Recepción documentos para pago a contratistas y/o proveedores del MHCP

Número de Radicado	Fecha de Radicado	Fecha de Presentación
1-2024-048528	30/05/2024 09:25	30/05/2024 09:25

Información del contratista del MHCP

º Tipo Documento : **NIT** º Identificación del Contratista : **901778397 6**

º Nombre del Contratista : **CONSORCIO MNEMO SOC-MHCP**

º Correo Electrónico donde desea recibir la respuesta : **asistencia.contable@mnemo.com**

º Digite su correo nuevamente : **asistencia.contable@mnemo.com**

Recepción Documentos para pago

º ¿Es usted obligado a facturar? : **SI**

º Nro. Factura : **FE-6** º Fecha Factura : **14/05/2024**

º Nro. Contrato Ejemplo 3.435-2020** : **3.471-2023**

º Concepto de cobro : **Monitoreo,Diagnóstico,Generación de Alertas y recomendaciones,Servicios de gestión y análisis de vul**

º Nombre del Supervisor en el Ministerio de Hacienda : **LUIS ORLANDO ARENAS** º Tipo de contratista : **Persona Jurídica**

[X] Mención Legal: La responsabilidad por la recolección, entrega y validez de la información requerida es responsabilidad exclusiva del Contratista

Expone / Solicita

Observaciones

Presentación electrónica del Trámite Recepción documentos para pago a contratistas y/o proveedores del MHCP

Asunto

Documento: 901778397 6 - Nombre del Contratista: CONSORCIO MNEMO SOC-MHCP - Nro. contrato: 3.471-2023 - Concepto cobro: Monitoreo,Diagnóstico,Generación de Alertas y recomendaciones,Servicios de gestión y análisis de vul - Supervisor Contrato: LUIS O

Casos seleccionados

º Si usted es PERSONA JURÍDICA y SI está obligado a facturar:

Documentos requeridos adjuntados

º 01. Evidencia solicitud de pago SECOP II (Archivo en PDF): Documento adjuntado 01.Pantallazo del Secop II.pdf

Identificador: rsokuI5EIFtSq0ITPgszImpKVdg=

º 02. Cumplido para pago (Archivo en PDF): Documento adjuntado 02.CUMPLIDO N. 5 CONSORCIO MNEMO SOC-MHCP.pdf

Identificador: ev7wc9dV5JE8lUfAVwgDzfcY/5A=

º 03. Informe de Ejecución o acta de entrega (Archivo en PDF): Documento adjuntado 03.SOC Informe de Ejecución y Supervisión de Contrato 3.471-2023 - Abril - V2.pdf

Identificador: V09p0koDafos/jGjF7sydD4FdEE=

º 04. Representación gráfica de la factura (Archivo en PDF): Documento adjuntado 04.Factura FE-6.pdf

Identificador: rnhHmWeifBepbbQ6qAf0pCmldMY=

º 05.Certificado pago de seguridad social (Archivo en PDF): Documento adjuntado 05.Certificado y pagos de seguridad de social.pdf

Identificador: zS6VbRRzpONQ8ukE43Gzax/FMUI=

Documentos requeridos opcionales adjuntados

º 06. Informe final de actividades (Archivo en PDF): Documento adjuntado 06.Informe finales de Actividades.pdf

Identificador: NAdsoHJA5I0hjHtOOb6ZxHr7Yjs=

Avisos legales

Datos Personales

En cumplimiento a la Ley 1581 de 2012, informamos que los datos aquí tratados serán debidamente protegidos según nuestra política de tratamiento de datos personales, la cual podrá consultar en http://www.minhacienda.gov.co sección Transparencia, Atención y Servicios a la ciudadanía, Información para Grupos de Interés Específicos, Políticas e Información de Interés (Política de Tratamiento de Datos Personales 2022).Cualquier inquietud o solicitud puede escribir al correo relacionciudadano@minhacienda.gov.co

Apo.4.1.Fr.002 Cumplido para Pago

Codigo:	Apo.4.1.Fr002	Fecha	31/01/2023	Versiòn	6

CONS **5**

PARA: SUBDIRECCION FINANCIERA Y GRUPO DE CONTRATOS RADICADO No.: CP -

DATOS GENERALES DEL CONTRATO

CONTRATO, ORDEN O CONVENIO No. **3** . **471** - **2023**

NIT O DOCUMENTO DE IDENTIFICACION DEL CONTRATISTA 901778397

OBJETO DEL CONTRATO, ORDEN O CONVENIO: CONTRATAR LOS SERVICIOS DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA EL MONITOREO, ALERTAMIENTO Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LA PLATAFORMA TECNOLÓGICA DEL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

No.Compromiso 179823

FECHA DE SUSCRIPCION DEL CONTRATO, ORDEN O CONVENIO 11/12/2023

NOMBRE CONTRATISTA CONSORCIO MNEMO SOC-MHCP

SALDO 1,978,136,431.00

VALOR DEL CONTRATO 2,313,205,920.00

VALOR ADICIONES .00

FECHA DE INICIO: 19/12/2023

FECHA DE TERMINACION: 31/10/2025

VALOR PAGADO: 335,069,489.00 **VALOR PENDIENTE POR EJECUTAR:** 1,978,136,431.00 **% EJECUCIÒN:** 14

DATOS ESPECIFICOS DEL PAGO

Tipo de Pago	No.	Condicion de Pago	Aclaracion del	Valor.Pago	Iva Aplicado	Valor Iva	Amortizacion Anticipada	Total a Pagar
FACTURA NO.	FE 6	CONDICION DE PAGO	MONITOREO DIAGNÓSTICO GENERACIÓN DE ALERTAS Y ECOMENDACIONES ABRIL 2024	74,749,495.80	19 %	14,202,404.20		88,951,900.00
FACTURA NO.	FE 6	CONDICION DE PAGO	SERVICIOS DE GESTIÓN Y ANÁLISIS DE VULNERABILIDADES ABRIL 2024	2,508,067.23	19 %	476,532.77		2,984,600.00
			TOTALES	77,257,563.03		14,678,936.97		

TOTAL A PAGAR 91,936,500.00

Anexos y No. de Folios

Factura	1	Cuenta de Cobro		Declaracion juramentada Seguridad Social	
Otros Anexos o Folios	68	Entrada a Almacen		Constancias de pago de la seguridad social	10
				Total de Folios Anexos	79

En calidad de Supervisor/Interventor del contrato enunciado, certifico que he verificado el cumplimiento a satisfaccion de las obligaciones que emanan del contrato, la acreditacion del pago de obligaciones con el sistema de seguridad social integral y las cifras y valores corresondientes al periodo certificado para el reconocimiento del pago que por este instrumento se acredita

SUPERVISORES Y/O INTERVENTORES

FIRMA: Firmado digitalmente por Luis Orlando Arenas Ruiz

NOMBRE: LUIS ORLANDO ARENAS RUIZ
CARGO: ASESOR
CEDULA: 79398357

CONSORCIO MNEMO SOC-MHCP
NIT 901.778.397-6
CALLE 99 10 19
Tel: (601) 5527210
Bogotá - Colombia
contadorjunior@mnemo.com

Factura electrónica de venta
No. FE 6

Señores	MINISTERIO DE HACIENDA Y CREDITO PUBLICO		
NIT	899.999.090-2	**Teléfono**	(601) 3811700 - Ext. 000
Dirección	Cra 8 6C 38	**Ciudad**	Bogotá - Colombia

Fecha y hora Factura	
Generación	14/05/2024, 08:51
Expedición	14/05/2024, 08:51
Vencimiento	13/06/2024

Ítem	Descripción	Cantidad	Vr. Total
1	Monitoreo,Diagnóstico,Generación de Alertas y recomendaciones. Contrato: 3.471-2023 Periodo de facturación:01/04/2024 al 30/04/2024.	1.00	88,951,900.00
2	Servicios de gestión y análisis de vulnerabilidades. Contrato: 3.471-2023 Periodo de facturación:01/04/2024 al 30/04/2024.	1.00	2,984,600.00

Total items: 2

Valor en Letras:
Noventa y un millones novecientos treinta y seis mil quinientos pesos m/cte

Condiciones de Pago:
Crédito - Cuota No. 001 vence el 2024-06-13 por $ 91,936,500.00

Total Bruto	77,257,563.03
IVA 19%	14,678,936.97
Total a Pagar	**91,936,500.00**

Observaciones:
#$13-01-01-000;13.471-2023;Luis.Arenas@minhacienda.gov.co#$

Distribución del ingreso:
Mnemo Colombia S.A.S. 99% NIT 900.396.176-1 Contribuyente
Mnemo Evolution & integration Service SA 1% NIT:901.306.687-2 Contribuyente

A esta factura de venta aplican las normas relativas a la letra de cambio (artículo 5 Ley 1231 de 2008). Con esta el Comprador declara haber recibido real y materialmente las mercancías o prestación de servicios descritos en este título - Valor. **Número Autorización Electrónica 18764061385993 aprobado en 20231205 prefijo FE desde el número 1 al 5000 Vigencia: 12 Meses Meses**
Responsable de IVA - Actividad Económica 6201 Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas) Tarifa 9.66
CUFE: 6a550a3594e08196954ca43fc36de132e5e8f16a8680133e08ecdb336bd58526e247ad5121889557b41f4d4cbf372b8e

Fabricante Software y Proveedor tecnológico: Siigo SAS - Nit 830.048.145-8. Nombre Software: Siigo Nube. Firma electrónica: ver en el XML

CONTENIDO DEL INFORME

1. Condiciones del Contrato 1
2. Objeto del Contrato..... 1
3. Obligaciones del Contrato, Actividades Ejecutadas y Productos Entregados 1

1. CONDICIONES DEL CONTRATO

Número de Contrato: **3.471 - 2023**
Nombre del Contratista: **CONSORCIO MNEMO SOC-MHCP**
Periodo informe: **Abril de 2024**
Supervisor: **Luis Orlando Arenas**
Área perteneciente: **Dirección de Tecnología - MHCP**

2. OBJETO DEL CONTRATO

Contratar los servicios de un Centro de Operaciones de Seguridad (SOC) para el monitoreo, alertamiento y gestión de la seguridad de la información de la plataforma tecnológica del Ministerio de Hacienda y Crédito Público.

3. OBLIGACIONES DEL CONTRATO, ACTIVIDADES EJECUTADAS Y PRODUCTOS ENTREGADOS

Las obligaciones adquiridas son las siguientes:

1. Actividades del Servicio Avance: Las actividades anteriormente descritas se desarrollaron satisfactoriamente quedando pendiente otras actividades

Productos del contrato

Las siguientes actividades fueron realizadas:

- Envió de alertas tempranas y preventivas para el servicio de CTI, SOC y Ejecución de análisis de vulnerabilidades y envió de informes técnicos y ejecutivos.
- vigilancia digital del mes de abril de 2024.
- Envió de los informes mensuales de abril para CTI, SOC y vigilancia digital.
- Implementación de plataforma de Análisis de Vulnerabilidades y SIEM
- Configuración de 32 casos de uso en el SIEM por parte de Mnemo
- Generación de credenciales en Cyberdefense para Hasbleidy Diaz, Fabio Ricardo Cardozo y restablecimiento de las credenciales para Luis Arenas y Jaime Molina.
- Capacitaciones en servicio de vigilancia digital.
- Ejecución de tercer análisis forense.

Las siguientes actividades se encuentran en ejecución al corte de abril:

- Configuración de permisos de red por parte de administradores de equipos de seguridad perimetral de MHCP para ejecutar los análisis de vulnerabilidades.
- Aprobación por parte del comité de seguridad de MHPC para instalar winwollect en el directorio activo para la integración con el SIEM.
- Definición por parte de MHCP de equipos que realmente se deben integrar con el SIEM.
- Sesiones semanales de afinamiento técnico.
- Sesiones semanales de seguimiento de proyecto.
- Envió de documentos de arranque para levantamiento de información de los 6 activos a analizar.
- Aprobación por parte de MHCP para integración de firewalls y directorio activo.

FIRMA CONTRATISTA

En mi calidad de supervisor del contrato me permito avalar el contenido del informe y el avance en la ejecución del mismo de acuerdo a lo descrito.

El contrato no presenta a la fecha dificultades en su ejecución, ni situaciones exógenas que afecten el normal desarrollo del mismo.

Firmado digitalmente por Luis Orlando Arenas Ruiz

FIRMA SUPERVISOR

MNEMO

SECURITY OPERATION CENTER

MINISTERIO DE HACIENDA Y CRÉDITO PUBLICO

ABRIL 2024

INFORME MENSUAL

OBJETIVO

Presentar los resultados del servicio de correlación. analítica y monitoreo de eventos de seguridad y ciberseguridad. de acuerdo con el contrato 3.471-2023 ejecutados por el equipo SOC-CERT de Mnemo Colombia S.A.S. permitiendo contar con la visibilidad de eventos y/o posibles ataques a la infraestructura que soporta los productos, servicios, canales y activos tecnológicos de Contactar. basado en las fuentes de información integradas en la actualidad.

