



Encuentro Nacional
de **JEFES** de

Tecnologías de la Información y las Comunicaciones

Oficina
de
Tecnologías de la
Información y las Comunicaciones.



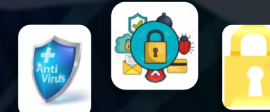
*Ciberdefensa Policial:
Más allá de un clic,
hacia la era de la
Confianza Cero*



INFRAESTRUCTURA



Análisis
bloqueo



Políticas Reglas
Antivirus



Red



Funcionarios



Amenaza interna



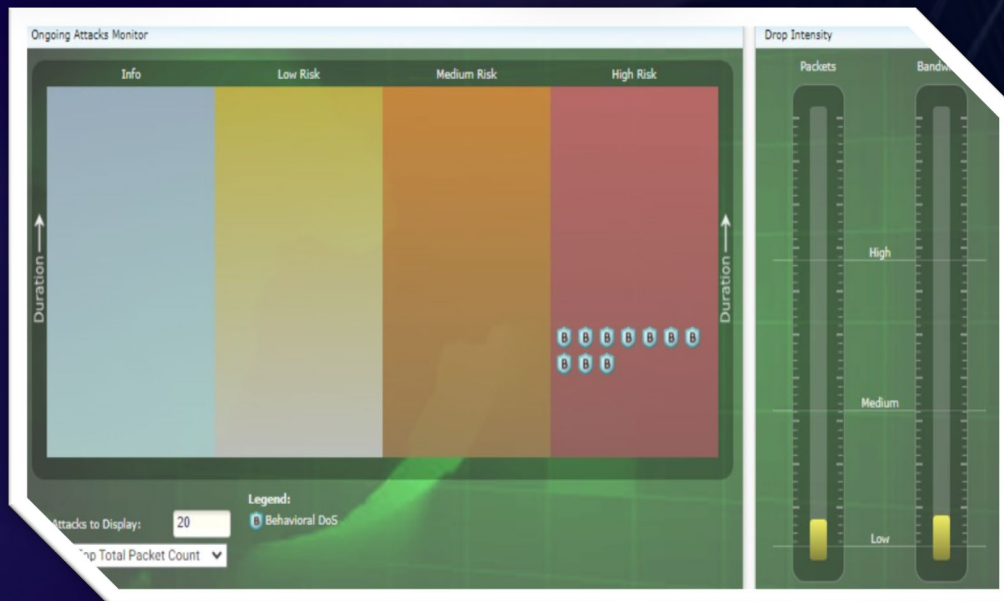
FIREWALL



Data center Principal



Data center
-alternativo



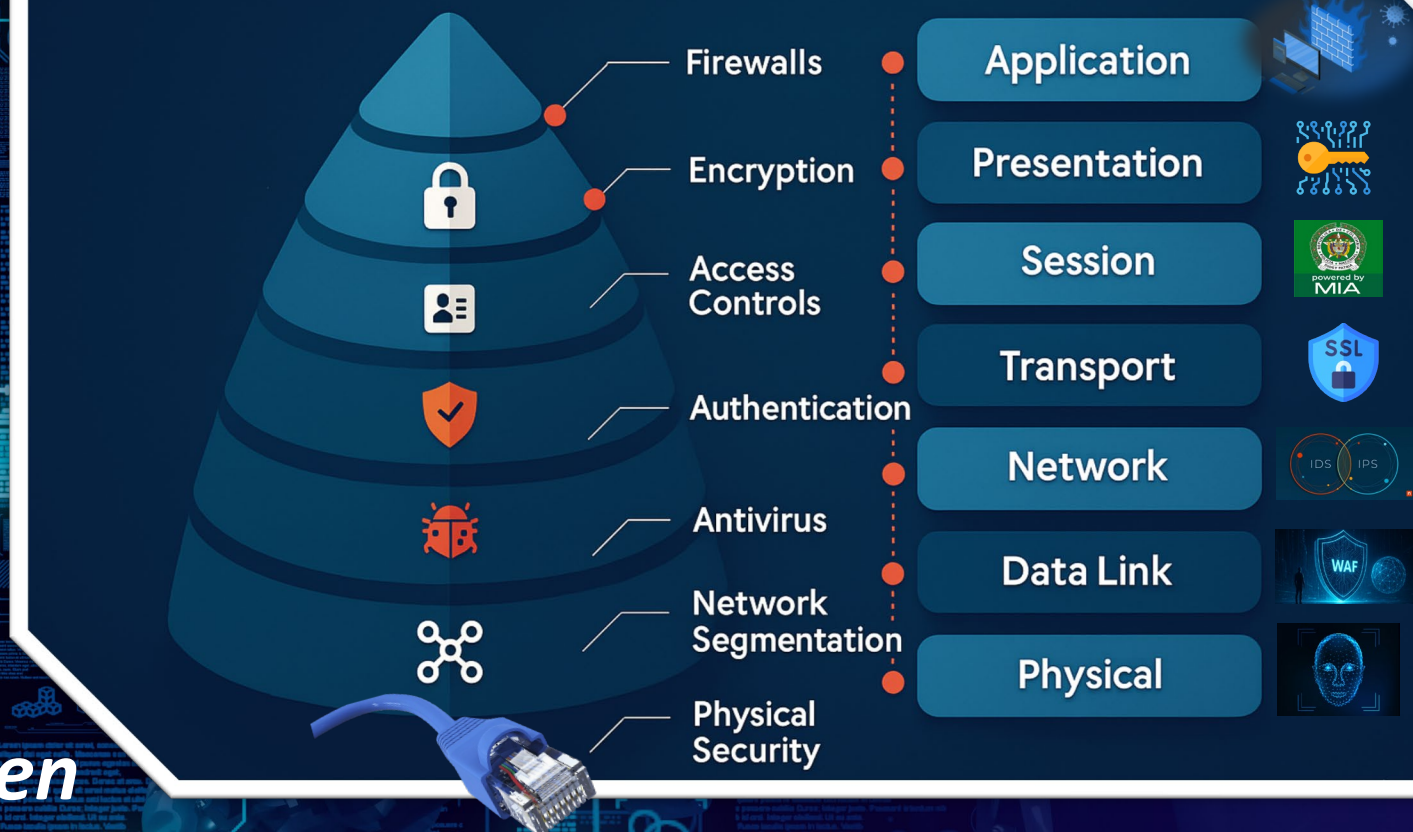


Encuentro Nacional
de JEFES de

Tecnologías de la Información y las Comunicaciones

Panorama de ciberseguridad en la Policía Nacional

DEFENSE IN DEPTH





Accesos remotos

TOP DE UNIDADES CON PERMISO DE VPN

Usuarios VPN

REGLAS

1. Se revoca si no se utiliza 45 días.
2. Si regresa de vacaciones se activa automáticamente.
3. No se solicita revocación.
4. Doble factor de autenticación.

1. DEANT: 1149
2. MEBOG: 923
3. DIJIN: 781
4. DIPRO: 729
5. DECUN: 614
6. DEVAL: 560
7. DEBOY: 536
8. DESAN: 508
9. DETOL: 388
10. MEBAR: 365
11. DENAR: 358
12. DIRAN: 353
13. DECAU: 348
14. MECAL: 299
15. DICAR: 270

TOTAL, VPN A LA FECHA:
14.005 Nivel País.





ZERO TRUST

Modelo de ciberseguridad basado en el principio de “nunca confiar, siempre verificar”.

