

Análisis: Presunto Incidente Fuga www.saludcapital.gov.co

Premisa:.....	1
Investigación de la información expuesta:.....	2
Investigación de los servidores relacionados:.....	4
Investigando el actor malicioso:.....	8
Mesa de Crisis 2PM 16/ENE/2026.....	9
Mesa de Crisis 8AM 19/ENE/2026	16

Premisa:

Supuestamente un usuario en Dark Forums ha publicado que ha logrado vulnerar la dirección de urgencias y emergencias en salud y relaciona la URL <https://www.saludcapital.gov.co/> donde habla de más de 90.000 registros.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

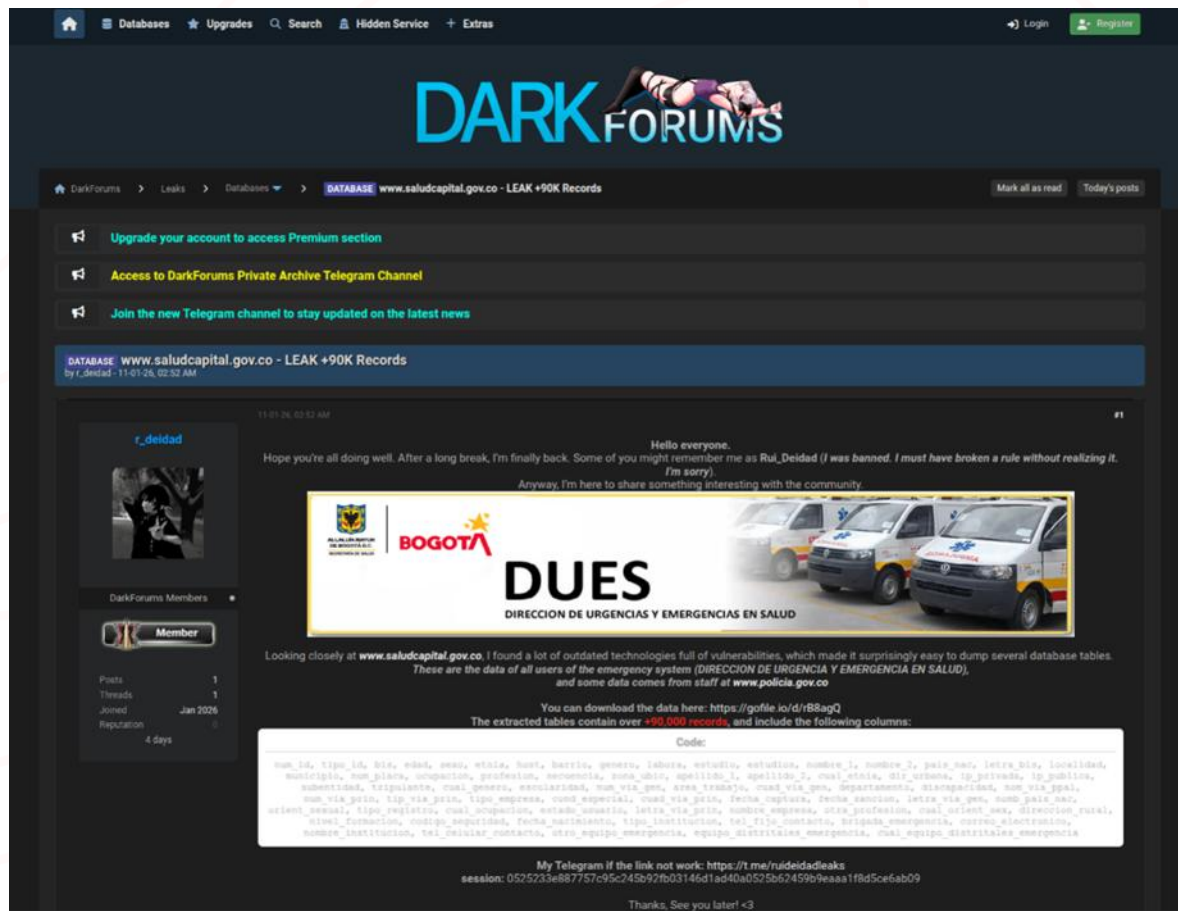
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454



Sin exponer detalles FalconFeeds ha traído de la Deep Web a la Web superficial la exposición.