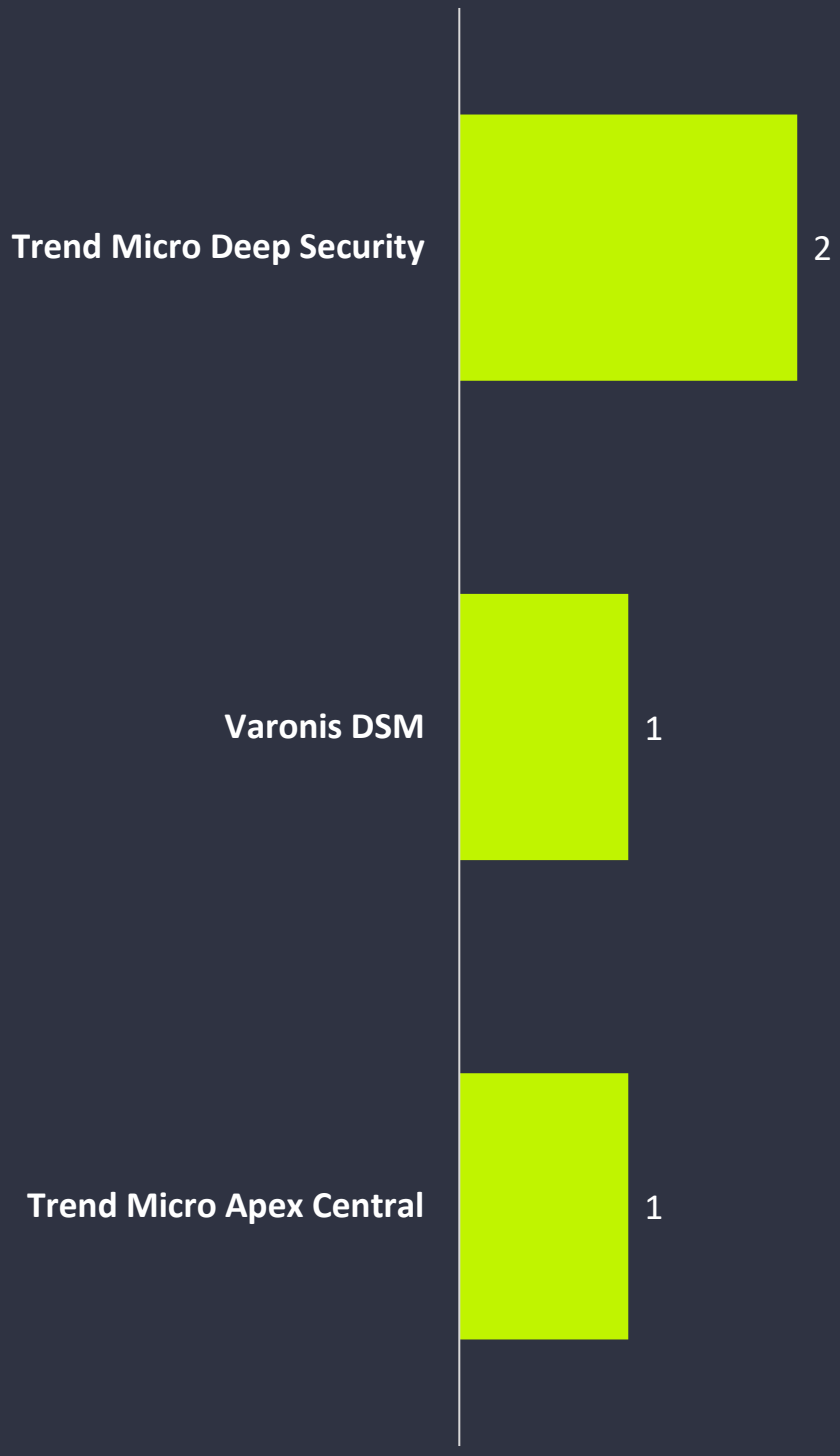
- Presentar el inventario de fuentes integradas.
- Presentar los eventos identificados de acuerdo a la taxonomía.
- Presentar los eventos maliciosos detectados.
- Identificar recomendaciones de mejora de acuerdo con los datos analizados.
- Presentar conclusiones relevantes.

ALCANCE

Exponer los eventos identificados en el servicio de monitorización ejecutado por SOC-CERT de Mnemo Colombia durante el periodo comprendido entre el 1 al 30 de Abril de 2024. comprendiendo los siguientes temas.

- Descripción de fuentes de información.
- Taxonomía y detalle de los eventos identificados.
- Categoría eventos.
- Resumen de alertas.
- Eventos relevantes de servicio.
- Recomendaciones.

FUENTES DE DATOS ACTUALES EN LA HERRAMIENTA QRADAR



141M
Eventos procesados

387
Ofensas generadas

55
Ticket

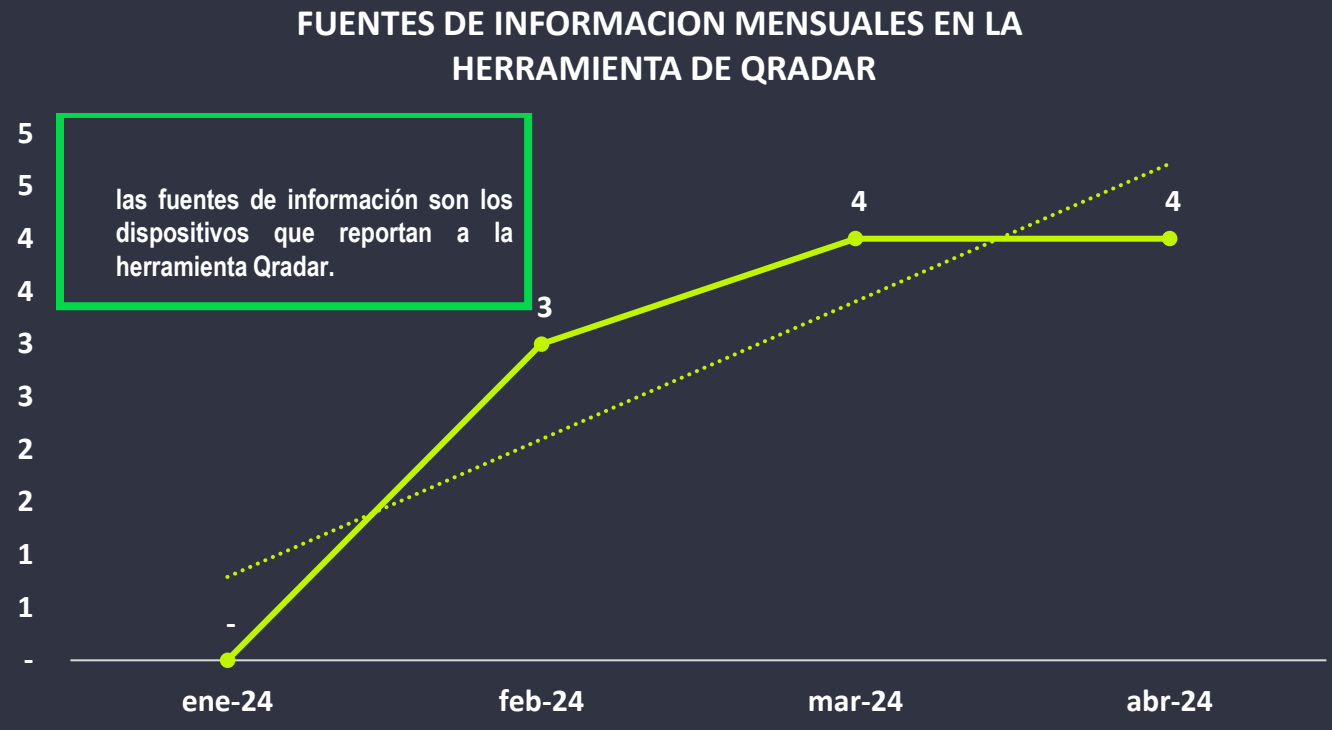
54
EPS

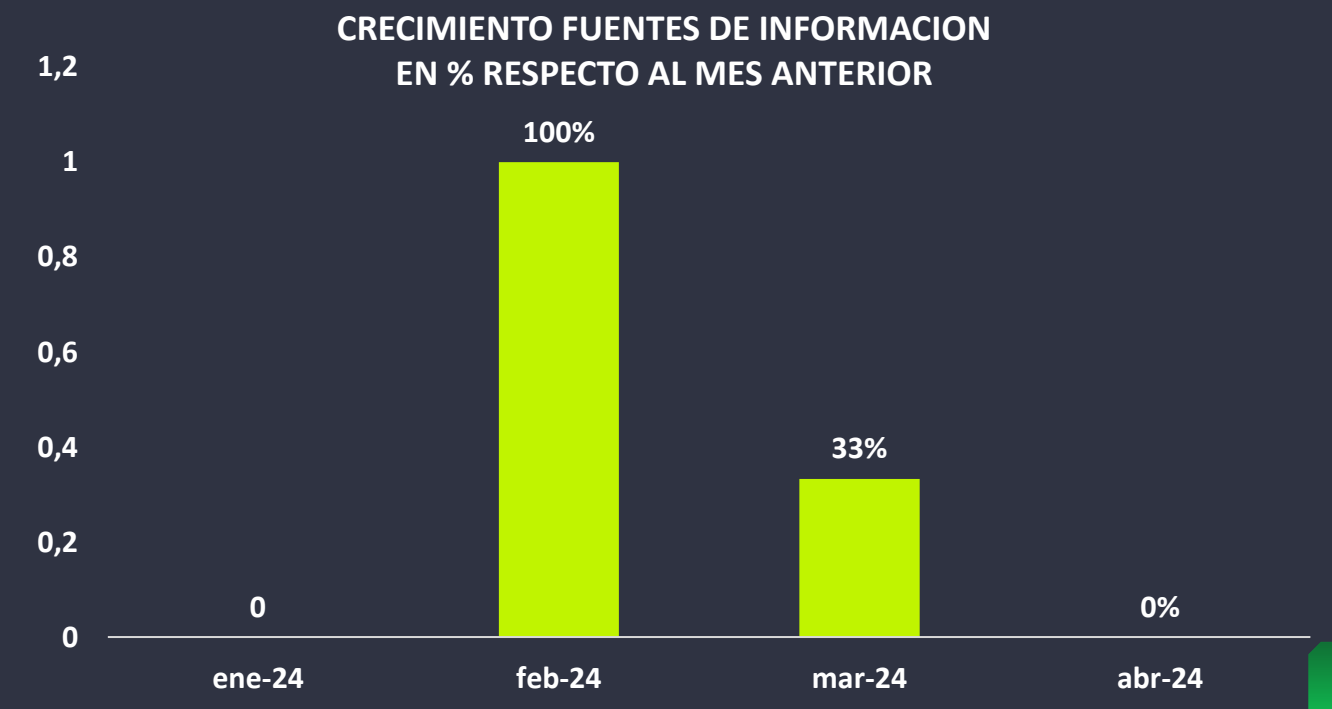
4
Fuentes activas

MNEMO

GENERALIDADES

A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología. dando a conocer el porcentaje de crecimiento respecto al mes inmediatamente anterior.

