

---

## Incidente de seguridad – Validación y medidas implementadas Mildred Michelle Sánchez Cepeda - MOODLE

---

**Desde** Ingrid Silvana, Escobar Castro <IEscobar@saludcapital.gov.co>

**Fecha** Lun 6/04/2026 2:19 PM

**Para** Juan Sebastian, Martinez Martinez <JSMartinez@saludcapital.gov.co>

**CC** Laura Isabel, Velez Rios <livelez@saludcapital.gov.co>; Diana del Pilar, Pinzon Gomez <DPPinzon@saludcapital.gov.co>; Alba Rocio, Castillo Cruz <arcastillo@saludcapital.gov.co>

Buenas tardes ingeniero Juan Sebastian

En seguimiento al incidente de seguridad identificado en la plataforma Aula Virtual (Moodle) el día de hoy frente a la instalación de una extensión o plugin me permito informar las acciones realizadas, los hallazgos obtenidos y el estado final del sistema.

### 1. Descripción del incidente

Durante el monitoreo de logs se identificó actividad inusual asociada a la cuenta de usuario *Mildred Michelle Sánchez Cepeda*, consistente en la carga masiva y automatizada de archivos tipo *.zip* en el área de borradores (draft) del sistema, incluyendo un archivo denominado **“moodle-webshell-plugin-1.1.0.zip”**, lo cual corresponde a un intento potencial de carga de código malicioso.

Se evidenció además el uso de múltiples direcciones IP en intervalos cortos de tiempo, confirmando un comportamiento automatizado y consistente con compromiso de credenciales.

### 2. Análisis técnico realizado

- Se verificó que el usuario no cuenta con roles administrativos ni privilegios a nivel sistema.
- La actividad se limitó al uso indebido de credenciales válidas, sin escalamiento de privilegios.
- No se evidenció instalación de plugins ni ejecución de código malicioso en la plataforma.
- Los archivos fueron cargados únicamente en el área temporal (draft), sin ser utilizados ni publicados.
- Intentos de acceso a rutas administrativas fueron bloqueados correctamente por el firewall (WAF).

### 3. Validación de integridad del sistema (webshell)

Se realizó una validación técnica para descartar la presencia de código malicioso activo, incluyendo:

- Revisión de plugins instalados en la plataforma.
- Verificación de carpetas críticas del sistema (mod, local, blocks, admin).
- Análisis del almacenamiento (moodledata) asociado a archivos temporales.
- Validación funcional de la plataforma (accesos, navegación y comportamiento general).

### Resultado:

No se encontró evidencia de ejecución de código malicioso, persistencia ni presencia activa de webshell en el sistema.

#### 4. Acciones de contención implementadas

- Suspensión inmediata de la cuenta de usuario involucrada: **Mildred Michelle Sánchez Cepeda con CC1014177050**

- Monitoreo y análisis detallado de logs.
- Deshabilitación de la instalación de plugins desde la interfaz web (configuración de seguridad en el sistema).
- Aislamiento preventivo del curso asociado (ID: 277 – año 2021), incluyendo restricción de acceso y revisión de actividades tipo tarea.

- Verificación de que no existen archivos maliciosos en envíos de actividades académicas.

#### 5. Solicitud de acciones adicionales

Se solicita realizar el bloqueo a nivel de firewall (WAF o infraestructura) de las siguientes direcciones IP identificadas como origen de la actividad sospechosa:

- 62.146.237.3
- 157.66.56.231
- 103.77.107.199
- 157.15.40.6

#### 6. Estado actual de la plataforma

La plataforma se encuentra operando con normalidad, sin evidencia de compromiso, afectación de la información ni ejecución de código malicioso.

Quedo atenta a cualquier indicación adicional y a acciones complementarias que se consideren necesarias.

Silvana Escobar Castro

Secretaría Distrital de Salud

Dirección TIC