<https://x.com/FalconFeeds/status/2010229363091091626>

Investigación de la información expuesta:

La información está publicada desde el 10/enero y se ha descargado 33 veces al 16/enero medio día.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

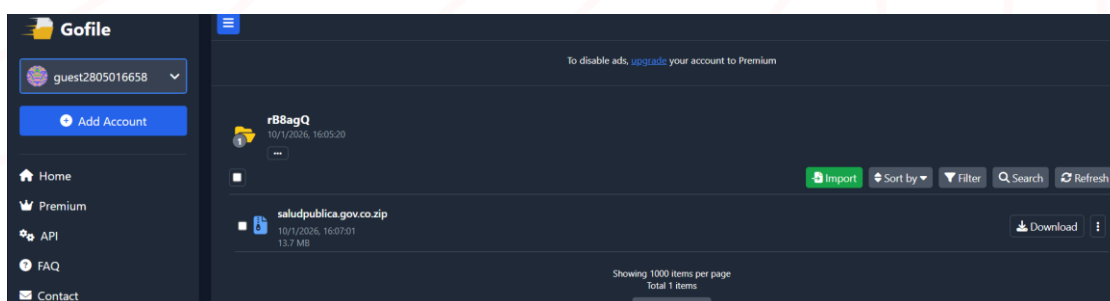
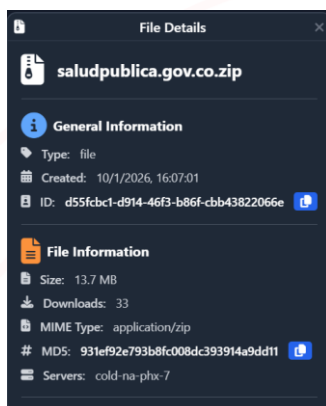
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454



El contenido son tres respaldos de base de datos

- usuarios_capacitados_final (19.100 Registros)
- usuarios-capacitados-2 (56.000 Registros)
- usuarios-capacitados-1 (16.800 Registros)

La base de datos “final” contiene datos de las otras dos, por los que aproximadamente hay +70.000 registros únicos con los siguientes atributos:

- | | | |
|---------------|--------------|----------------|
| • `num_id` ; | • `etnia` , | • `estudio` , |
| • `tipo_id` , | • `aprobo` , | • `estudios` , |
| • `bis` , | • `barrio` , | • `nombre_1` , |
| • `edad` , | • `genero` , | • `nombre_2` , |
| • `sexo` , | • `labora` , | • `pais_nac` , |



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

- `letra\_bis` ,
- `localidad` ,
- `municipio` ,
- `num\_placa` ,
- `ocupacion` ,
- `profesion` ,
- `secuencia` ,
- `zona\_ubic` ,
- `apellido\_1` ,
- `apellido\_2` ,
- `cual\_etnia` ,
- `dir\_urbana` ,
- `subentidad` ,
- `tripulante` ,
- `cual\_genero` ,
- `escolaridad` ,
- `fecha\_curso` ,
- `num\_via\_gen` ,
- `area\_trabajo` ,
- `cuad\_via\_gen` ,
- `departamento` ,
- `discapacidad` ,
- `nom\_via\_ppal` ,
- `nombre\_curso` ,
- `num\_via\_prin` ,
- `tip\_via\_prin` ,
- `tipo\_empresa` ,
- `cond\_especial` ,
- `cuad\_via\_prin` ,
- `fecha\_captura` ,
- `fecha\_sancion` ,
- `letra\_via\_gen` ,
- `nomb\_pais\_nac` ,
- `orient\_sexual` ,
- `cual\_ocupacion` ,
- `estado\_usuario` ,
- `fecha\_registro` ,
- `letra\_via\_prin` ,
- `nombre\_empresa` ,
- `otra\_profesion` ,
- `cual\_orient\_sex` ,
- `direccion\_rural` ,
- `nivel\_formacion` ,
- `usuario\_aprueba` ,
- `codigo\_seguridad` ,
- `fecha\_nacimiento` ,
- `intensidad\_horas` ,
- `tipo\_institucion` ,
- `tel\_fijo\_contacto` ,
- `brigada\_emergencia` ,
- `correo\_electronico` ,
- `nombre\_institucion` ,
- `tel\_celular\_contacto` ,
- `otro\_equipo\_emergencia` ,
- `equipo\_distritales\_emergencia` ,
- `cual\_equipo\_distritales\_emergencia` ,

Investigación de los servidores relacionados:

En la copia de la base de datos habla de MariaDB 10.19-11.8.3, for debian-linux, analizando el sitio web no se observa que lo proteja un WAF.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454



Firewall

Firewall	 No*
----------	---

*The domain may be protected with a proprietary or custom WAF which we were unable to identify automatically

Tampoco cuenta con las cabeceras del sitio web para limitar ataques de Cross Site Scripting, SQL Injection, Clickjacking,



HTTP Security

Content Security Policy	 No
Strict Transport Policy	 No
X-Content-Type-Options	 No
X-Frame-Options	 No
X-XSS-Protection	 No



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Security.Txt

Present

✗ No

Having a security.txt ensures security researchers know how and where to safely report vulnerabilities.

HSTS Check

HSTS Enabled?