8.809 contraseñas filtradas



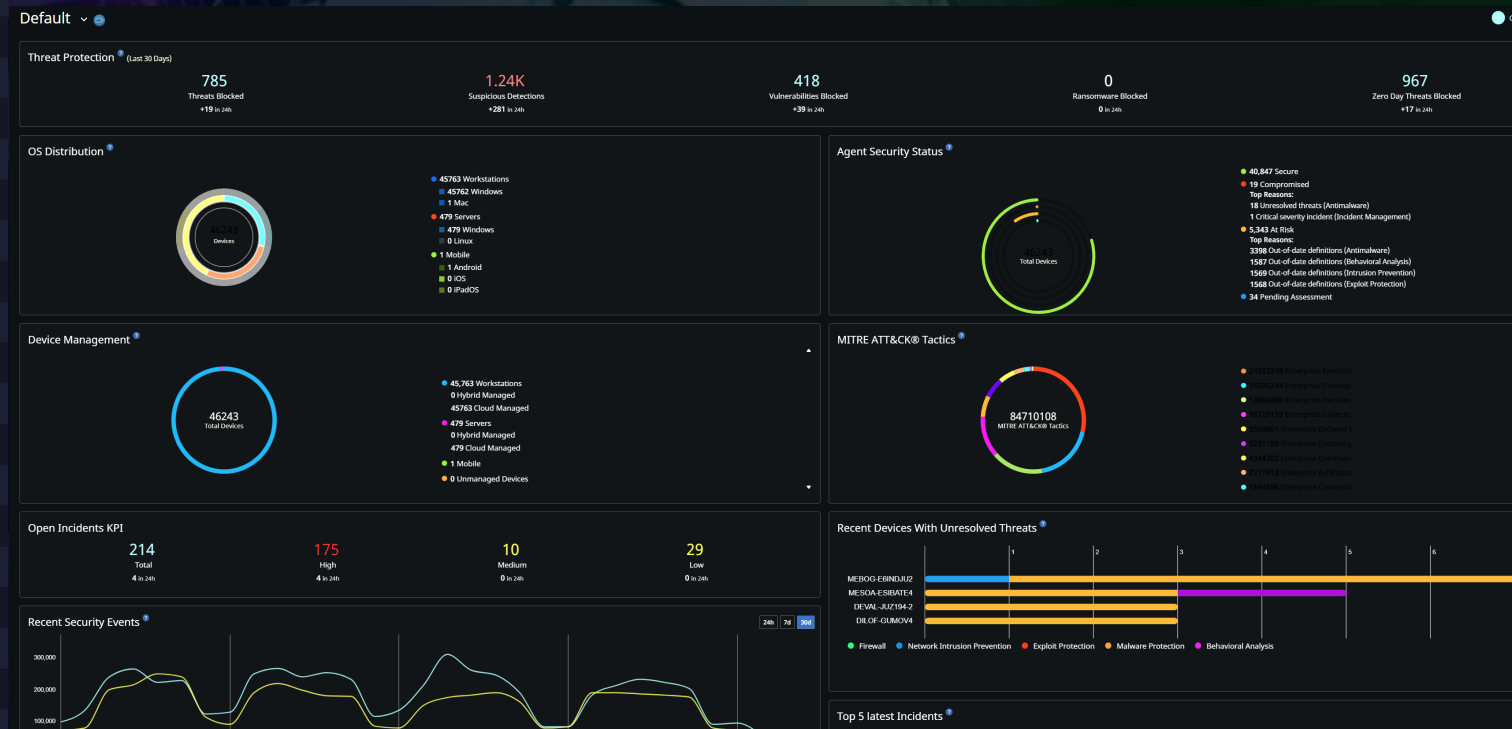
Este enfoque asume que ninguna persona, dispositivo o aplicación es confiable por defecto, incluso si está dentro de la red corporativa.