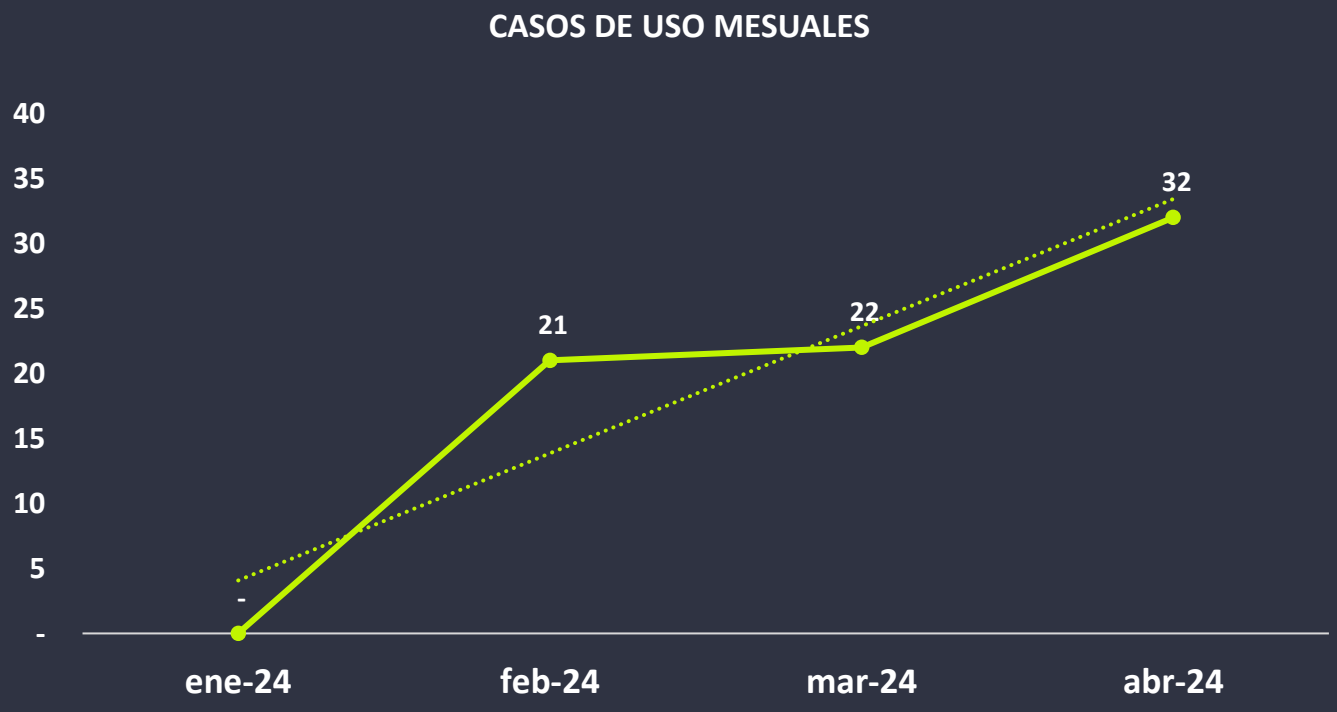


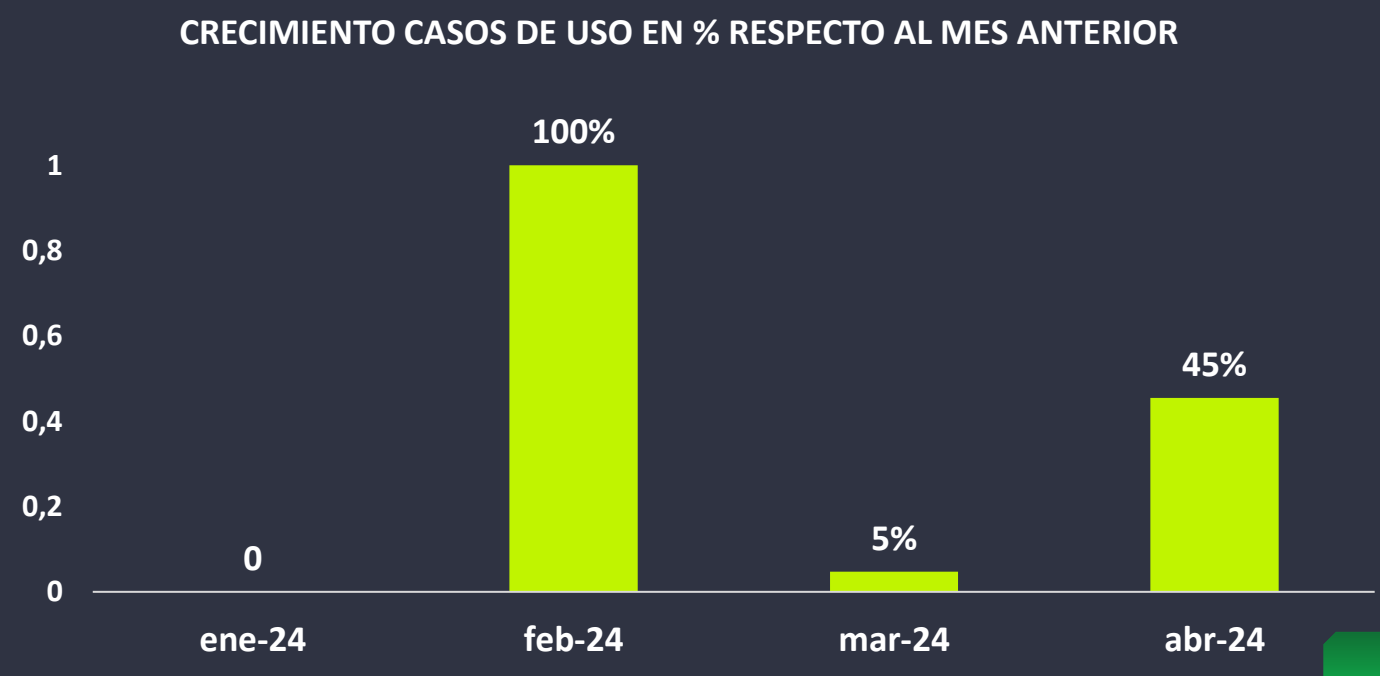


MNEMO

GENERALIDADES

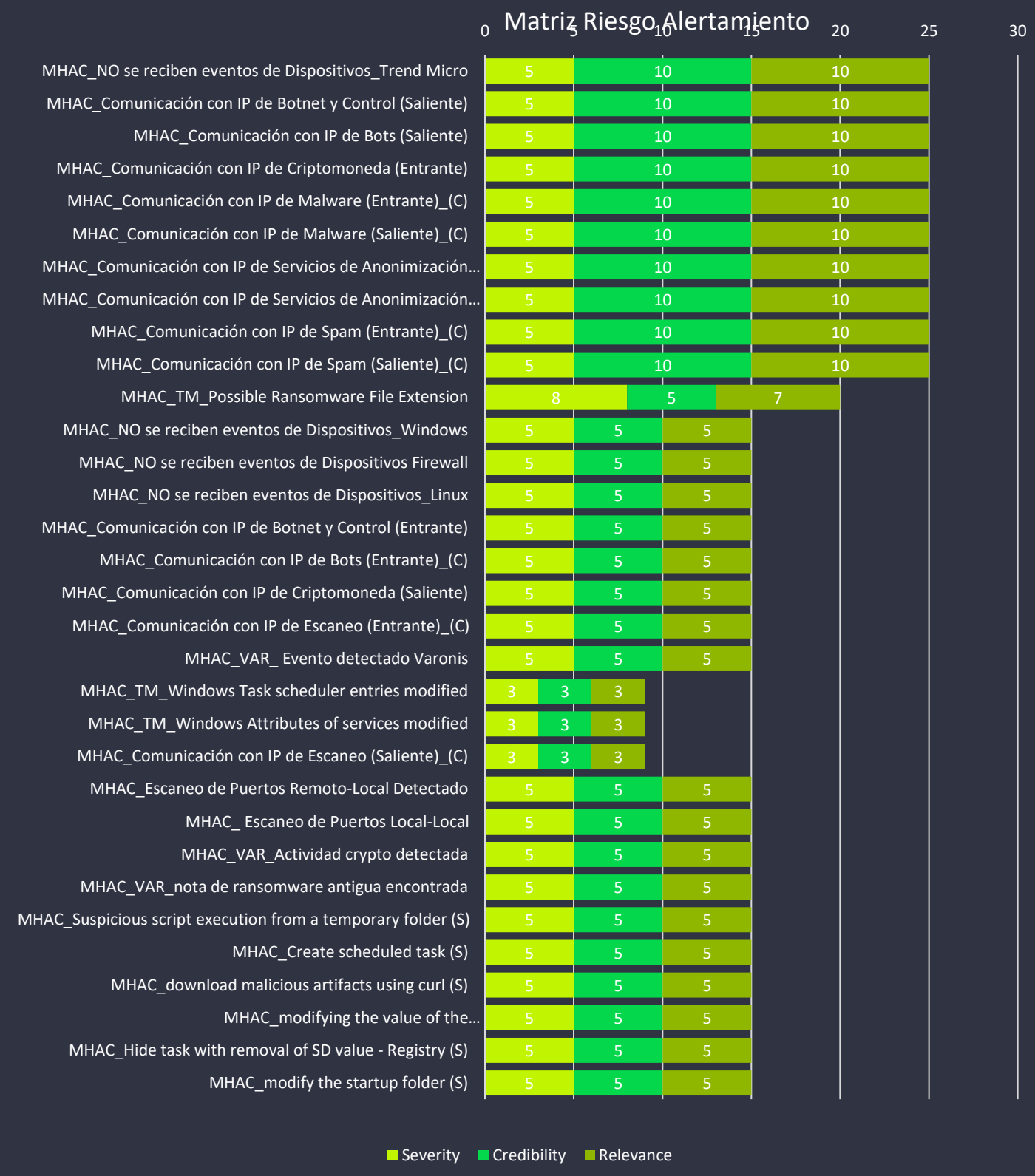
A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología. dando a conocer el porcentaje de crecimiento respecto al mes inmediatamente anterior.





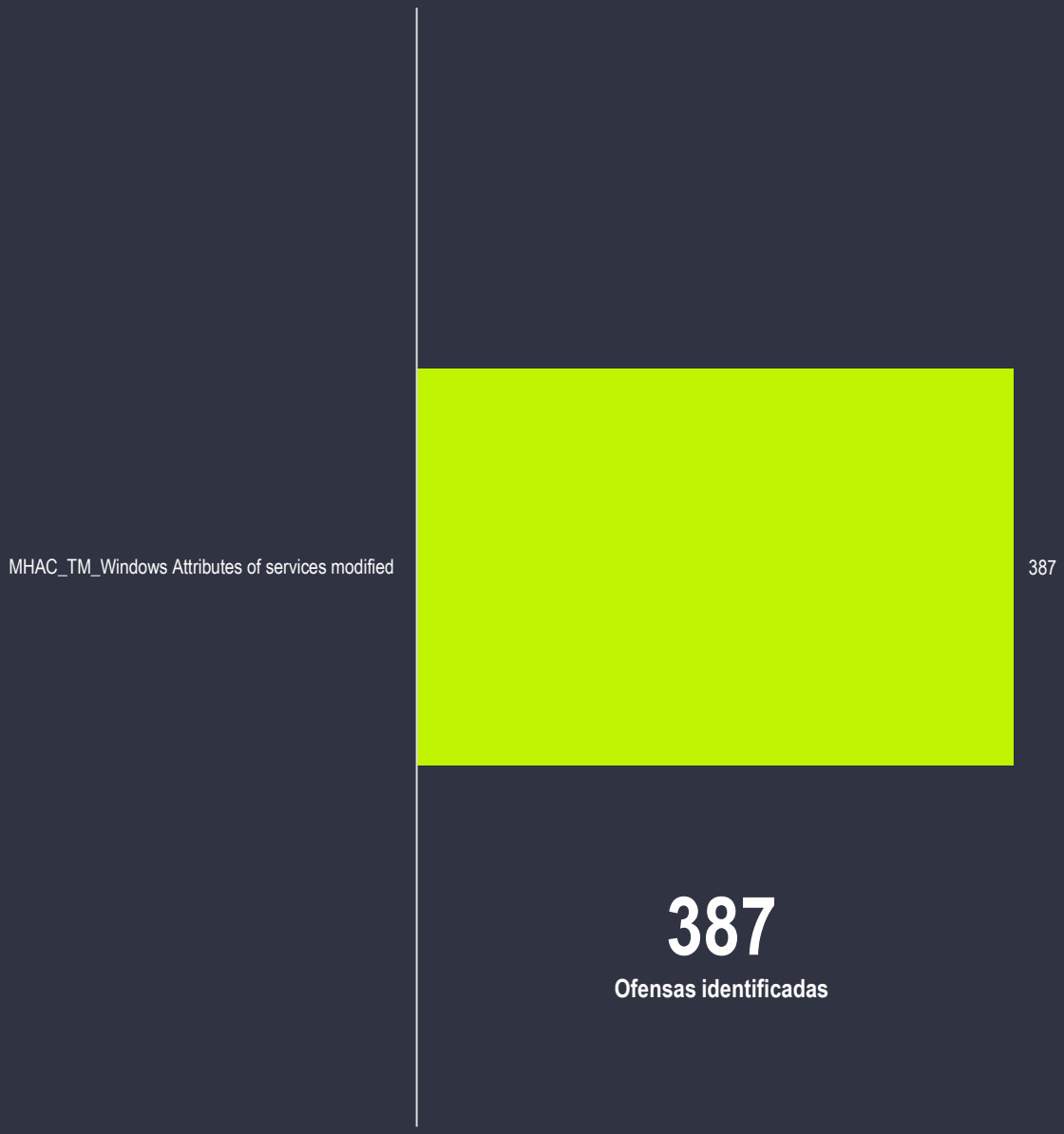
MNEMO

MATRIZ DE ALERTAMIENTO



GESTIÓN DE EVENTOS SOC

TOP EVENTOS



387

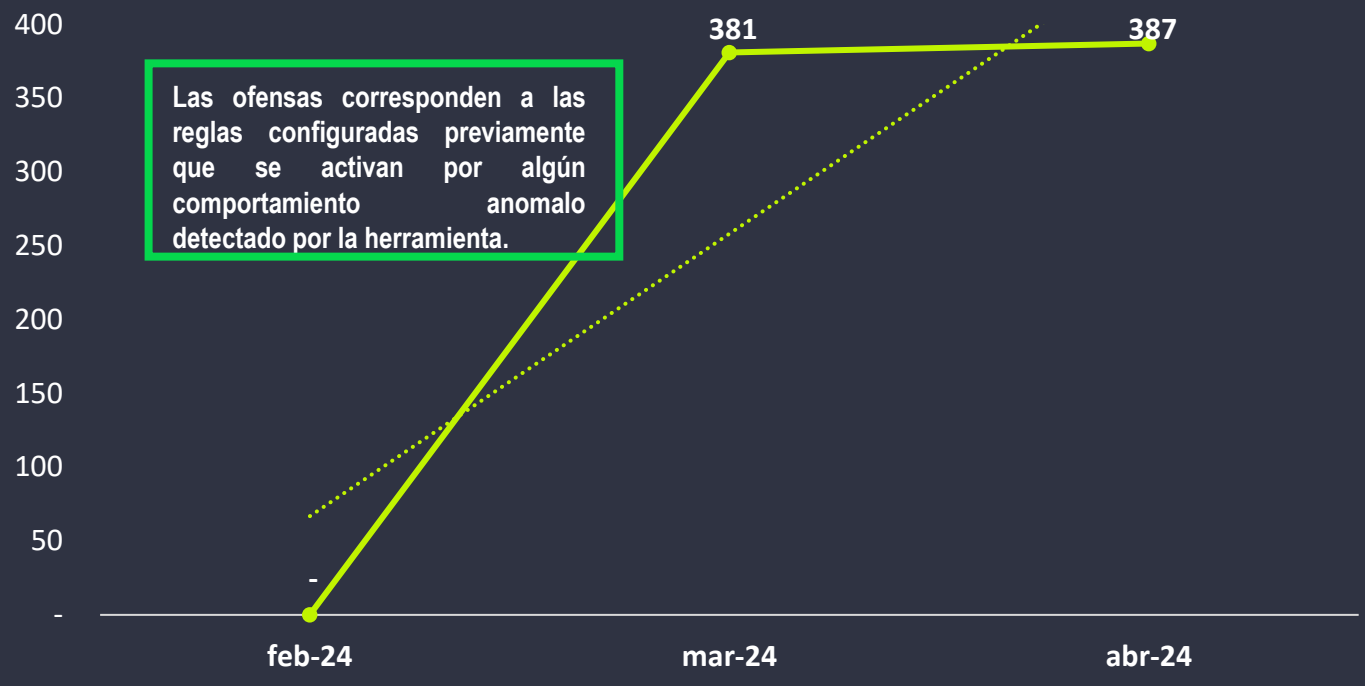
Ofensas identificadas

Durante ABRIL se registraron un total de 387 ofensas representadas en 1 reglas de correlación . posteriormente al respectivo análisis y filtro de falsos positivos o duplicidad se generaron un total de 55 tickets enviados vía correo electrónico.

GENERALIDADES

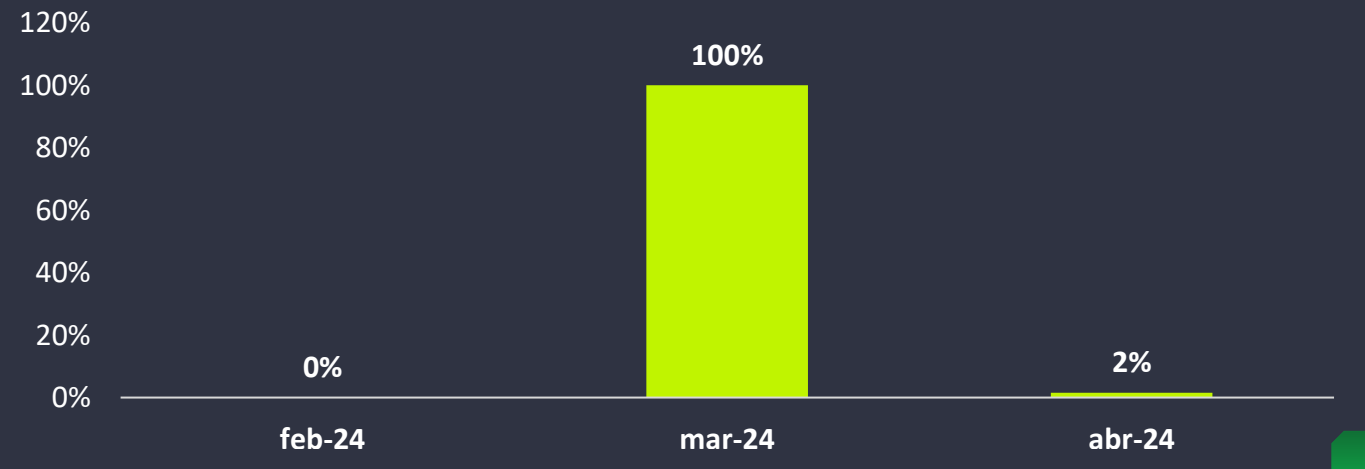
A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología. dando a conocer el porcentaje de crecimiento respecto al mes inmediatamente anterior.