✗ No

Site does not serve any HSTS headers.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

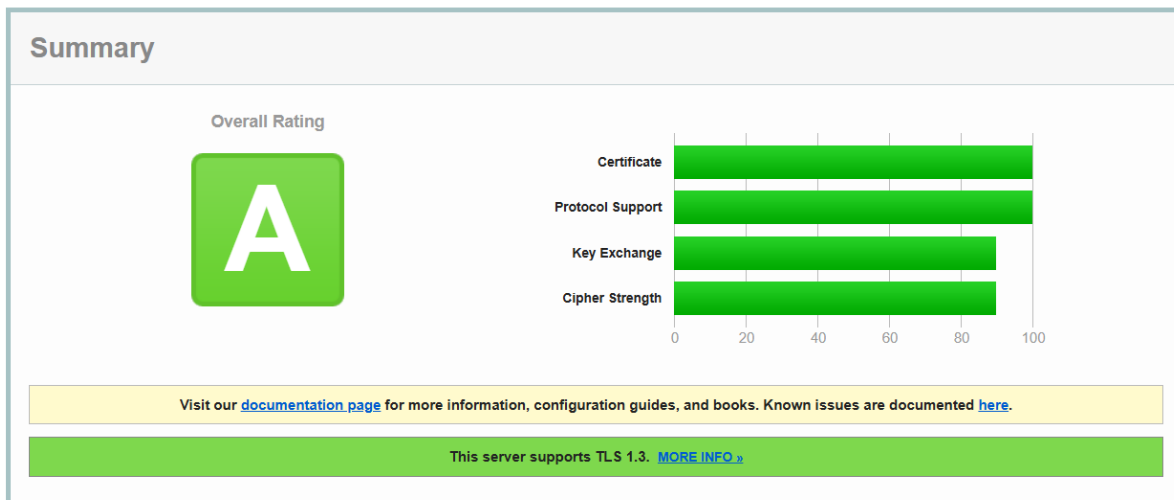
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

El certificado y TLS está bien configurado.

SSL Report: fappd.saludcapital.gov.co (172.212.113.140)

Assessed on: Fri, 16 Jan 2026 16:50:19 UTC | [Hide](#) | [Clear cache](#)

[Scan Another](#)



Observando la publicación se ve fuera de la infraestructura monitoreada por el GammaCSOC ya que aparentemente está en la nube de Azure, encontrando en el sitio “fappd” posee PHP, MySQL y el “www” aparentemente es ASP.NET o hasta un SharePoint como <https://www.saludcapital.gov.co/sitios/VigilanciaSaludPublica/Lists/Contactenos/DispForm.aspx?ID=2972663>

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
2	172.212.113.140	AS Autonomous System	8075 (MICROSOFT-CORP-MSN-AS-BLOCK)			
2	1					

403 Forbidden

Detected technologies

PHP (Programming languages)

Expand

Page Statistics

2	100 %	0 %	1	1
Requests	HTTPS	IPv6	Domains	Subdomains
1	1	1 kB	1 kB	0
IPs	Countries	Transfer	Size	Cookies



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

www.saludcapital.gov.co

4.255.85.26  **Public Scan**

Submitted URL: <http://www.saludcapital.gov.co/>

Effective URL: <https://www.saludcapital.gov.co/Paginas2/Inicio.aspx>

Submission: On January 16 via manual (January 16th 2026, 5:54:47 pm UTC) from  — Scanned from 

[Summary](#) [HTTP 175](#) [Redirects](#) [Links 50](#) [Behaviour](#) [Indicators](#) [Similar](#) [DNS](#)

Summary

This website contacted **22 IPs** in **3 countries** across **15 domains** to perform **175 HTTP transactions**. The main IP is **4.255.85.26**, located in **Washington, United States** and belongs to **MICROSOFT-CORP-MSN-AS-BLOCK, US**. The main domain is **www.saludcapital.gov.co**.
TLS certificate: Issued by **GeoTrust TLS RSA CA G1** on July 2nd 2025. Valid for: a year.

www.saludcapital.gov.co scanned **1867 times** on urlscan.io

[Show Scans 1867](#)

urlscan.io Verdict: No classification 

Live information

Current DNS A record: 4.255.85.26 (AS8075 - MICROSOFT-CORP-MSN-AS-BLOCK, US)

Investigando el actor malicioso:

No hay reputación, historial o datos relacionados a dicho actor, hay una consulta registrada que realizaron desde Canada sobre la publicación a los minutos de publicarla, lo que puede ser una confirmación del atacante validando su exposición como preservando un screenshot de su exposición.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

darkforums.io

185.178.208.154 

URL: <https://darkforums.io/Thread-DATABASE-www-saludcapital-gov-co-LEAK-90K-Records>