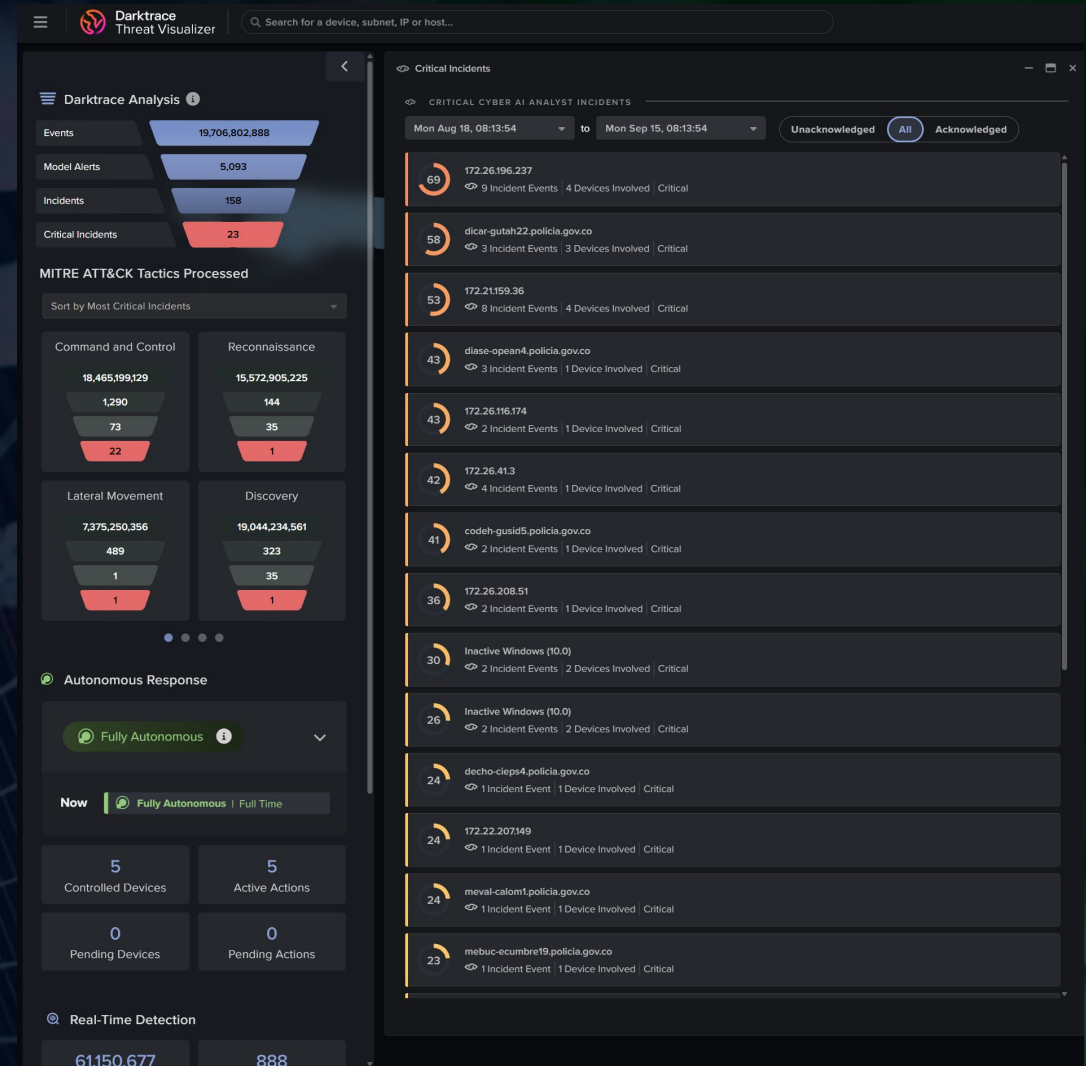