OFENSAS GENERADAS MENSUALES



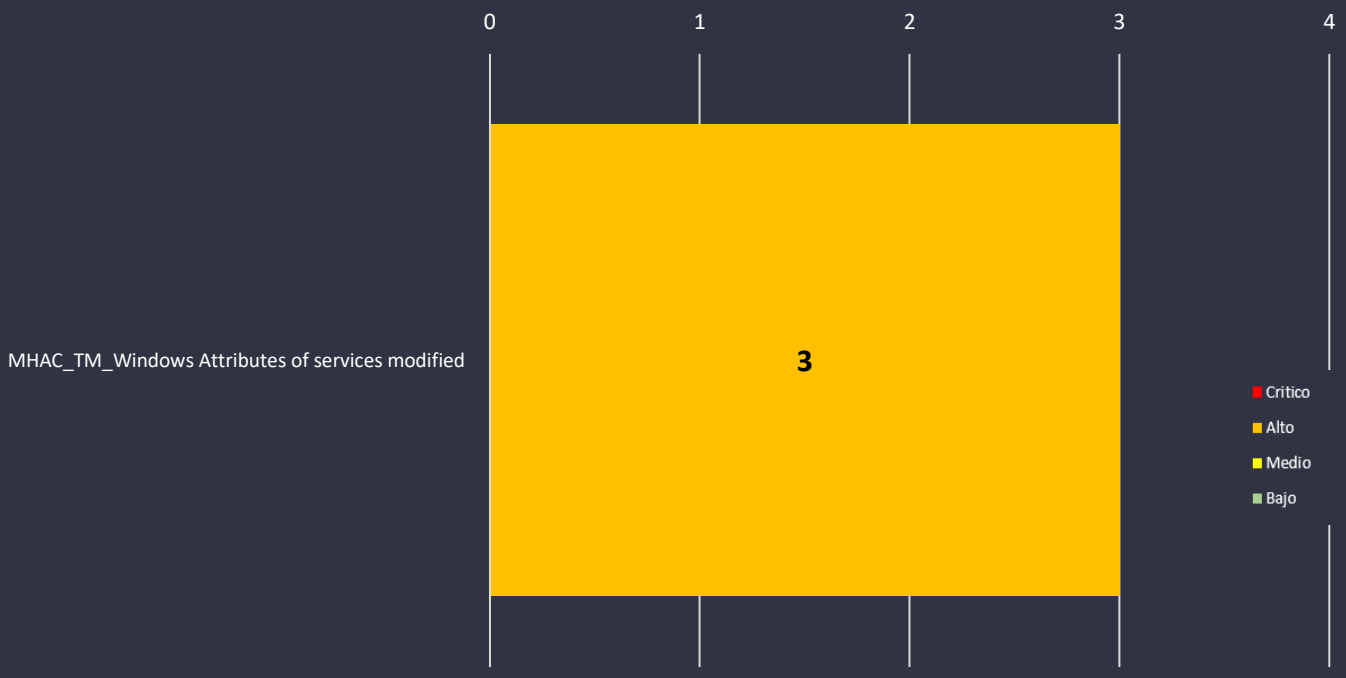
Las ofensas corresponden a las reglas configuradas previamente que se activan por algún comportamiento anomalo detectado por la herramienta.

OFENSAS GENERADAS EN % RESPECTO AL MES ANTERIOR



CRITICIDAD CASOS DE USO

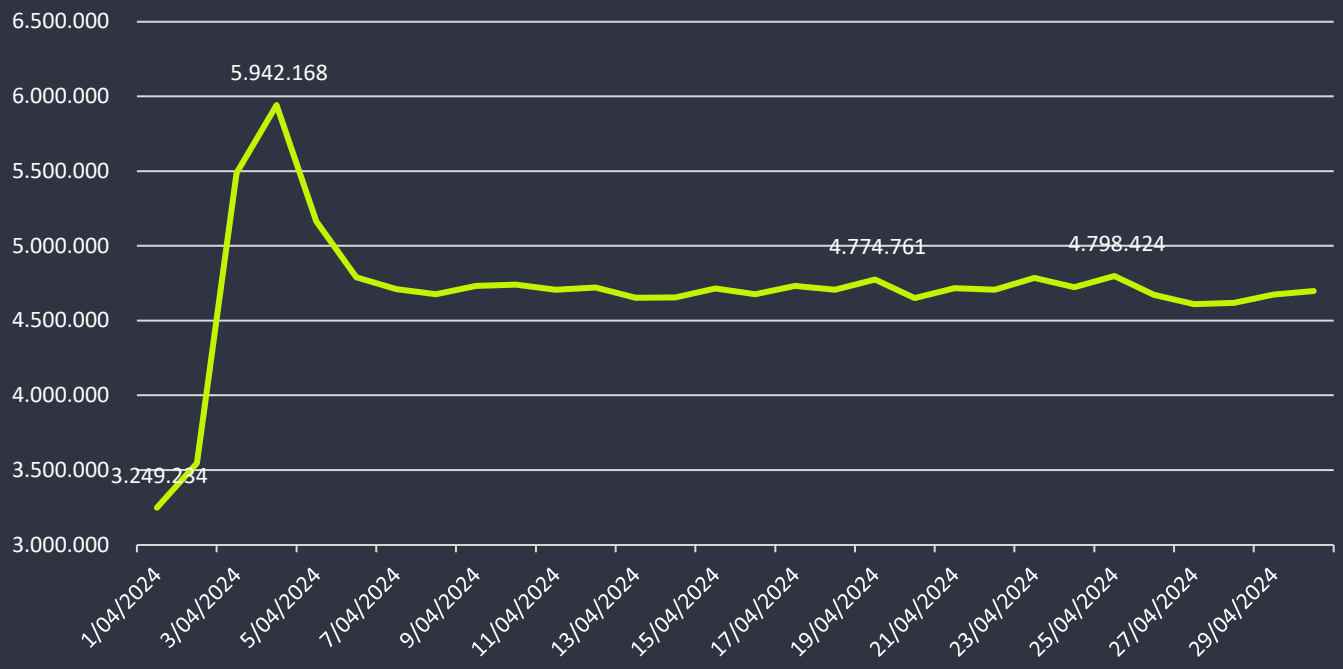
A continuación, se presentan los casos de uso que tuvieron activaciones en el mes de ABRIL junto con su criticidad.

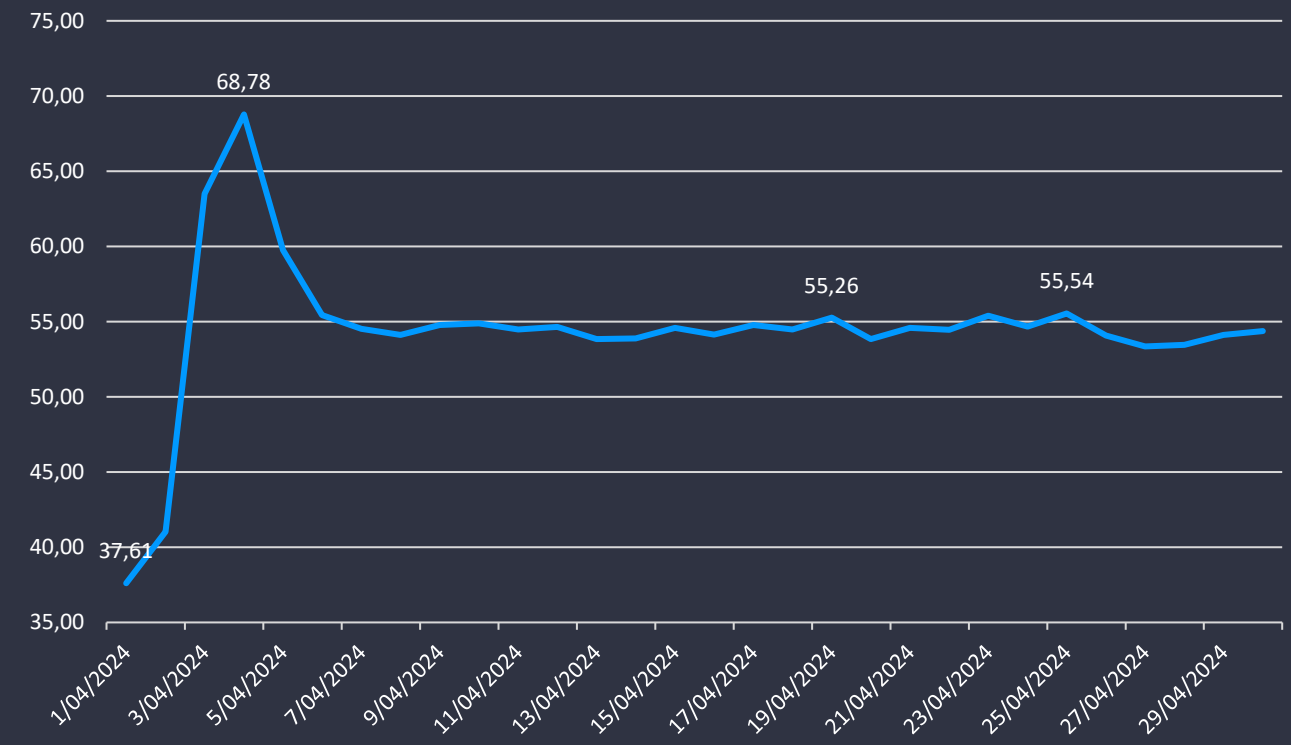


EVENTOS MENSUALES

141 M

Total, de eventos mensuales





54

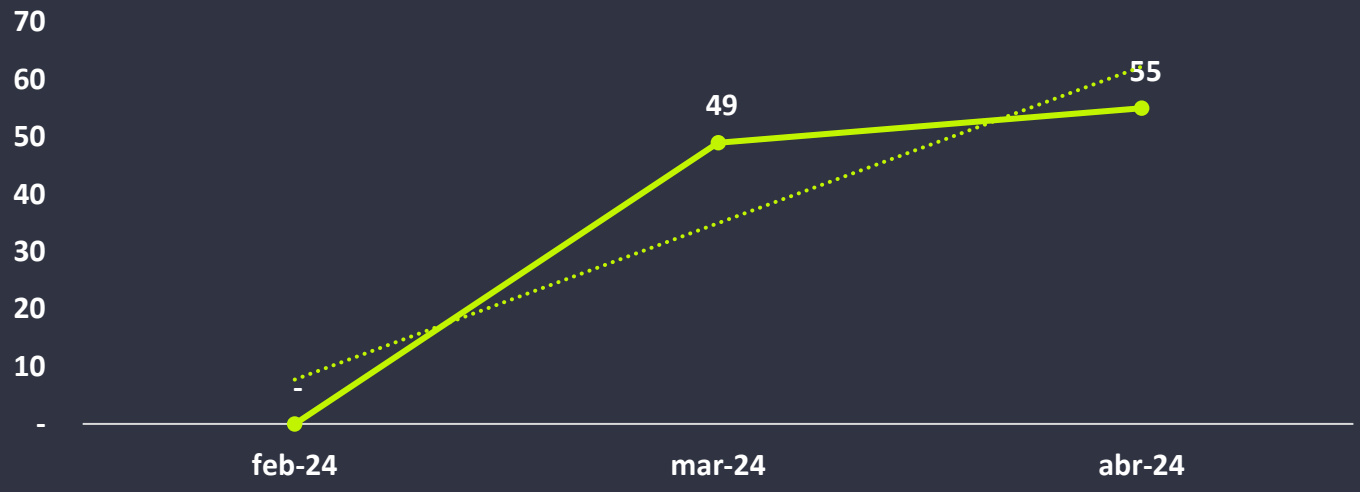
Promedio Eventos por segundo

MNEMO

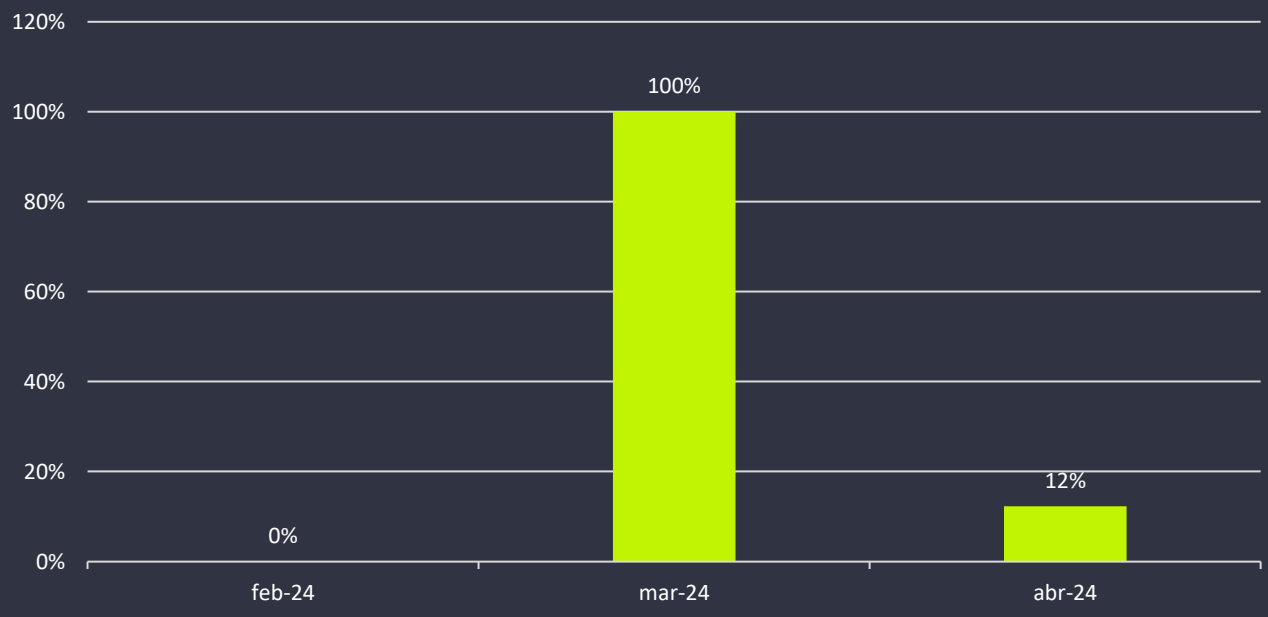
GENERALIDADES

A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología. dando a conocer el porcentaje de crecimiento respecto al mes inmediatamente anterior.