Submission: On January 14 via manual (January 14th 2026, 4:39:12 pm UTC) from  — Scanned from 

[Summary](#) [HTTP 26](#) [Redirects](#) [Links 7](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 2 IPs in 2 countries across 2 domains to perform 26 HTTP transactions. The main IP is 185.178.208.154, located in Russian Federation and belongs to DDOS-GUARD DDOS-GUARD LTD, RU. The main domain is darkforums.io. TLS certificate: Issued by R12 on December 22nd 2025. Valid for: 3 months.

darkforums.io scanned 14 times on urlscan.io

Show Scans 14

urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  No classification for darkforums.io

Current DNS A record: 185.178.208.154 (AS57724 - DDOS-GUARD DDOS-GUARD LTD, RU)

Domain created: December 21st 2025, 11:00:00 (UTC)

Domain registrar: NICENIC INTERNATIONAL GROUP CO., LIMITED

Domain & IP information

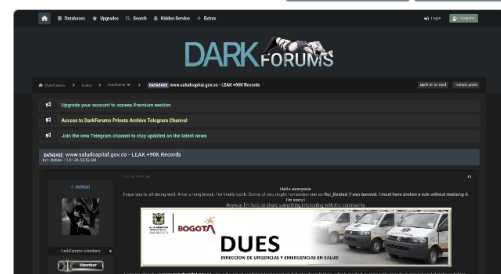
IP/ASNs [IP Detail](#) [Domains](#) [Domain Tree](#) [Links](#) [Certs](#) [Frames](#)

 IP Address [AS Autonomous System](#)

[Lookup](#) [Go To](#) [Rescan](#)
[Add Verdict](#) [Report](#)

Screenshot

[Live screenshot](#) [Full Image](#)



Page Title

www.saludcapital.gov.co - LEAK + 90K Records

Detected technologies

 jQuery (JavaScript libraries)

[Expand](#)

Page Statistics

Mesa de Crisis 2PM 16/ENE/2026

Contexto por los ingenieros sobre lo que se ha revisado y se hará.

Aplicativo afectado es el supuesto SIDCRUE de la Dirección de Urgencias y Emergencias | en Salud (DUES)

<https://fappd.saludcapital.gov.co/CRUE/>



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

- Aplicación legacy de hace 10 años.
- CRUE tiene permisos privilegiados para 8 usuarios con DELETE y muchas más.
- Hasta el 15/enero/2026 estaba activo el phpadmin
- Esta mañana se reunión con el secretario para plantear opción de bajar el sitio o restringir acceso
- 5pm Angela conversará con el secretario para tomar decisiones.
- 3pm secretario conversará con el equipo Desarrollo del aplicativo
- La Fiscalia ya fue avisa el día ayer 15/ene/2026 y se está trabajando en el reporte de la SIC.

Sobre el plan de trabajo se declararon las siguientes tareas y pendientes:

- 1) Tomar la postura de que existe un atacante al interior. @Bocanegra

EL 21/diciembre del 2025 pasó algo en el servidor involucrado según el BitDefender revisará si hay más situaciones parecidas en otros servidores



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Threats Xplorer

Ransomware*

Detenido en: 17 oct 2025 00:00 - 15 ene 2026 ... Categoría: Todos Acción realizada: Todos Nombre del endpoint: Q Tipo de amenaza: Todos IP: 10.237.0.133

Categoría	Detalles	Acción realizada	Nombre del endpoint	Detectado en	Usuario
Archivo	E:\xampp2\htdocs\cruel\PHP\genera1.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:59	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\PHP\genera4.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:59	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\PHP\generahword.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:59	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\OLD16122025\genera1.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:32	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\OLD16122025\generahword.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:32	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\OLD16122025\genera4.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:32	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\genera4.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 09:06	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\genera1.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:59	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BKE34KPs.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:48	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BKGU7LW\genera1.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:46	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BKGU7LW\generahword.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:46	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BKGU7LW\genera4.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:46	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BPAFCR.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:43	SYSTEM
Archivo	E:\\$RECYCLE.BIN\S-1-5-21-30088263-1664249155-3593176988-1003\BRTQWWh.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 07:41	SYSTEM
Archivo	E:\Bk_3\genera1.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 06:40	SYSTEM
Archivo	E:\Bk_3\generahword.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 06:40	SYSTEM
Archivo	E:\Bk_3\genera4.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 06:40	SYSTEM
Archivo	E:\xampp2\htdocs\cruel\generahword.php	Eliminados (1 veces)	SDSFAPP02	21 Dec 2025 03:10	SYSTEM

Volver arriba 18 elementos (número de ocurrencias: 18) CARGAR MÁS 250

2) Cambiar todos los controles de detección a respuesta. @Carlos

Se activa el WAF modo prevención, pendiente redireccionar todos los enlaces diferentes a <https://fappd.saludcapital.gov.co/CRUE/>

Ejemplo <https://fappd.saludcapital.gov.co/dashboard/> no debe ser accesible.