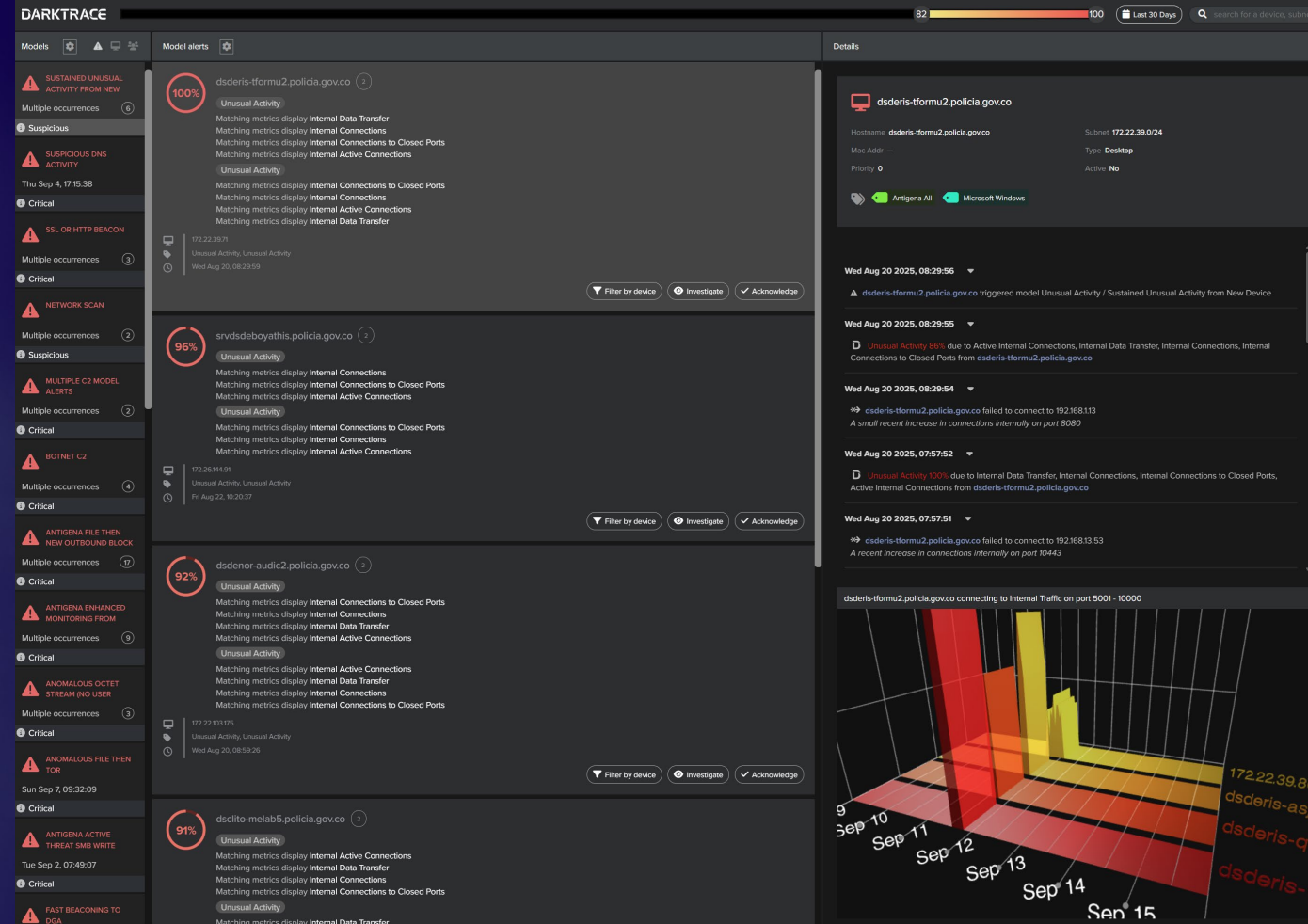
Escenarios de riesgo