CANTIDAD DE ALERTAS EN LA HERRAMIENTA I-SIGHT MENSUALES



ALERTAS I-SIGHT EN % RESPECTO AL MES ANTERIOR



MNEMO

MHAC_VAR_NOTA DE RANSOMWARE ANTIGUA ENCONTRADA

A continuación, se presentan los eventos que fueron identificados por Varonis como posibles notas de ransomware encontradas

<14>Apr 12 15:34:16 MH-VARDSPSA01 LEEF:9.1.0|Varonis|DatAdvantage|8.6.32|Old ransomware note was found in the system| cat=Other devTime=Apr 12 2024 15:34:16 devTimeFormat=MMM dd yyyy HH:mm:ss proto=Syslog sev=4 src=10.120.211.6 Device_Name=OMORENO Alert_Description= usrName=MINHACIENDA.RED\Otoniel Moreno Molina accountName=omoreno domain=MINHACIENDA.RED Event_Type=File opened Event_Type_ID=1 Event_Status=Success Affected_Object=LEAME.TXT Event_File_Server_Domain=MH-DFSUSA05.MINHACIENDA.RED Affected_Object_Path=N:\DT\SART\SO\COMPROMISOS_LABORALES\OMORENO\Backup12.04.24\MH-SIED\~GD\0.SOFTWARE\Of2007-ES-32\UPDATES\LEAME.TXT Event_Additional_Data= Threshold_Value= Threshold_First_Timestamp= Event_by_MailboxOwner= Email_Sender= Email_Date= Account_of_Changed_Permissions= Permissions_Changes=None Permissions_before_Change=None Permissions_after_Change=None Alert_Page_URL=https://MH-VARDSPSA01.MINHACIENDA.RED:443/DatAdvantage/#/app/analytics/entity/Alert/fce3f3c8-4e75-4668-8504-6e4ac6a22bea Alert_ID=fce3f3c8-4e75-4668-8504-6e4ac6a22bea

<14>Apr 11 14:33:35 MH-VARDSPSA01 LEEF:9.1.0|Varonis|DatAdvantage|8.6.32|Old ransomware note was found in the system| cat=Other devTime=Apr 11 2024 14:33:33 devTimeFormat=MMM dd yyyy HH:mm:ss proto=Syslog sev=4 src=127.0.0.1 Device_Name= Alert_Description= usrName=MINHACIENDA.RED\Fernando Rosero accountName=frosero0 domain=MINHACIENDA.RED Event_Type=File opened Event_Type_ID=1 Event_Status=Failure Affected_Object=leame.txt Event_File_Server_Domain=MH-DFSUHISTSA01.MINHACIENDA.RED Affected_Object_Path=F:\DGCPTN\SO\Despacho\usuarios-NDGONZAL\leame.txt Event_Additional_Data= Threshold_Value= Threshold_First_Timestamp= Event_by_MailboxOwner= Email_Sender= Email_Date= Account_of_Changed_Permissions= Permissions_Changes=None Permissions_before_Change=None Permissions_after_Change=None Alert_Page_URL=https://MH-VARDSPSA01.MINHACIENDA.RED:443/DatAdvantage/#/app/analytics/entity/Alert/545e3c5b-e7fa-4bbe-ad5a-dd73e2133cc0 Alert_ID=545e3c5b-e7fa-4bbe-ad5a-dd73e2133cc0

2

Ofensas identificadas

Acting Object (custom)	Affected Object (custom)	Affected Object Path (custom)	Event Type (custom)
MINHACIENDA.RED\Otoniel Moreno Molina	LEAME.TXT	N:\DT\SART\SO\COMPROMISOS_LABORALES\OMORENO\Backup12.04.24\MH-SIED\~GD\0.SOFTWARE\Of2007-ES-32\UPDATES\LEAME.TXT	File opened
MINHACIENDA.RED\Fernando Rosero	leame.txt	F:\DGCPTN\SO\Despacho\usuarios-NDGONZAL\leame.txt	File opened

Las ofensas detectadas corresponden a falso positivos se procede a crear la regla de correlación **MHAC_VAR_nota de ransomware antigua encontrada** con el fin de evaluar por parte del SOC futuros eventos similares.

MHAC_VAR_NOTA DE RANSOMWARE ANTIGUA ENCONTRADA

A continuación, se presentan los eventos que fueron identificados por Varonis como posibles notas de ransomware encontradas

<14>Apr 12 15:34:16 MH-VARDSPSA01 LEEF:9.1.0|Varonis|DatAdvantage|8.6.32|Old ransomware note was found in the system| cat=Other devTime=Apr 12 2024 15:34:16 devTimeFormat=MMM dd yyyy HH:mm:ss proto=Syslog sev=4 src=10.120.211.6 Device_Name=OMORENO Alert_Description= usrName=MINHACIENDA.RED\Otoniel Moreno Molina accountName=omoreno domain=MINHACIENDA.RED Event_Type=File opened Event_Type_ID=1 Event_Status=Success Affected_Object=LEAME.TXT Event_File_Server_Domain=MH-DFSUSA05.MINHACIENDA.RED Affected_Object_Path=N:\DT\SART\SO\COMPROMISOS_LABORALES\OMORENO\Backup12.04.24\MH-SIED\~GD\0.SOFTWARE\Of2007-ES-32\UPDATES\LEAME.TXT Event_Additional_Data= Threshold_Value= Threshold_First_Timestamp= Event_by_MailboxOwner= Email_Sender= Email_Date= Account_of_Changed_Permissions= Permissions_Changes=None Permissions_before_Change=None Permissions_after_Change=None Alert_Page_URL=https://MH-VARDSPSA01.MINHACIENDA.RED:443/DatAdvantage/#/app/analytics/entity/Alert/fce3f3c8-4e75-4668-8504-6e4ac6a22bea Alert_ID=fce3f3c8-4e75-4668-8504-6e4ac6a22bea

<14>Apr 11 14:33:35 MH-VARDSPSA01 LEEF:9.1.0|Varonis|DatAdvantage|8.6.32|Old ransomware note was found in the system| cat=Other devTime=Apr 11 2024 14:33:33 devTimeFormat=MMM dd yyyy HH:mm:ss proto=Syslog sev=4 src=127.0.0.1 Device_Name= Alert_Description= usrName=MINHACIENDA.RED\Fernando Rosero accountName=frosero0 domain=MINHACIENDA.RED Event_Type=File opened Event_Type_ID=1 Event_Status=Failure Affected_Object=leame.txt Event_File_Server_Domain=MH-DFSUHISTSA01.MINHACIENDA.RED Affected_Object_Path=F:\DGCPTN\SO\Despacho\usuarios-NDGONZAL\leame.txt Event_Additional_Data= Threshold_Value= Threshold_First_Timestamp= Event_by_MailboxOwner= Email_Sender= Email_Date= Account_of_Changed_Permissions= Permissions_Changes=None Permissions_before_Change=None Permissions_after_Change=None Alert_Page_URL=https://MH-VARDSPSA01.MINHACIENDA.RED:443/DatAdvantage/#/app/analytics/entity/Alert/545e3c5b-e7fa-4bbe-ad5a-dd73e2133cc0 Alert_ID=545e3c5b-e7fa-4bbe-ad5a-dd73e2133cc0

2

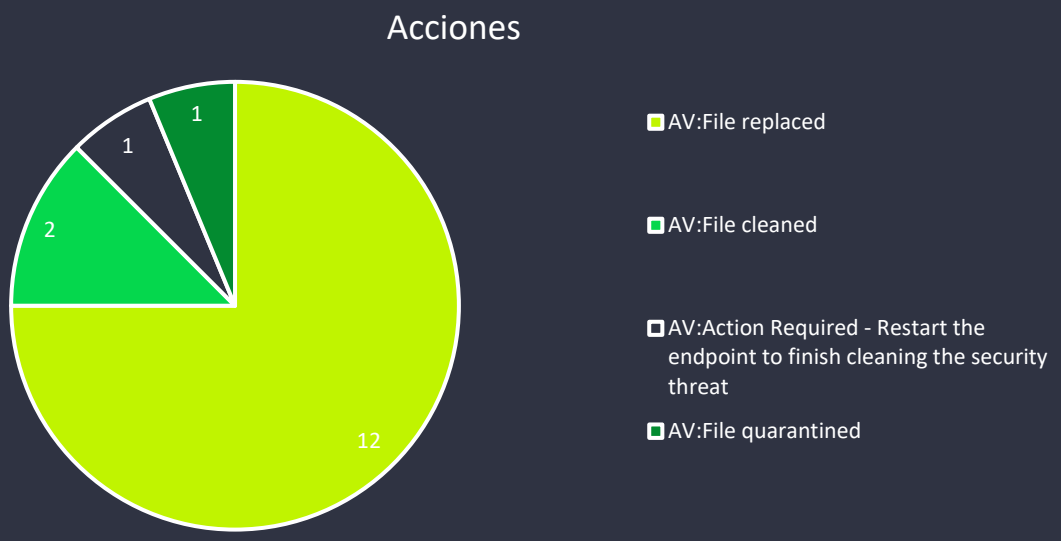
Ofensas identificadas

Acting Object (custom)	Affected Object (custom)	Affected Object Path (custom)	Event Type (custom)
MINHACIENDA.RED\Otoniel Moreno Molina	LEAME.TXT	N:\DT\SART\SO\COMPROMISOS_LABORALES\OMORENO\Backup12.04.24\MH-SIED\~GD\0.SOFTWARE\Of2007-ES-32\UPDATES\LEAME.TXT	File opened
MINHACIENDA.RED\Fernando Rosero	leame.txt	F:\DGCPTN\SO\Despacho\usuarios-NDGONZAL\leame.txt	File opened

Las ofensas detectadas corresponden a falso positivos se procede a crear la regla de correlación **MHAC_VAR_nota de ransomware antigua encontrada** con el fin de evaluar por parte del SOC futuros eventos similares.

VIRUS DETECTED

A continuación, se presentan los eventos que fueron identificados por TrendMicro como detecciones de virus



Las ofensas detectadas corresponden a falso positivos se procede a crear la regla de correlación **MHAC_TM_Virus/Malware Detected** con el fin de evaluar por parte del SOC futuros eventos similares.

MNEMO

VIRUS DETECTED

A continuación, se presentan los eventos que fueron identificados por TrendMicro como detecciones de virus

Detalle de acciones archivos y host	Suma de Event Count
AV:File replaced	12
MAERSK LINE -SHIPPING DOCUMENTS.zip	2
notificacionesjudiciales@minhaciendagovco.mail.onmicrosoft.com	1
tutelasmhcp@minhaciendagovco.mail.onmicrosoft.com	1
MSC-SHIPPING DOCUMENTS.zip	10
notificacionesjudiciales@minhaciendagovco.mail.onmicrosoft.com	3
siiffacelec@minhaciendagovco.mail.onmicrosoft.com	3
tutelasmhcp@minhaciendagovco.mail.onmicrosoft.com	4
AV:File cleaned	2
2fa0645e-42a9-458f-9fbf-0b28d774d654	1
WXSERVASEO1	1
FreeAudioEditor.exe	1
CXHCLAVIJO	1
AV:Action Required - Restart the endpoint to finish cleaning the security threat	1
NoChangingWallpaper	1
CXHCLAVIJO	1
AV:File quarantined	1
f_000a3c	1
GESINFO18	1
Total general	16

Las ofensas detectadas corresponden a falso positivos se procede a crear la regla de correlación **MHAC_TM_Virus/Malware Detected** con el fin de evaluar por parte del SOC futuros eventos similares.