3) Validar si la información fugada si pertenece al servidor identificado. @GammaCSOC

Si, en la sesión se confirma que son bases de datos del servidor SDSFAPP02 de IP 10.237.0.133/27; el cuál es un aplicativo que tiene muchos años y a pesar de las advertencias de los ingenieros fue migrado así a Azure.

Afirmar que la información si es de ellos implica que el punto 11 relacionado con el reporte del incidente es fundamental.

El ingeniero Carlos comenta que había más datos que parece que hubieran recortado los datos.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

GammaCSOC revisará constante si hay nuevas publicaciones

4) Corregir las políticas de redes entre servidores para que solo pueda conectarse a lo estrictamente necesario. @Bocanegra y Carlos García

Bocanegra confirma que ese server SDSFAPP02 10.237.0.133/27, también reconocen que tienen permisos de acceso Cristóbal Zurita, Carlos Garcia y un tercer administrador, además un usuario genérico como usrtic724

Se evalúan los permisos:

Permisos de entrada están controlados

Filter by name							Port == all	Protocol == all	Source == all	Destination == all	Action == all
Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑					
☐ 100	AllowCidBlockCustom4Inbound	80,443	Any	10.237.1.192/27	Any	Allow					
☐ 110	AllowCidBlockCustom8Inbound	80	TCP	40.76.130.90	Any	Allow					
☐ 120	AllowTagHTTPInbound	80	TCP	AzureFrontDoorBackend	Any	Allow					
☐ 130	AllowCidBlockMySQLInbound2	3306	TCP	10.1.112.34,10.1.80.57,10.1.80.34,10.1.80.34	Any	Allow					
☐ 65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow					
☐ 65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow					
☐ 65500	DenyAllInbound	Any	Any	Any	Any	Deny					

Permisos salida

Search	Filter by name	Port == all	Protocol == all	Source == all	Destination == all	Action == all
Priority ↑	Name ↑	Port ↑	Protocol ↑	Source ↑	Destination ↑	Action ↑
☐ 65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
☐ 65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
☐ 65500	DenyAllOutbound	Any	Any	Any	Any	Deny

Quedan los pendientes Tarea crear política denegación de todo y permitir



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Restringir navegación del APP02 hacia internet @Carlos

Restringir conectividad del APP02 hacia on-premise @Bocanegra

5) Aplicar todas las recomendaciones y/o retroalimentación a los reportes del GammaCSOC.
@Angela

Definir un protocolo de comunicación para el fin de semana, por ahora será la siguiente mesa de crisis después de las reunión Angela y el secretario de las 5PM.

6) No apagues el servidor, instale las herramientas de monitoreo en todas las componentes relacionadas. @Zurita

@Zurita revisará y tomará las evidencias del servidor, programas instalados, archivos temporales, usuarios registrados, carpetas de usuarios.

@Zurita los que se loguearon alguna vez deben cambiar la credencial.

El servidor ya se le instaló el agente de Stellar Cyber y se pidió validen que tiene además del antivirus los demás controles.

7) Toma un *snapshot* de las máquinas involucradas inmediatamente. @Carlos García, @Jose Saquer

Carlos García backup azure

Jose Saquer, Feghali Jabr (JSFeghali@saludcapital.gov.co); validar catálogo de backup onpremise



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

8) Reemplace las credenciales de todos los usuarios y bases de datos relacionados en los servidores involucrados, ya que se debe suponer que se pudo hacer un volcado de memoria de los datos del servidor. @Cristobal Zurita

Bocanegra confirma que ese server SDSFAPP02 10.237.0.133/27, también reconocen que tienen permisos de acceso Cristóbal Zurita, Carlos Garcia y un tercer administrador, además un usuario genérico como usrtic724, el cual debe deshabilitarse y los administradores cambiar su credencial

9) Valide que el acceso a la base de datos solo se puede conectar desde un ambiente de red privada. @Luis

Se Cambiaron la clave de la aplicación a la base de datos de los 5 usuarios.

Compartir los privilegios específicos que tiene el usuario de la aplicación.

Se va a crear un permiso para solo ejecutar un SP y retirar tantos usuarios.

10) Disminuya los permisos del usuario de la aplicación en conexión con la base de datos. @Luis
Depende del punto 9.

11) Involucrar el área legal y comunicaciones para definir una postura frente a la información ya publicada, validando la normativa a la que debe aplicar a la entidad como: @Angela

Ley Estatutaria 1581 de 2012 (Ley General de Protección de Datos) y su Decreto Reglamentario 1377 de 2013.