Service URL	Account Login	Password	Pwd Policy Met?
https://sibis.policia.gov.co/DibieEnLineaUSF/Seguridad/Sesion	calpa	*****	No
https://educacion.policia.edu.co/	EDWI	Blanca2425	No
https://policia.edu.co/repoMultimediaDinae/VECO/99647_Diplomado...	Cristi	Policia2024..	Yes
https://educacion.policia.edu.co/	Cristi	Policia2024..	Yes
https://srvpsp.policia.gov.co:8443/Login.aspx	pedro	Tegen19356	No
https://calvirtual.policia.gov.co/registrar	djom	B@ltamora5	Yes
https://sgs.policia.gov.co:8080/PSS/	2728	Paramili99#	Yes
https://webescolar.policia.gov.co/escolar_ponal/Inicio.aspx	5205	fxyiue	No
https://webescolar.policia.gov.co/escolar_ponal/Inicio.aspx	5205	qfyepm	No
https://sibis.policia.gov.co/DibieEnLineaUSF/Seguridad/Sesion	ricar	*****	No
https://sinco.policia.gov.co/pnvp/zonapublica/Login.aspx	1004	457ebc2b-b	No
https://sibis.policia.gov.co/DibieEnLineaUSF/Seguridad/Sesion	yepat	*****	No
https://psi2.policia.gov.co:8443/PSI/	lisa.c	JacoboW2024++	Yes
https://psi.policia.gov.co/PSI/Login.aspx	lisa.c	JacoboW1944**	Yes
http://srvreservas.policia.gov.co:8888/ReservasDIBIE-war/faces/templa...	wilm	Ahmedowns/*8463	Yes
https://psi.policia.gov.co/PSI/Login.aspx	lisa.c	Jacobo1001/*-	Yes
https://sibis.policia.gov.co/DibieEnLineaUSF/Seguridad/Sesion	dellis	*****	No
https://psi.policia.gov.co/PSI/	sergi	Bienestar1986...	Yes
https://psi.policia.gov.co/PSI/Login.aspx	yerso	Capitan2024	No
https://psi2.policia.gov.co:8443/PSI/	lisa.c	Lacruz2025//	Yes
https://sinco.policia.gov.co/PNVP/zonapublica/login.aspx	1081	73f98d15-d	No
http://srvtabcore3.policia.gov.co/	ANDF	Raziel880108..	Yes
https://gepol.policia.gov.co/Gepol/	omar	Isabel2022..	Yes
https://svncpc.policia.gov.co/CNPC/Login.aspx	gt.pir	Colombia2025-+	Yes