2

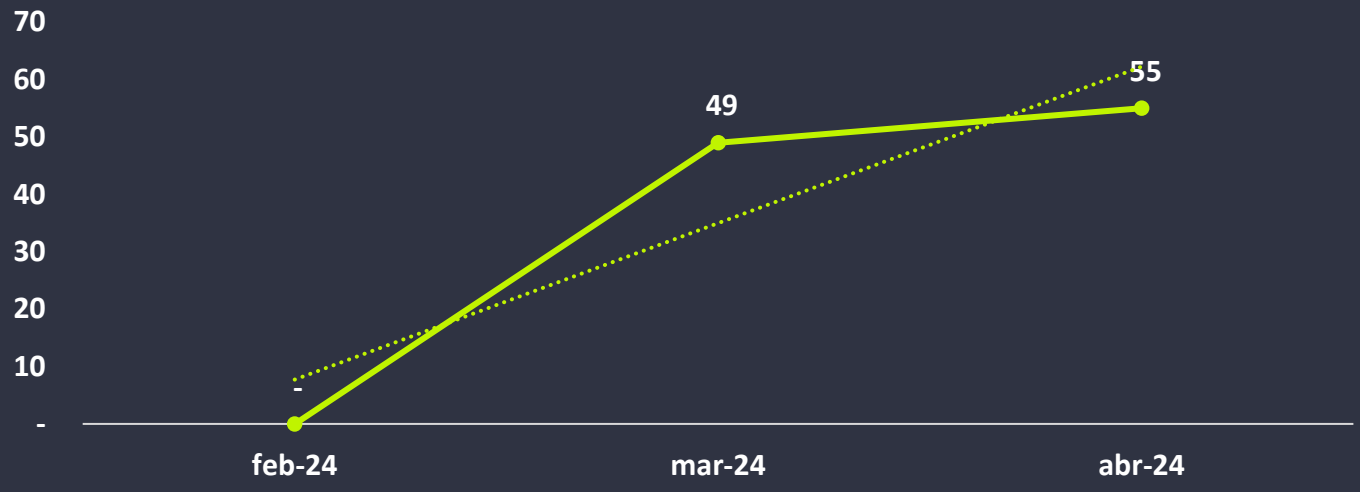
Ofensas identificadas

MNEMO

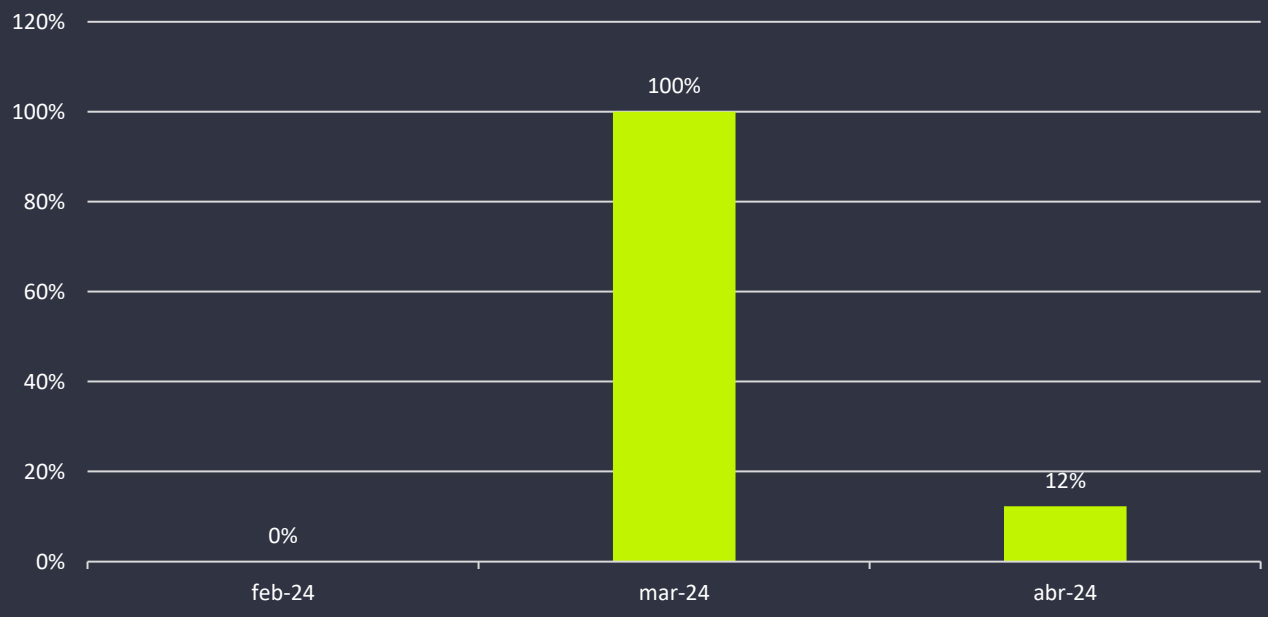
GENERALIDADES

A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología. dando a conocer el porcentaje de crecimiento respecto al mes inmediatamente anterior.

CANTIDAD DE ALERTAS EN LA HERRAMIENTA I-SIGHT MENSUALES



ALERTAS I-SIGHT EN % RESPECTO AL MES ANTERIOR



MNEMO

MATRIZ DE TICKETS SOC

CLASIFICACION DE LOS TICKETS

CLASIFICACIÓN	Tipo de incidente
Contenido abusivo	Spam
	Delito de odio
	Pornografía infantil, contenido sexual o violento inadecuado
Contenido dañino	Sistema infectado
	Servidor C&C
	Distribución de malware
	Configuración de malware
Obtención de información	Ingeniería social
	Escaneo de redes (scanning)
	Análisis de paquetes (Sniffing)
Intento de intrusión	Explotación de vulnerabilidades conocidas
	Intento de acceso con vulneración de credenciales
	Ataque desconocido
Intrusiones	Compromiso de cuentas con privilegios
	Compromiso de cuenta sin privilegios
	Compromiso de aplicaciones
	Robo
Disponibilidad	DoS (Denegación de Servicio)
	DDoS (Denegación Distribuida de Servicio)
	Sabotaje
	Mala configuración
	Interrupciones
Compromiso de la información	Acceso no autorizado a información
	Modificación no autorizada de información
	Pérdida de datos
Fraude	Suplantación
	Uso no autorizado de recursos
	Phishing
	Derechos de autor
Vulnerable	Criptografía débil
	Amplificador DDoS
	Servicios con acceso potencial no deseado
	Revelación de información
	Sistema vulnerable
Otros	APT
	Ciberterrorismo
	Daños informáticos PIC
	Otros

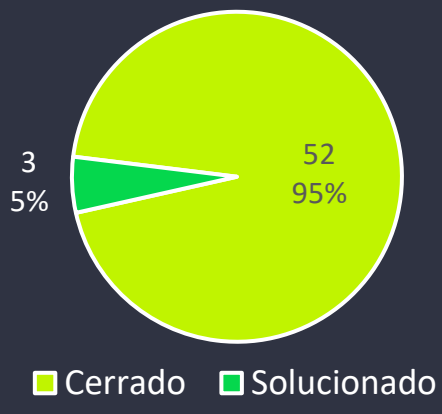
***I-SIGHT Plataforma de gestión de tickets por parte de MNEMO COLOMBIA al finalizar implementación**

ESTADÍSTICA GENERAL CASOS REPORTADOS

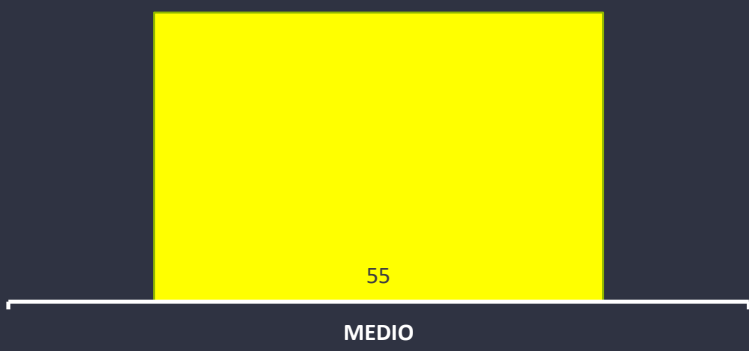
Ninguno de los eventos reportados indican ataques exitosos.

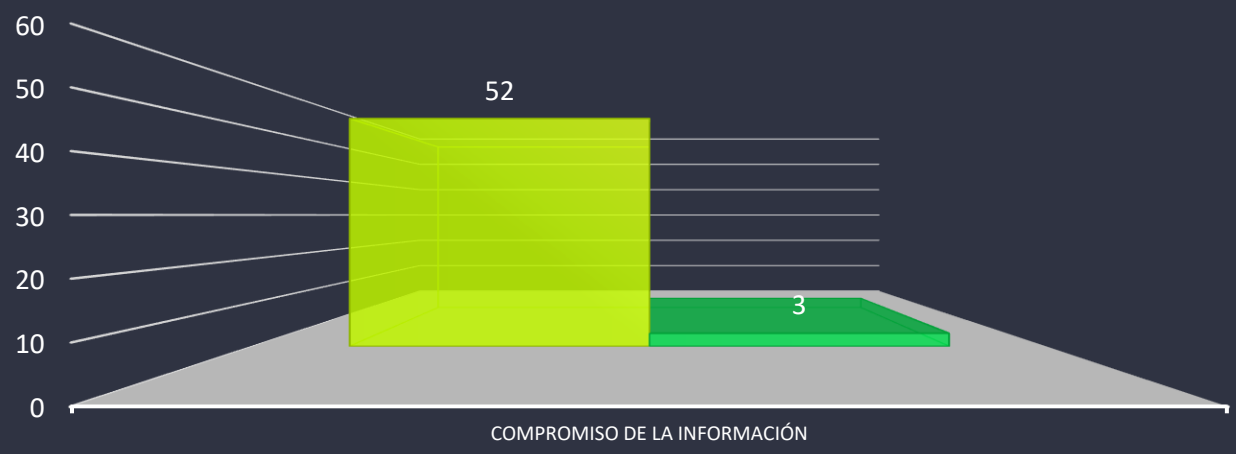
Compromiso de la información

Estado de Tickets



Criticidad de Tickets





ACTIVIDADES REALIZADAS

- **Sesiones conjuntas para agregar fuentes de información.**
  - **MHAC_VARONIS_10.3.1.29 MH-VARDSPSA01**

- **Afinación de reglas de correlación.**
  - MHAC_NO se reciben eventos de Dispositivos_Windows
  - MHAC_NO se reciben eventos de Dispositivos Firewall
  - MHAC_NO se reciben eventos de Dispositivos_Linux
  - MHAC_TM_Possible Ransomware File Extension
  - MHAC_TM_Windows Task scheduler entries modified
  - MHAC_TM_Windows Attributes of services modified

- **Creación de reglas de correlación.**
  - MHAC_Escaneo de Puertos Remoto-Local Detectado
  - MHAC_ Escaneo de Puertos Local-Local
  - MHAC_VAR_Actividad crypto detectada
  - MHAC_VAR_nota de ransomware antigua encontrada
  - MHAC_Suspicious script execution from a temporary folder (S)
  - MHAC_Create scheduled task (S)
  - MHAC_download malicious artifacts using curl (S)
  - MHAC_modifying the value of the HKEY_CURRENT_USER\ Environment registry key (S)
  - MHAC_Hide task with removal of SD value - Registry (S)
  - MHAC_modify the startup folder (S)

SLA

SLA DE EVENTOS DE SEGURIDAD

criticidad	Máx. de diferencia	Promedio de diferencia	Mín. de diferencia
Bajo	00:00:00	00:00:00	00:00:00
Medio	00:58:00	00:26:41	00:05:00
Alto	00:00:00	00:00:00	00:00:00
Total general	00:58:00	00:26:41	00:05:00

CRITICIDAD	CUMPLIMIENTO	SLA	TIEMPO MAX. SLA
Bajo	100%	120 MINUTOS	02:00:00
Medio	100%	60 MINUTOS	01:00:00
Alto	100%	30 MINUTOS	00:30:00

RECOMENDACIONES Y CONCLUSIONES

- Se recomienda hacer el bloqueo de las IPs enviadas con indicadores de compromiso en alertas tempranas y preventivas ya que pueden generar una brecha de seguridad en la entidad.

- Se recomienda continuar con la integración de fuentes de información para tener una mayor visibilidad de la actividad dentro de la organización , ya que un numero muy bajo de fuentes de información impide al SOC verificar algún tipo de evento malicioso dentro de la entidad.

- Se recomienda continuar con el constante análisis de los eventos reportadas por el equipo SOC y realizar el seguimiento de alertas y comportamientos que presenten alguna amenaza en la entidad.

- Se recomienda reforzar la capacitación del personal perteneciente a la organización respecto a temas de ciberseguridad con el fin de que se evite ser víctima de campañas de phishing.

- Se recomienda reforzar la capacitación del personal perteneciente a la organización para prevenir la instalación de software que viole las leyes de derechos de autor y que contengan posible malware.

MNEMO

SECURITY OPERATION CENTER

MINISTERIO DE HACIENDA Y CRÉDITO PUBLICO

ABRIL 2024

INFORME MENSUAL

MN E MO

CYBER THREAT INTELLIGENCE
by MN E MO

INFORME
CYBER SECURITY WARNING
EARLY

Abril / 2024

EQUIPO DE CYBER THREAT INTELLIGENCE

Ministerio de Hacienda y Crédito Público

MNEMO

ALERTAS REPORTADAS

39

ESTAS ALERTAS COMPRENDEN ACTUALIZACIONES DE DIFERENTES FABRICANTES Y SUS RESPECTIVOS PRODUCTOS, LOS CUALES ESTÁN ESPECIFICADOS EN EL SIGUIENTE INFORME.

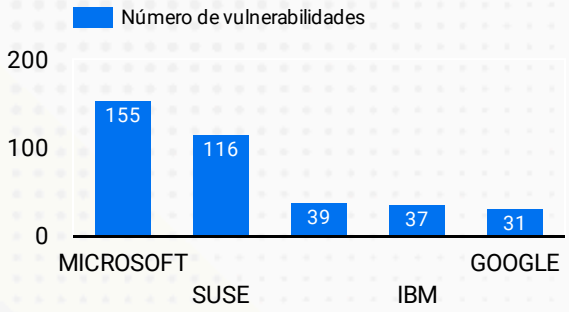
VULNERABILIDADES REPORTADAS

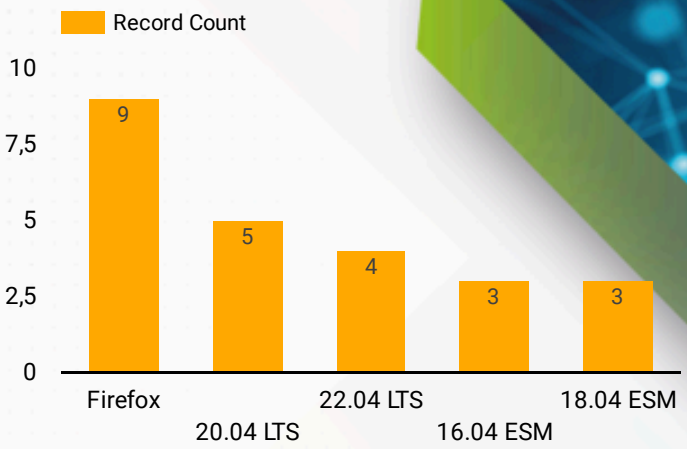
504

ERRORES REPORTADOS

1

MNEMO

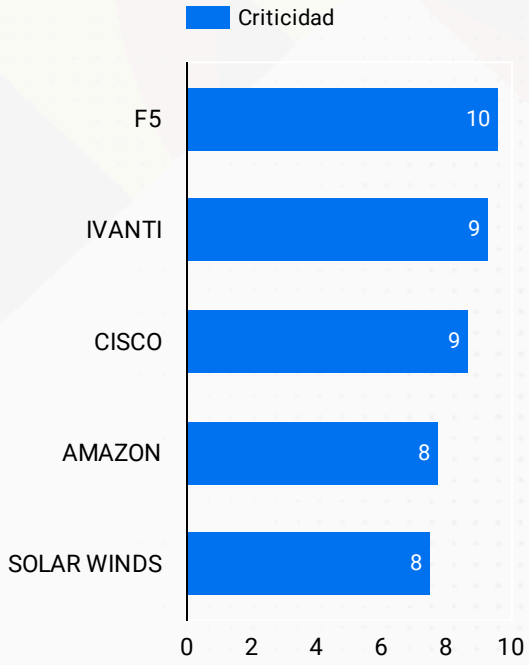




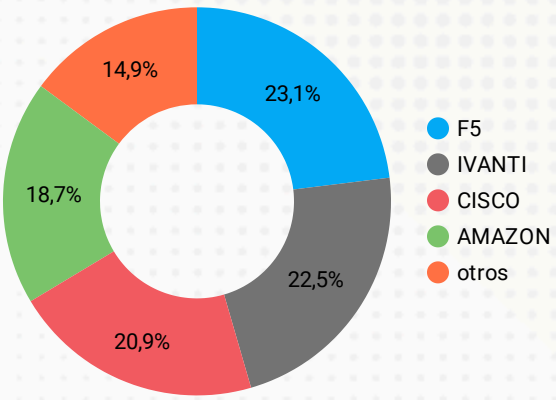
Top 5 fabricantes con mayor número de vulnerabilidades reportadas

Top 5 productos con mayor número de reportes en el mes

ESTAS ALERTAS COMPRENDEN ACTUALIZACIONES DE DIFERENTES FABRICANTES Y SUS RESPECTIVOS PRODUCTOS, LOS CUALES ESTÁN ESPECIFICADOS EN EL SIGUIENTE INFORME.