Circular 005 de 2021 y normas sobre Historia Clínica Electrónica



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Ejemplo tomar un plan de acción:

- **Inmediato:** Documentar todo (fecha de detección, alcance, tipo de datos).
- **Antes de 15 días hábiles:** Radicar el informe en el RNBD de la SIC.
- **Estratégico:** Preparar comunicación a los pacientes (transparencia proactiva).

@Angela a las 5Pm tiene un punto de control.

12) Buscar servicios complementarios para identificar antelada mente estos riesgos digitales
@Angela

Futuramente hablar de lecciones aprendidas

13) Autorizar ejecutar un análisis de vulnerabilidades con los diferentes activos. @Angela
Angela define si aplica



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Mesa de Crisis 8AM 19/ENE/2026

No fue autorizado deshabilitar el sitio, se procede a validar el cumplimiento de las tareas.

Sobre el plan de trabajo se declararon las siguientes tareas y pendientes:

1) Tomar la postura de que existe un atacante al interior. @Bocanegra

Se revisaron los últimos 90 días de eventos en BitDefender, solo un server tuvo alertamientos que fue el de Moodle, también migrado a Azure y ya se le había enviado a la ingeniera Silvana, en el pasado se argumentó que los usuarios podían subir información y el BitDefender toma las acciones sobre los sospechosos.

2) Cambiar todos los controles de detección a respuesta. @Carlos Andrés Olarte

Se activa el WAF modo prevención, pendiente redireccionar todos los enlaces diferentes a <https://fappd.saludcapital.gov.co/CRUE/>

Ejemplo <https://fappd.saludcapital.gov.co/dashboard/> no debe ser accesible, Se evidencia la labor de ocultar todos los destinos dentro de la carpeta “dashboard”.

3) Validar si la información fugada si pertenece al servidor identificado. @GammaCSOC

GammaCSOC revisará constante si hay nuevas publicaciones, para el 18/enero no hubo nueva información.

4) Corregir las políticas de redes entre servidores para que solo pueda conectarse a lo estrictamente necesario. @Bocanegra y @Carlos

Juan Carlos Bocanegra confirma que el servidor SDSFAPP02 10.237.0.133/27, tiene los siguientes permisos o conexiones:

Restringir conectividad del APP02 hacia on-premise @Bocanegra

- Se revisó el tráfico y hacia el dominio en premisas está denegado por el puerto DNS



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

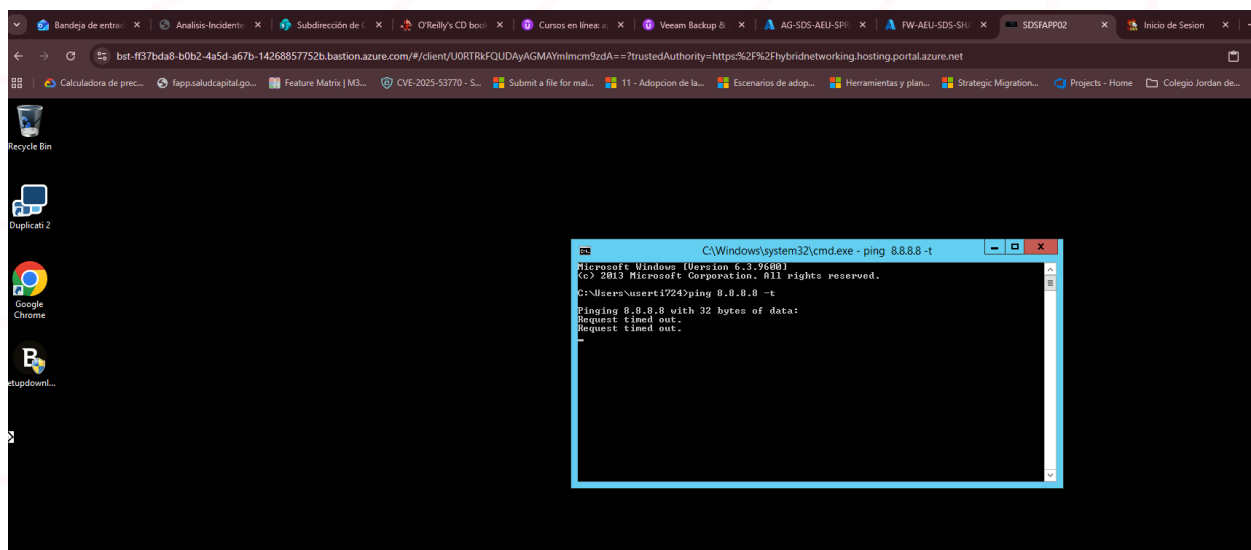
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

- Tiene un tráfico permitido hacia 172.16.0.38 SRSMTA (relay de correo - La política está permitiendo de Host a Host solo con el puerto SMTP), la cual se mantiene. (No hay comportamiento extraño, SPAM o anormales, explica Juan David Rey)
- Se requiere el tráfico desde el agente de Stellar Cyber al colector por los puertos TCP: 6640-6648, 8443, 8888, 8889
- Hacia el servidor está autorizado la comunicación MySQL (3306) solo desde los orígenes específicos como 10.1.112.34, 10.1.80.57, 10.1.80.34, 10...