Escenarios de riesgo



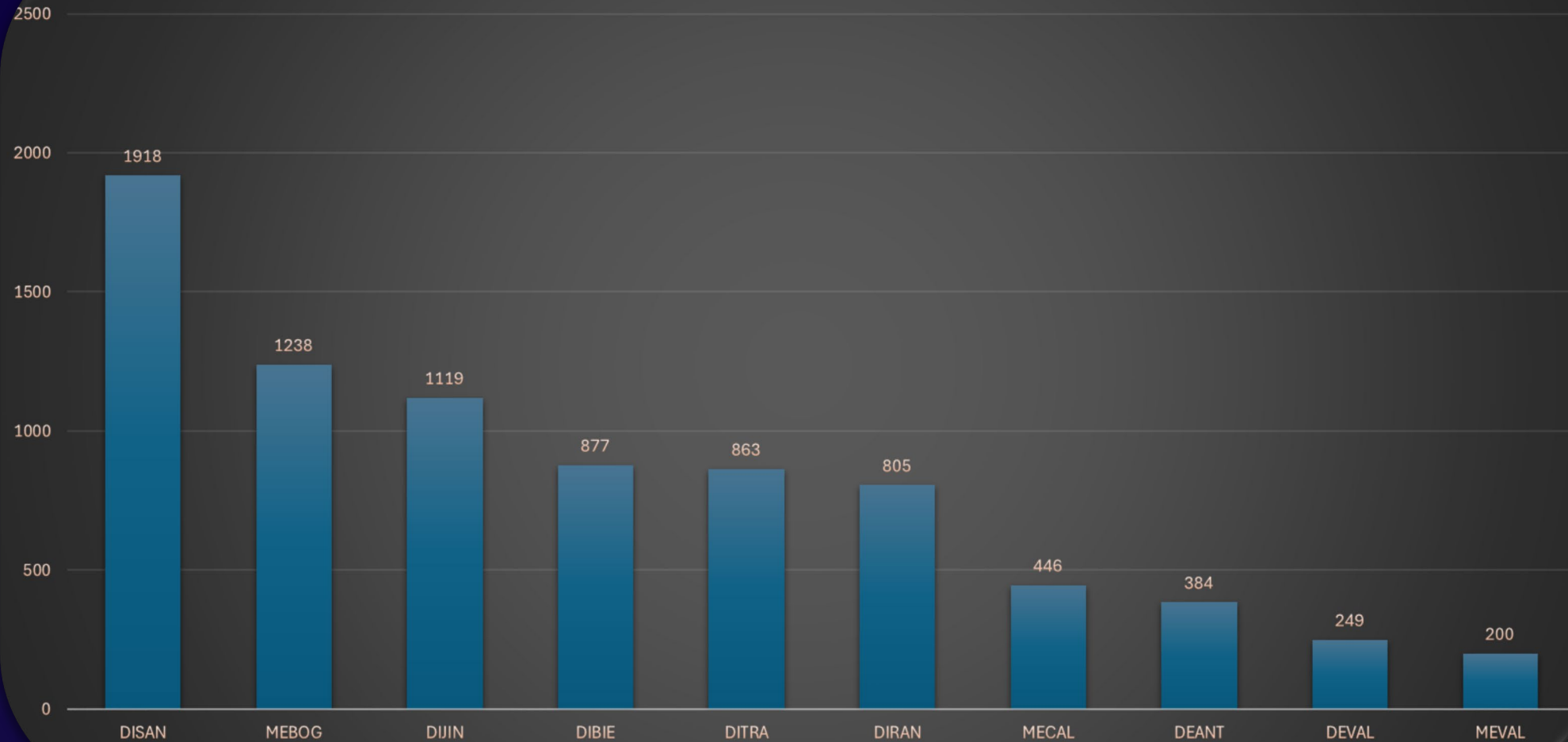
Herramienta de monitoreo en red





Escenarios de riesgo

ENDPOINT SIN ANTIVIRUS INSTITUCIONAL



REPORTE DE FECHA 10/09/2025





Amenazas por falta de actualización



213 equipos

3.093
vulnerabilidades
registradas



1.491 equipos

2.216
vulnerabilidades
registradas



27.511 equipos

3.022
vulnerabilidades
registradas



17.603 equipos

1.478
vulnerabilidades
registradas



49
323
222
295
278

win server 2008
win server 2012
win server 2016
win server 2019
win server 2022

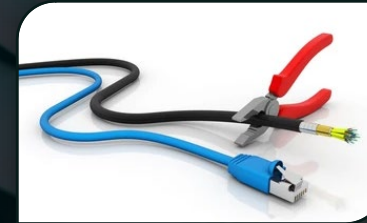




Incidentes de seguridad

Reporte de Incidente: por que cada incidente se genera lección aprendida.

QUE ES UN INCIDENTE?