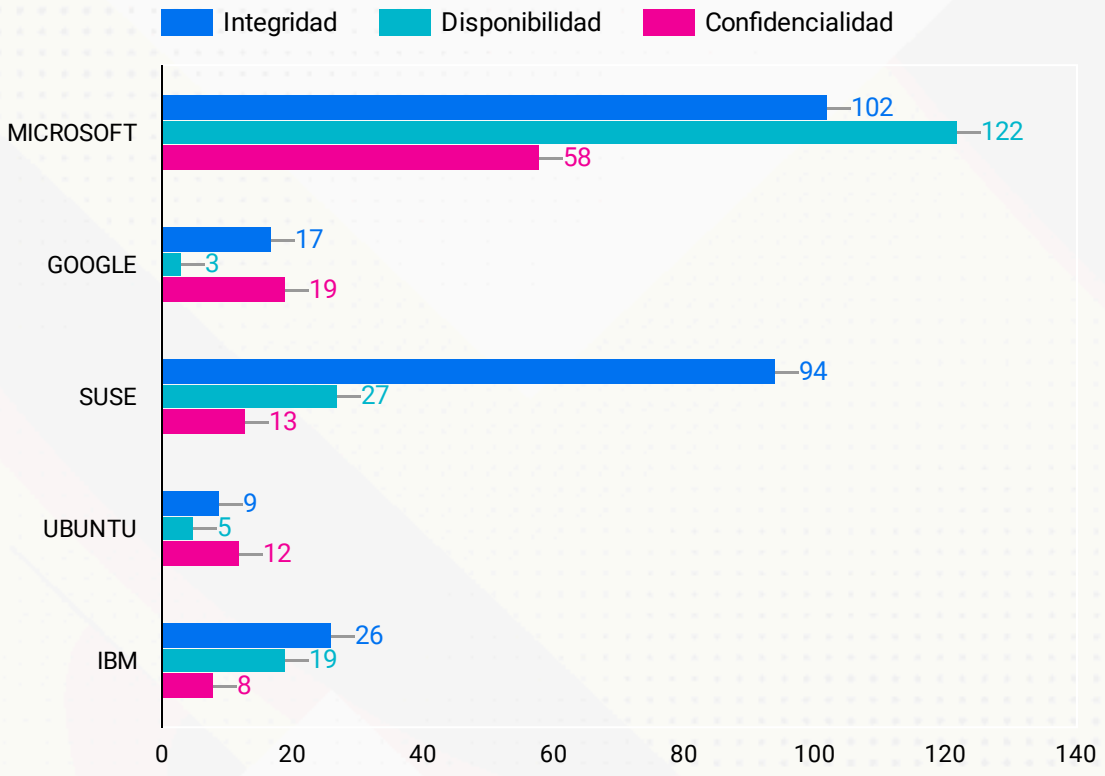
Nivel de criticidad promedio por fabricante, tomando el cvss reportado por cada uno



CYBER THREAT INTELLIGENCE

MNEMO

Nivel de afectación de fabricantes en los pilares del SGSI, reportados.



Detectar e informar las afectaciones al Sistema de Gestión de Seguridad de la Información (SGSI) basándose en el nivel de afectación determinado por el total de alertas emitidas por fabricantes, donde se identifican las CVE (Vulnerabilidades y Exposiciones Comunes) que afectan la integridad, confidencialidad o disponibilidad de los datos alojados en los software afectados, sirve para varios propósitos importantes en la ciberseguridad y la gestión de la seguridad de la información:

Gestión de Riesgos: Permite a las organizaciones evaluar y gestionar los riesgos asociados a las vulnerabilidades conocidas en su SGSI. Esto es crucial para identificar amenazas y tomar medidas proactivas para mitigar los riesgos.
Priorización de Acciones: Ayuda a priorizar las acciones de seguridad. Al comprender cuáles de las vulnerabilidades conocidas tienen un mayor impacto en la integridad, confidencialidad o disponibilidad de los datos, las organizaciones pueden centrarse en abordar las más críticas primero.
Cumplimiento Normativo: Contribuye al cumplimiento de requisitos normativos relacionados con la gestión de vulnerabilidades y la protección de datos. Informar sobre afectaciones ayuda a demostrar que se están tomando medidas adecuadas para proteger la información sensible.
Mejora Continua: Facilita la mejora continua del SGSI al proporcionar datos concretos sobre áreas donde se pueden fortalecer las defensas y la seguridad. Esto es esencial en un entorno en constante evolución de amenazas cibernéticas.
Comunicación y Concienciación: Ayuda en la comunicación interna y externa sobre el estado de la seguridad de la información. Puede utilizarse para informar a partes interesadas clave, incluidos los equipos de dirección, sobre la necesidad de inversión en seguridad.

MNEMO

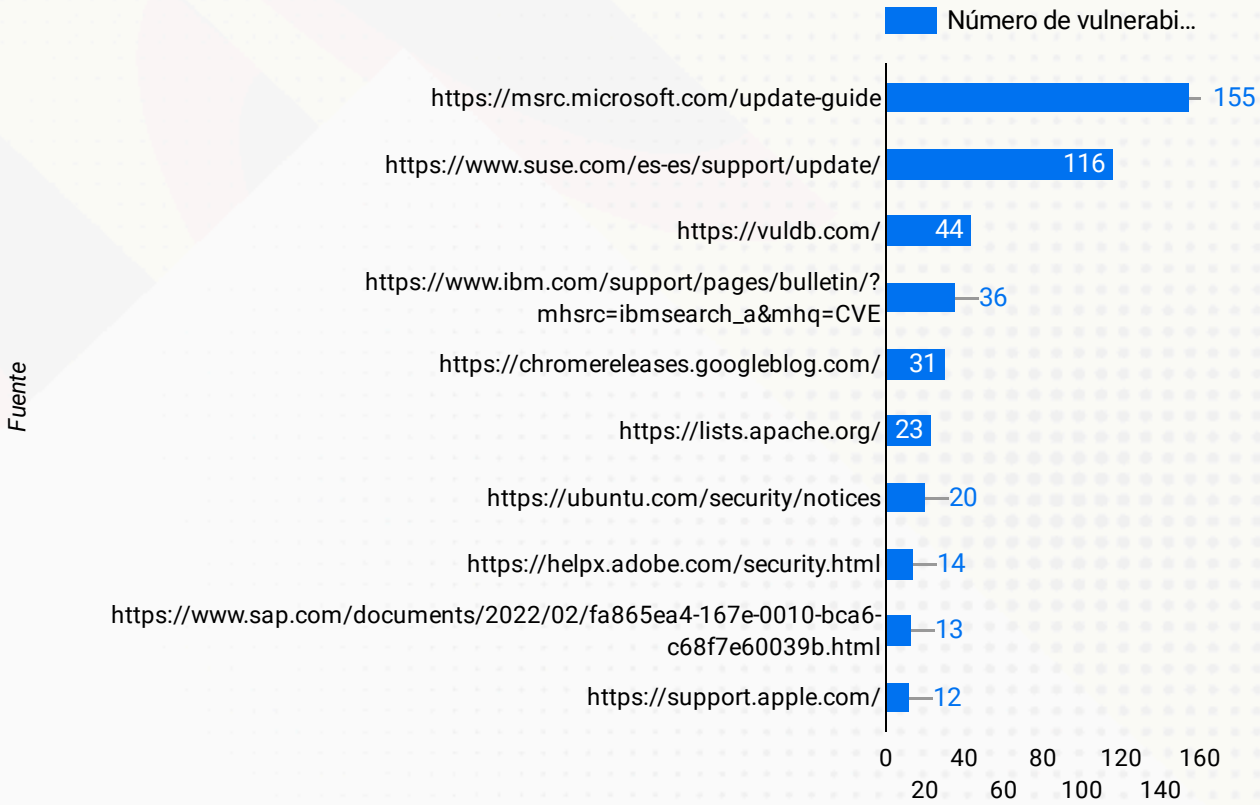
Total productos reportados

259

Total fabricantes reportados

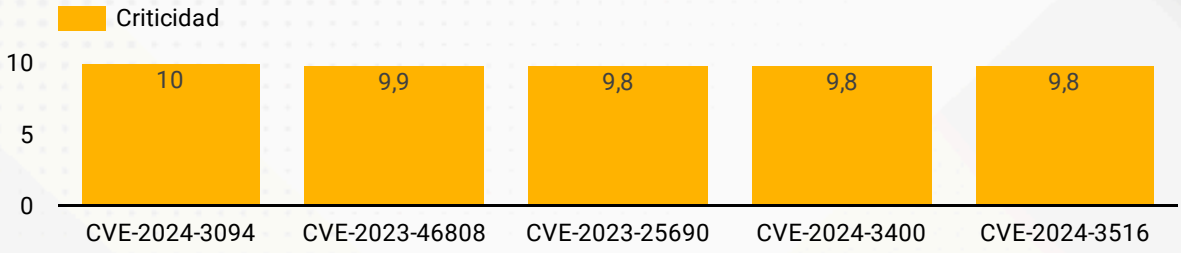
25

Número de CVE reportadas por fuente



MNEMO

Top 5 de los CVE con la mayor criticidad reportada en el transcurso del mes

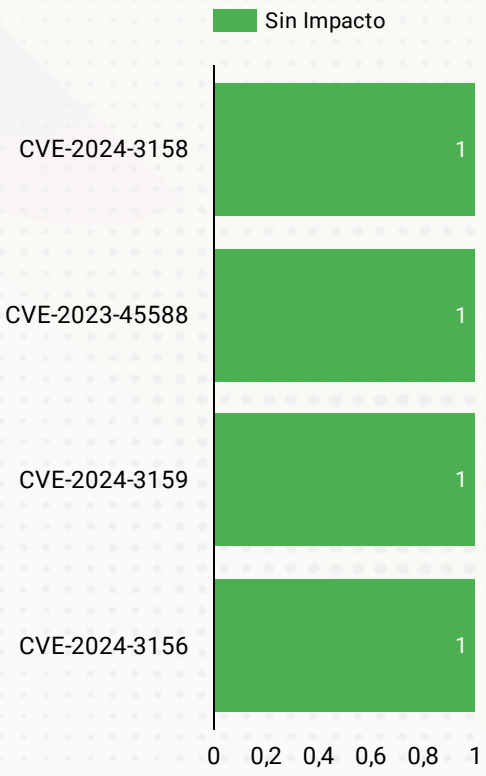


Totlal vulnerabilidades

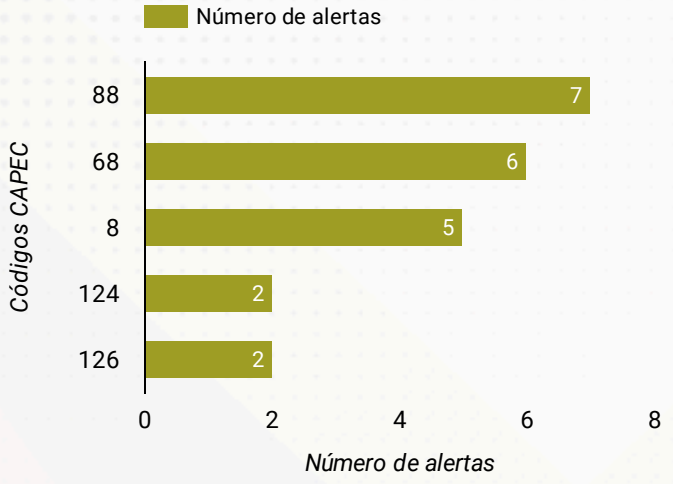
504

Cantidad general de Indicadores recopilados y reportados en el transcurso del mes.

Vulnerabilidades sin criticidad reportada



Top 5 de Códigos Capec con mayor índice de reporte



NÚMERO DE CÓDIGOS CAPEC REPORTADOS

99

NÚMERO DE EVENTOS CON CÓDIGOS CAPEC REPORTADOS

149

Descripción

CAPEC-8: Buffer Overflow in an API Call

Descripción: Un atacante explota un desbordamiento de búfer en una llamada de API para ejecutar código arbitrario. Esto puede permitir al atacante eludir controles de seguridad y ejecutar código malicioso en el sistema objetivo.

CAPEC-88: OS Command Injection

Descripción: Un atacante inserta comandos maliciosos en los campos de entrada de una aplicación web para ejecutar comandos del sistema operativo subyacente con privilegios elevados. Esto puede permitir al atacante tomar el control del sistema objetivo.

CAPEC-80: Using UTF-8 Encoding to Bypass Validation Logic

Este ataque implica manipular la codificación de caracteres para eludir las comprobaciones de validación en un sistema. La codificación UTF-8 es un estándar ampliamente utilizado que representa cada carácter en el conjunto de caracteres Unicode. Al utilizar la codificación UTF-8, los atacantes pueden introducir caracteres que pueden no ser interpretados correctamente por las rutinas de validación del sistema objetivo, lo que permite evitar las comprobaciones de seguridad. Esta técnica puede ser particularmente efectiva contra sistemas que no manejan correctamente la codificación UTF-8 o que no validan correctamente las cadenas de entrada.