Restringir navegación del APP02 hacia internet @Carlos

Se bloquea el acceso a internet del servidor



5) Aplicar todas las recomendaciones y/o retroalimentación a los reportes del GammaCSOC. @Angela

Durante el fin de semana hubo comunicación con Angela y no hubo incidentes .

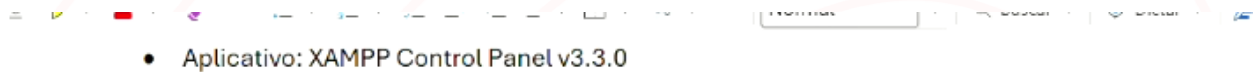


Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

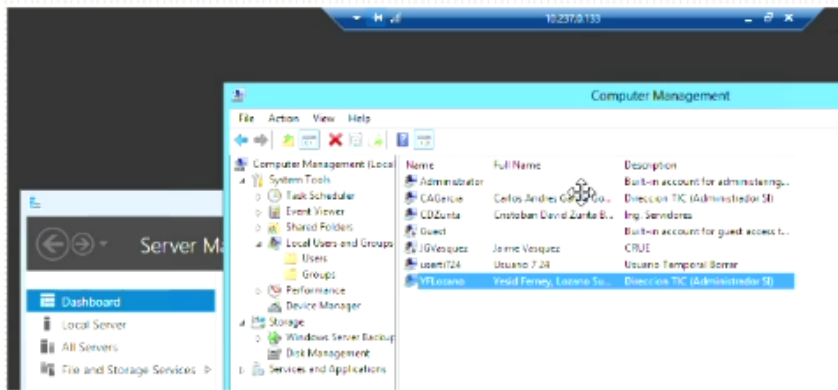
6) No apagues el servidor, instale las herramientas de monitoreo en todas las componentes relacionadas. @Zurita

Zurita levantó la información del servidor.



Acciones Tomada 16 de enero de 2025

Se cambia la contraseña y se deshabilitan de los siguientes usuarios locales en el Windows Server:



Estos son los usuarios que son administradores

7) Toma un *snapshot* de las máquinas involucradas inmediatamente. @Carlos García, @Jose Saquer

Carlos respaldos en Azure



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Start Date	End Date	Recovery point consistency	Recovery point type	Recovery point tags
09/01/2025	12/21/2025	All restore points	All restore points	All
Long term retention points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here				
CRASH CONSISTENT APPLICATION CONSISTENT FILE-SYSTEM CONSISTENT				
Time	Consistency	Recovery Type	Expiry time	Recent scan status
12/1/2025, 10:03:52 AM	Application Consistent	Vault-Standard	12/8/2026, 10:03:52 AM	Not available
10/27/2025, 10:09:33 AM	Application Consistent	Vault-Standard	11/3/2026, 3:09:33 PM	Not available
9/29/2025, 10:05:47 AM	Application Consistent	Vault-Standard	10/6/2026, 3:05:47 PM	Not available