Procedimiento IDT-PR-0004

Reporte al CSIRT



Plan de tratamiento

Lecciones aprendidas





Filtraciones de información

infobae

Trends Movilización Bogotá María Fernanda Cabal Miguel Uribe Turbay Política colombiana Abastecido de la Esplanada

COLOMBIA >

Habrà fuerte restructuraci3n en la Polic3a Nacional: ser3n trasladados 19 altos mandos en el pa3s

La reorganizaci3n policial incluye rotaciones de oficiales, ascensos estrat3gicos y designaciones en ciudades con mayor violencia urbana, en respuesta a la creciente preocupaci3n por la seguridad ciudadana en todo el pa3s

Traslados Poligramas Comunicados

MINISTERIO DE DEFENSA NACIONAL					
POLICIA NACIONAL					
DIRECCION DE TALENTO HUMANO					
TRASLADOS OFICIALES SUPERIORES PENDIENTES POR RADICAR EN M.D.N.					
Nº	FOTO	GR	APELLIDOS Y NOMBRES	UNIDAD ACTUAL	UNIDAD AUTORIZADA
1		BO	BELLO CUBIOS JERRY VESIO	MERICU	MERICU
2		BO	QUINTERO SALAZAR WILLIAM	MERICU	MERICU
3		BO	OVIEDO LAMPREA CARLOS GERMÁN	MERICU	DIJAR
4		BO	SERPA RUSTAMANTE ANDRÉS FERNANDO	DEGUN	JESEP
5		OR	OJEDA ERASO LUISMIGUEL FABIÁN	DEPARTAMENTO DE TOLIMA	LA METROPOLITANA DE CUCUTA
6		OR	PUELAGÁN GARCÍA CARLOS EFREN	DEPARTAMENTO DE SANTANDER	LA METROPOLITANA DE TOLIMA
7		OR	ROLDÁN MELO PUERTO	JESEP	Comandante Departamento de Calles
8		OR	EMBROSÁ MOLANO FREY YAMIR	DEPARTAMENTO DE BOYACÁ	DEPARTAMENTO DE BOLÍVAR
9		OR	JOHN FREY ZAMBRANO LÓPEZ	MEDIOY	METROPOLITANA DE BOGOTÁ
10		OR	LÓPEZ DUQUE SANDRA BIBIANA	METROPOLITANA DE COCAJANA	DIRECTOR (A) ESCUELA ECAJAN

Nº	FOTO	GR	APELLIDOS Y NOMBRES	UNIDAD ACTUAL	UNIDAD AUTORIZADA	ACTO ADMINISTRATIVO
11		PO	GERMAN ALFONSO VARRIQUE	MERICU	METROPOLITANA DE BOGOTÁ	
12		PO	PINEDA LUIS ENRIQUE	MERICU	METROPOLITANA DE BOGOTÁ	

PO-2025-001051-JESEP

MINISTERIO DE DEFENSA NACIONAL
POLICIA NACIONAL
JEFATURA NACIONAL DE SERVICIO DE POLICIA
CENTRO DE ANALITICA DEL SERVICIO DE POLICIA

Origen: JESEP-CEPOL-14.19
Procedencia: JESEP
Destinatario: PAIS
Asunto: MEDIDAS DE SEGURIDAD PERSONAL, OPERACIONAL Y DE INSTALACIONES.

SIGUIENDO INSTRUCCIONES DEL SEÑOR BRIGADIER GENERAL WHARLINTON IVÁN GUALDRÓN GUALDRÓN JEFE NACIONAL DEL SERVICIO DE POLICIA EN ATENCION A LOS HECHOS OCURRIDOS EL DÍA DE HOY JUEVES 21/08/2025 EN DIFERENTES ZONAS DEL PAÍS Y TENIENDO EN CUENTA EL COMANDANTE DE REGION, METROPOLITANAS, DEPARTAMENTOS DE POLICIA Y DIRECTORES DE ESCUELAS DE FORMACIÓN, IMPARTIR AMPLIA INSTRUCCIONAL AL PERSONAL BAJO SU MANDO SOBRE **EXTREMAR MEDIDAS DE SEGURIDAD PERSONAL, OPERACIONAL Y DE INSTALACIONES**, COMO LA PROTECCIÓN DE BIENES ESTRATÉGICOS DE LA NACIÓN, ESTO CON EL FIN DE PREVENIR HECHOS TERRORISTAS QUE AFECTEN LA CONVIVENCIA Y SEGURIDAD CIUDADANA.

ES NECESARIO ADOPTAR MEDIDAS DE SEGURIDAD PERSONAL, OPERACIONAL Y DE INSTALACIONES, ASÍ:

