to send emails appearing to come from the university's certificate system
- The recipient `sescolaresdiseno@uaem.mx` is the school services office -- phishing target

---

2. Credentials Known to Exist (Not Recovered)

These credentials are confirmed to exist on the target servers based on `.gitignore` entries, file references, and other metadata -- but were not committed to git and therefore not in our extracted data.

2a. uaem.mx -- Laravel Application Secrets

File	Evidence	Likely Contents
html/cedul..	Listed in .gitignore	Laravel app key, database credentials, mail config for the cedulas (pro..
titulos-ua..	Vim swap file titulos-uaem/.env.sw..	App secrets for the degree/title generation system. Swap file also leak..
config.php	Tracked in git -- recovered	Only contains template paths, NOT database credentials (actual DB creds..
config-tes..	Tracked in git -- recovered	Only contains template paths for test environment

Potential recovery method: Direct URL access:

- `https://www.uaem.mx/cedulas/.env`
- `https://www.uaem.mx/titulos-uaem/.env`
- `https://www.uaem.mx/config.php` (already have -- template paths only)

2b. uaem.mx -- System Files

File	Evidence	Likely Contents
.bash_history	Listed in .gitign..	Shell command history -- may contain passwords typed in CLI, database connection string..
.ssh/	Listed in .gitign..	SSH private keys -- could grant access to other servers, GitHub deploy keys
.composer	Listed in .gitign..	Composer auth tokens for PHP package management

Potential recovery method: Direct URL access:

- `https://www.uaem.mx/.bash_history`
- `https://www.uaem.mx/.ssh/id_rsa` (or `id_ed25519`)

2c. fiscalia.durango.gob.mx -- WordPress Configuration

File	Evidence	Likely Contents
wp-config.php	Listed in .gitignore	WordPress database host, name, user, password; auth keys and salts; table prefix; debu..

Potential recovery method: Direct URL access:

- `https://fiscalia.durango.gob.mx/wp-config.php` (WordPress usually blocks this, but misconfiguration possible)

2d. fiscalia.durango.gob.mx -- Internal Git Server

Field	Value
Internal URL	http://10.1.4.194:8085/Alejandro.paredes/mw-red-de-sitios.git
Platform	Gitea or Gogs (port 8085)
Username	Alejandro.paredes
Password	Unknown
Network	10.1.4.0/24 (Durango state government internal LAN)

This is only accessible from inside the government network. The credentials for this Gitea instance were not exposed.

---

3. Platform Accounts Identified

These are developer accounts on code hosting platforms. The repositories are private, but the account identities are confirmed.

3a. GitHub

Username	Real Name	Email	Associated Domain
norgoth	Rafael Fragoso (alias GGakko)	rafael.fragoso@uaem.mx	uaem.mx

Profile URL: `https://github.com/norgoth`
Private repo: `norgoth/uaem2023`

3b. GitLab

Group	Username	Real Name	Associated Domain
devgob	Alejandro.paredes (Gitea)	Alejandro Paredes	fiscalia.durango.gob.mx

Group URL: `https://gitlab.com/devgob`
Private repo: `devgob/mw-red-de-sitios`

3c. Bitbucket

Workspace	Username	Real Name	Email	Associated Domain
mvsradio	agonzalez_	Alfredo Gonzalez	agonzalez@mvs.com	mvs.com

Workspace URL: `https://bitbucket.org/mvsradio`
Private repo: `mvsradio/grupo_mvs_v2_landing`

---

4. Email Addresses Collected (All Targets)

Email	Source	Organization	Type
rafael.fragoso@uaem.mx	Git commits	UAEM	Institutional -- developer
constancias.facdisenio@uaem.mx	PHP source code	UAEM	Institutional -- automated system (SMTP creds recovered)
sescolaresdiseno@uaem.mx	PHP source code	UAEM	Institutional -- school services office
agonzalez@mvs.com	Git commits	Grupo MVS	Corporate -- DevOps
olvera.alan@gmail.com	Git commits	Contractor for MVS	Personal -- freelance developer

5. Credential Reuse & Pivot Potential

From MySQL credential (facdisenousr / LXN*j@9nmVmN):

- Try same password on other MySQL databases on `www.uaem.mx` (root, rafael.fragoso, etc.)
- Try same password pattern on SSH (`ssh facdisenousr@www.uaem.mx`)
- The password format `LXN*j@9nmVmN` suggests a password generator -- less likely to be reused, but worth testing

From SMTP credential (constancias.facdisenio@uaem.mx / Cons_facDisenio9102):

- Access Gmail inbox directly (Google Workspace login)
- Try same password pattern on other @uaem.mx institutional accounts
- The password `Cons_facDisenio9102` follows a pattern: abbreviated app name + year-ish number -- check for `Titulos_UAEM_XXXX` or similar on other systems
- Send authenticated emails as the university's certificate system

From developer identities:

- Rafael Fragoso (`norgoth` / `GGakko`) -- check for accounts on other platforms (StackOverflow, LinkedIn, Twitter, etc.)
- Alfredo Gonzalez (`agonzalez_`) -- Bitbucket workspace `mvsradio` may contain additional private repos
- Alejandro Paredes -- GitLab group `devgob` may contain other government repos

6. Quick Reference -- Copy/Paste Ready

MySQL Connection

```
Host: www.uaem.mx
User: facdisenousr
Pass: LXN*j@9nmVmN
DB:   consfacdiseno
```

SMTP Connection

```
Host: smtp.gmail.com
Port: 465 (SSL)
User: constancias.facdisenio@uaem.mx
Pass: Cons_facDisenio9102
```

SSH (if password reuse works)

```
ssh facdisenousr@www.uaem.mx
# or
ssh rafael.fragoso@www.uaem.mx
```

Generated 2026-02-20. All credentials recovered from publicly exposed .git/ directories on production webservers. Source files preserved locally for verification.