SDSFAPP02 Backup				
Overview	Activity log	Access control (IAM)	Tags	Diagnose and solve problems
Resource visualizer	Connect	Networking	Settings	Availability + scale
Security	Backup + disaster recovery	Backup	Disaster recovery	Restore point
Operations	Monitoring	Automation	Help	
Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data Restore to Secondary Region Undo Feedback Alerts (in last 24 hours) View alerts Jobs (in last 24 hours) View jobs Source scan integration Not configured Latest restore point 1/17/2026, 10:03:52 AM (4 hours(s) ago) Included disk(s) All disks Source scan summary +				
Recovery points				
This list is filtered for last 30 days of recovery points. To recover from recovery point older than 30 days, as well as vault archive, click here.				
Long term recovery points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, click here.				
Creation time	Consistency	Recovery type	Expiry time	Recent scan status
1/19/2026, 10:10:55 AM	Application Consistent	Snapshot and Vault-Standard		Not available
1/19/2026, 2:20:14 AM	Application Consistent	Snapshot		Not available
1/18/2026, 6:25:33 PM	Application Consistent	Snapshot	1/23/2026, 6:25:33 PM	Not available
1/18/2026, 10:08:20 AM	Application Consistent	Snapshot and Vault-Standard		Not available
1/18/2026, 2:28:39 AM	Application Consistent	Snapshot	1/23/2026, 2:28:39 AM	Not available
1/17/2026, 6:23:17 PM	Application Consistent	Snapshot	1/23/2026, 6:23:17 PM	Not available
1/17/2026, 10:10:29 AM	Application Consistent	Snapshot and Vault-Standard	1/22/2026, 10:10:29 AM	Not available
1/17/2026, 2:17:44 AM	Application Consistent	Snapshot	1/22/2026, 2:17:44 AM	Not available
1/16/2026, 6:32:10 PM	Application Consistent	Snapshot	1/21/2026, 6:32:10 PM	Not available
1/16/2026, 4:28:54 PM	Crash Consistent	Snapshot and Vault-Standard	2/15/2026, 4:28:54 PM	Not available
1/16/2026, 10:04:44 AM	Application Consistent	Snapshot and Vault-Standard	1/21/2026, 10:04:44 AM	Not available
1/16/2026, 2:20:48 AM	Application Consistent	Snapshot	1/21/2026, 2:20:48 AM	Not available
1/15/2026, 6:24:31 PM	Application Consistent	Snapshot	1/20/2026, 6:24:31 PM	Not available
1/15/2026, 10:11:26 AM	Application Consistent	Snapshot and Vault-Standard	1/20/2026, 10:11:26 AM	Not available
1/15/2026, 2:19:20 AM	Application Consistent	Snapshot	1/20/2026, 2:19:20 AM	Not available
1/14/2026, 6:31:22 PM	Application Consistent	Snapshot	1/19/2026, 6:31:22 PM	Not available
1/14/2026, 10:06:12 AM	Application Consistent	Snapshot and Vault-Standard	1/19/2026, 10:06:12 AM	Not available
1/14/2026, 2:24:21 AM	Application Consistent	Snapshot	1/19/2026, 2:24:21 AM	Not available
1/13/2026, 10:12:18 AM	Application Consistent	Vault-Standard	1/20/2026, 10:12:18 AM	Not available
1/12/2026, 10:11:16 AM	Application Consistent	Vault-Standard	2/6/2026, 10:11:16 AM	Not available
1/5/2026, 10:05:51 AM	Application Consistent	Vault-Standard	2/2/2026, 10:05:51 AM	Not available
12/29/2025, 10:08:48 AM	Application Consistent	Vault-Standard	1/2/2031, 10:08:48 AM	Not available
12/22/2025, 10:09:04 AM	Application Consistent	Vault-Standard	1/18/2026, 10:09:04 AM	Not available

Jose Saquer, Feghali Jabr (JSFeghali@saludcapital.gov.co); validar catálogo de backup onpremise

8) Reemplace las credenciales de todos los usuarios y bases de datos relacionados en los servidores involucrados, ya que se debe suponer que se pudo hacer un volcado de memoria de los datos del servidor. @Cristobal Zurita

Todas las claves fueron reemplazadas, solo faltaría YFlozano que está de vacaciones.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

9) Valide que el acceso a la base de datos solo se puede conectar desde un ambiente de red privada. @Luis Gaitan

Hoy se les explica como funciona el SP a los usuarios y ya no tienen permisos, falta reconocer el nombre de los Workstation, esta labor se realizará con demás BD.

10) Disminuya los permisos del usuario de la aplicación en conexión con la base de datos. @Luis
Depende del punto 9.

11) Involucrar el área legal y comunicaciones para definir una postura frente a la información ya publicada, validando la normativa a la que debe aplicar a la entidad como: @Angela

Se está preparando el informe de la mejor manera con planeación institucional, contando con los 15 días hábiles que se tiene para el trámite.

12) Buscar servicios complementarios para identificar antelada mente estos riesgos digitales @Angela

Futuramente hablar de lecciones aprendidas

13) Autorizar ejecutar un análisis de vulnerabilidades con los diferentes activos. @Angela

Ya se tiene un Análisis de primer semestre del 2025 el cuál está en manos del equipo de desarrollo.

14) Instalar Agente Colector 10.232.5.12 – sds Moodle @Cristobal Zurita



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000
Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147
Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906
Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927
Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454

Instalar software de Stellar Cyber **10.232.5.12 – sds Moodle** y otros que Angela considere.



Bogotá | Calle 166 No. 20-45 | **PBX:** +5714076000

Cali | Carrera 18 No. 10-38 | **PBX:** +57 2 5574147

Barranquilla | Carrera 49c No. 75 - 47 | **PBX:** +57 2 5574147

Medellín | Calle 15 No. 35-1 Edificio C34 | **PBX** +57 4 3229906

Bucaramanga | Carrera 27 No. 37 - 33 Oficina 302 | **CEL** +57 3107692927

Eje Cafetero | Calle 4a No.19 - 33 Barrio Los Alcázares Manizales | **CEL** +57 3102233454