- FORTALECER LOS REGISTROS A VEHÍCULOS, PAQUETES, ENCOMIENDAS U OTRO MEDIO, POR EL CUAL SE PUEDA MATERIALIZAR UN HECHO DE AFECTACIÓN A LA INTEGRIDAD DE LOS FUNCIONARIOS, INSTALACIONES POLICIALES Y POBLACION EN GENERAL.
- FORTALECER LOS PROTOCOLOS DE SEGURIDAD FRENTE AL INGRESO DE PERSONAS Y VEHÍCULOS (TANTO PARTICULARES COMO INSTITUCIONALES), AL INGRESO A LAS INSTALACIONES POLICIALES.
- ORGANIZAR PATRULLAJES TANTO INTERNOS COMO EXTERNOS, A INTERVALOS Y EN HORARIOS ESTRATÉGICOS, LA PROGRAMACIÓN DE ESTOS PATRULLAJES DEBE SER VARIABLE PARA EVITAR PATRONES PREDECIBLES Y FORTALECER LA COBERTURA DE SEGURIDAD EN TODOS LOS MOMENTOS.
- EXTREMAR LAS MEDIDAS DE SEGURIDAD EN LOS DESPLAZAMIENTOS, MINIMIZANDO LOS RIESGOS.
- EVITAR FORMACIONES ANTES, DURANTE Y DESPUÉS DE LOS SERVICIOS, EN LUGARES AJENOS A LAS UNIDADES POLICIALES.
- SUPERVISIÓN Y CONTROL DE LOS ELEMENTOS DEL SERVICIO TALES COMO (CASCO, CHALECO BALÍSTICO, ARMA DE DOTACIÓN, TONFA, ESPOSAS, ARMAS DE LETALIDAD REDUCIDA, RADIO DE COMUNICACIÓN Y PDA, ENTRE OTROS).
- DESPLIEGAR ACTIVIDADES DE SUPERVISIÓN Y CONTROL CON EL PERSONAL EN SERVICIO, PARA EVITAR COMPORTAMIENTOS INADECUADOS TALES COMO EL USO DE ELEMENTOS DISTRACTORES, QUE AMENACEN LA SEGURIDAD PERSONAL Y DE LAS INSTALACIONES.
- ADELANTE LAS COORDINACIONES CON UNIDADES MILITARES EN TERRITORIO.

ESTAS ACCIONES TAMBIÉN SE PODRÍAN MATERIALIZAR MEDIANTE LAS MODALIDADES DE ADECUACIÓN, ACTIVACIÓN O LANZAMIENTO DE ARTEFACTOS EXPLOSIVOS, AFECTACIÓN A INFRAESTRUCTURAS, HOSTIGAMIENTO, ATAQUE A PATRULLA, HOMICIDIOS, OBSERVACIÓN CRIMINAL

PO-2025-001052-JESEP

MINISTERIO DE DEFENSA NACIONAL
POLICIA NACIONAL
JEFATURA NACIONAL DE SERVICIO DE POLICIA
CENTRO DE ANALITICA DEL SERVICIO DE POLICIA

Origen: JESEP-CEPOL-14.19
Procedencia: JESEP
Destinatario: PAIS
Asunto: ALISTAMIENTO DE PRIMER GRADO PAIS

SIGUIENDO INSTRUCCIONES DEL SEÑOR BRIGADIER GENERAL ARNALDO ROSÉNBERG NOVOA PINERO SUBDIRECTOR GENERAL POLICIA NACIONAL, EN ATENCION A LOS HECHOS OCURRIDOS EL DÍA DE HOY JUEVES 21/08/2025 EN DIFERENTES ZONAS DEL PAÍS, DE MANERA ATENTA ME PERMITO INFORMAR A LOS SEÑORES JEFES NACIONALES, JEFES DE OFICINAS, ASESORES Y DE CONTROL, DIRECTORES, COMANDANTES DE REGION, METROPOLITANAS, DEPARTAMENTOS DE POLICIA, Y DIRECTORES DE ESCUELAS DE FORMACIÓN, A PARTIR DEL MOMENTO INICIA ALISTAMIENTO DE PRIMER GRADO **HASTA NUEVA ORDEN**.

Firmado digitalmente por Norberto Caballero Fernando Martínez Vargas
Cargo: Responsable Centro de Analitica Del Servicio De Policia
Cedula: 10966300
Titulo: Administrador Policial
Dependencia: Centro De Analitica Del Servicio De Policia
Unidad: Jefatura Nacional De Servicio De Policia
Correo: norberto.martinez@serpol.gov.co
21/08/2025 6:16:39 p.m.

ORDEN PERMANENTE
GS-2025-006323-OFTIC





Ciberataque a la Justicia Penal Militar y Policial

El 15 de junio de 2025, la Unidad Administrativa Especial de la Justicia Penal Militar y Policial fue blanco de un ciberataque tipo **ransomware Gunra**.

El ransomware utilizado cifró la información y dejó notas de rescate denominadas **"R3ADM3.txt"**, que es un indicio característico del grupo atacante.





GRACIAS