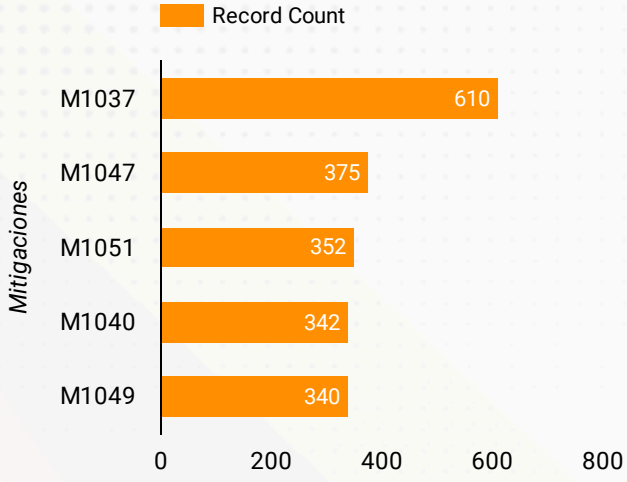
CAPEC-7: Blind SQL Injection

Este ataque se basa en intentar deliberadamente bloquear una cuenta de usuario en un sistema mediante una serie de intentos fallidos de acceso. El objetivo es agotar los intentos de inicio de sesión permitidos, lo que resulta en el bloqueo temporal o permanente de la cuenta afectada. Los atacantes pueden utilizar diversas técnicas, como la fuerza bruta o el uso de contraseñas conocidas o comunes, para intentar iniciar sesión repetidamente en una cuenta hasta que se bloquee.

CAPEC-63: Cross-Site Scripting (XSS)

Descripción: Un adversario incrusta scripts maliciosos en contenido que será servido a navegadores web. El objetivo del ataque es hacer que el software objetivo, el navegador del lado del cliente, ejecute el script con el nivel de privilegio de los usuarios. Un ataque de este tipo explota las vulnerabilidades de los programas que permiten a los hosts remotos ejecutar código y scripts.

Top 5 de Mitigaciones con mayor índice de reporte



NÚMERO DE CÓDIGOS DE MITIGACIÓN REPORTADOS

82

NÚMERO DE EVENTOS CON CÓDIGOS DE MITIGACIÓN REPORTADOS

148

Descripción

M1037 - Filter Network Traffic:
Esta mitigación implica el uso de dispositivos de red para filtrar el tráfico de entrada y salida en una red. También implica la configuración de software en los puntos finales para filtrar el tráfico de red. El objetivo es limitar o bloquear el tráfico malicioso que pueda intentar ingresar o salir de la red, lo que ayuda a prevenir ataques como el tráfico no autorizado, el acceso a recursos no deseados y la comunicación con servidores maliciosos.

M1049 - Antivirus/Antimalware:
Esta mitigación consiste en utilizar firmas o heurísticas en software antivirus o antimalware para detectar y bloquear software malicioso. El antivirus escanea los archivos en busca de patrones conocidos de código malicioso o comportamiento sospechoso, ayudando a proteger los sistemas contra amenazas como virus, gusanos, troyanos y ransomware.

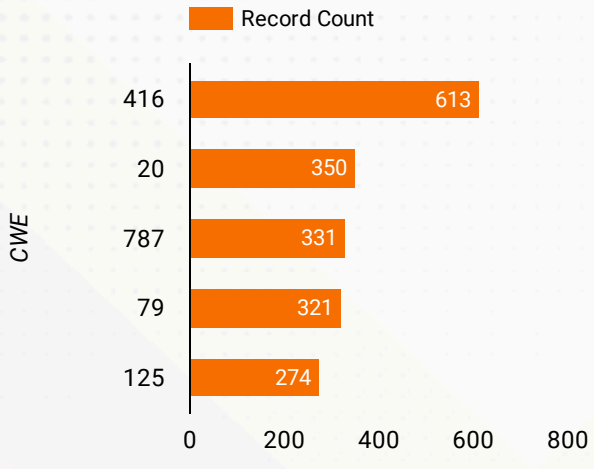
M1047 - Audit:
Esta mitigación implica realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc., para identificar posibles debilidades de seguridad. La auditoría ayuda a detectar y corregir configuraciones incorrectas, vulnerabilidades conocidas y comportamientos sospechosos en los sistemas, lo que mejora la postura de seguridad general y reduce el riesgo de explotación por parte de adversarios.

M1040 - Behavior Prevention on Endpoint:
Esta mitigación consiste en utilizar capacidades de software para prevenir la ocurrencia de patrones de comportamiento sospechoso en sistemas de punto final. Esto puede incluir la detección y prevención de actividades como procesos, archivos o llamadas a API sospechosas que podrían indicar la presencia de malware o actividades maliciosas. Al prevenir estos comportamientos, se reduce el riesgo de compromiso del sistema y la pérdida de datos.

M1048 - Application Isolation and Sandboxing:
Esta mitigación implica restringir la ejecución de código a un entorno virtual en o en tránsito hacia un sistema de punto final. Al aislar las aplicaciones del sistema operativo principal y de otras aplicaciones, se limita el impacto de posibles vulnerabilidades o ataques en una aplicación específica, lo que ayuda a prevenir la propagación de malware y la explotación exitosa de vulnerabilidades.

Las mitigaciones de MITRE, en el ámbito de la ciberseguridad, se refieren a las estrategias y técnicas implementadas para reducir o prevenir vulnerabilidades y amenazas en sistemas informáticos. MITRE, una organización sin fines de lucro, desarrolla y mantiene un marco de mitigación ampliamente utilizado en el sector de la seguridad. Este marco proporciona una guía detallada sobre cómo abordar y contrarrestar vulnerabilidades específicas, ofreciendo recomendaciones prácticas y soluciones técnicas.

Top 5 de Códigos CWE con mayor índice de reporte



NÚMERO DE CÓDIGOS CWE REPORTADOS

92

NÚMERO DE EVENTOS CON CÓDIGOS CWE REPORTADOS

494

Descripción

CWE-416: Use of Uninitialized Variable:
Este error ocurre cuando un programa utiliza una variable antes de asignarle un valor inicial. Esto puede conducir a comportamientos inesperados, incluidos fallos en la ejecución del programa o resultados incorrectos.

CWE-79: Cross-Site Scripting (XSS):
El Cross-Site Scripting (XSS) es una vulnerabilidad que permite a los atacantes insertar scripts maliciosos en páginas web vistas por otros usuarios. Esto puede ocurrir cuando una aplicación web no valida correctamente la entrada del usuario y luego incluye esta entrada no validada en las páginas web devueltas al navegador del usuario.

CWE-787: Out-of-bounds Write:
Este tipo de vulnerabilidad ocurre cuando un programa intenta almacenar más datos en un búfer de los que puede contener, lo que puede resultar en la sobrescritura de datos adyacentes en la memoria. Esto puede ser aprovechado por un atacante para ejecutar código malicioso o causar una denegación de servicio.

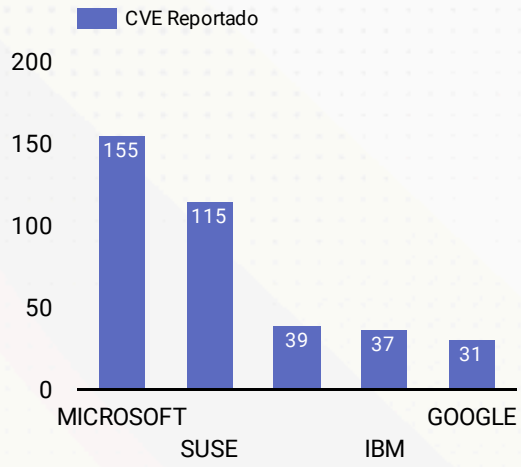
CWE-20: Improper Input Validation:
Esta debilidad de seguridad ocurre cuando un programa no valida correctamente los datos de entrada antes de procesarlos. Esto puede llevar a una variedad de ataques, como inyección de código, denegación de servicio o manipulación de datos.

CWE-125: Reuse of a Non-Returnable Resource:
Esta debilidad de seguridad ocurre cuando un sistema utiliza la misma clave para múltiples instancias de cifrado o autenticación. Esto puede hacer que el sistema sea vulnerable a ataques criptográficos, como el cifrado de texto plano o la autenticación débil.

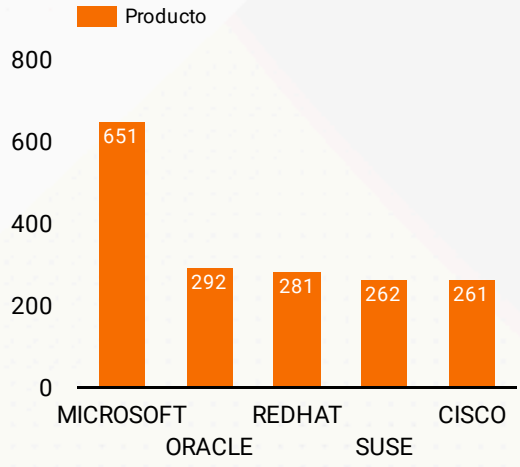
Los códigos CWE (Common Weakness Enumeration) se utilizan para identificar y categorizar debilidades comunes de seguridad en software y sistemas. Estos códigos son una lista numérica y alfanumérica que asigna un identificador único a cada tipo de debilidad o vulnerabilidad de seguridad conocida. CWE se utiliza para estandarizar la comunicación y la identificación de vulnerabilidades en el campo de la seguridad informática, lo que facilita el análisis, la mitigación y la corrección de estos problemas. Los códigos CWE son ampliamente utilizados en la industria de la ciberseguridad y son una parte fundamental de muchas prácticas y herramientas de seguridad.

MNEMO

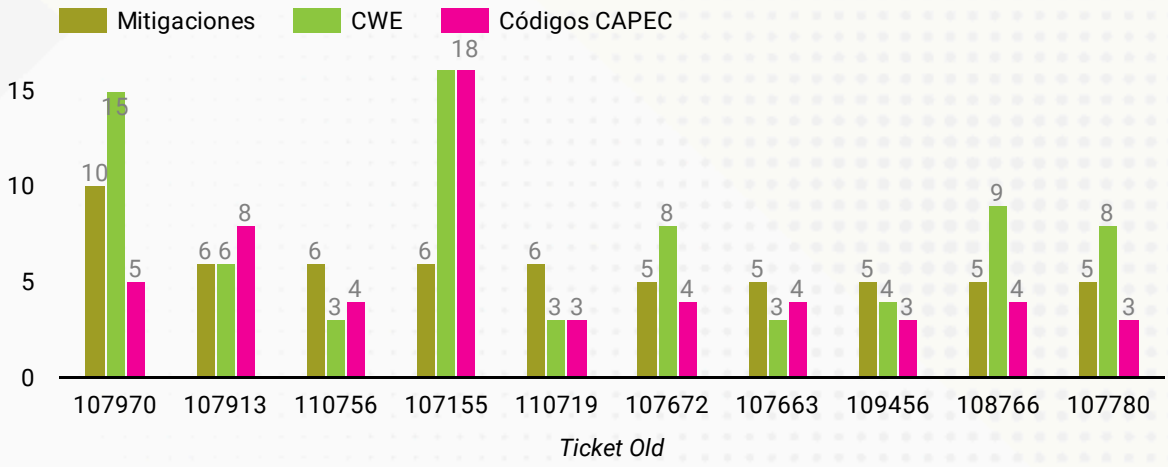
Top 5 de fabricantes con base en CVE reportados



Top 5 de fabricantes con base en Productos reportados



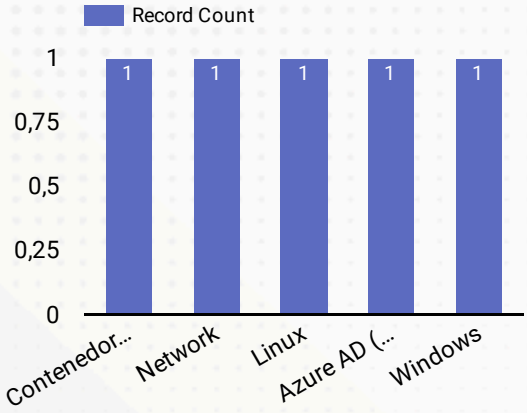
Comparativa TOP 10 tikets reportados Mitigaciones, Técnicas, Tácticas Mitre ATT&CK

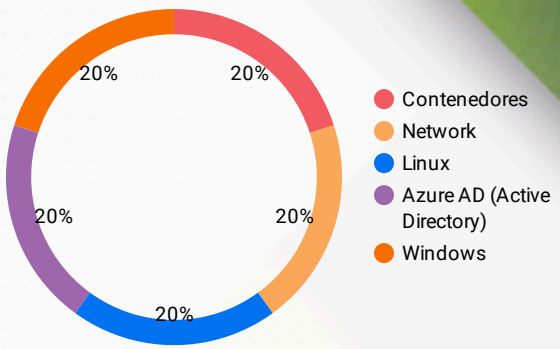


CYBER THREAT INTELLIGENCE

MNEMO

Top 5 de plataformas afectadas

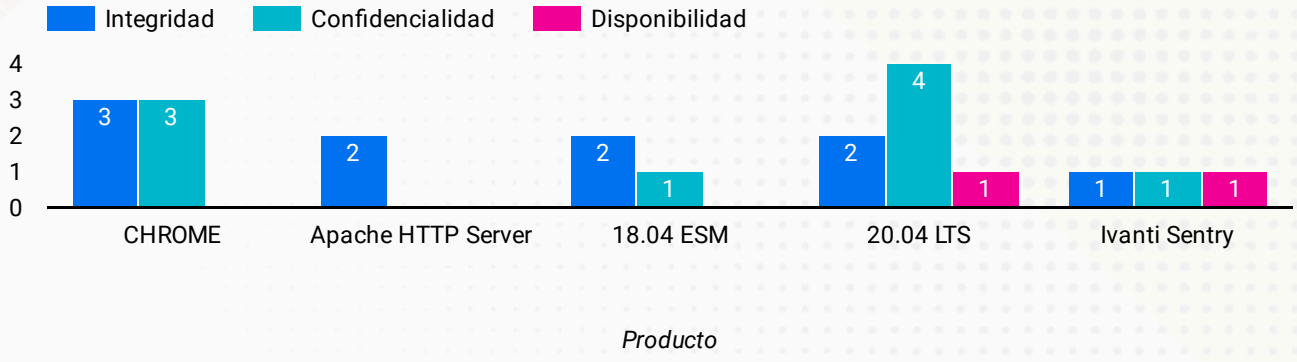




Tener en cuenta las tácticas de MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es fundamental en ciberseguridad por varias razones:

Detección y respuesta avanzadas: Las tácticas de MITRE ATT&CK proporcionan una estructura sólida para comprender cómo los atacantes operan y qué objetivos persiguen. Al conocer estas tácticas, las organizaciones pueden mejorar su capacidad para detectar comportamientos maliciosos tempranamente y responder de manera más efectiva a los incidentes de seguridad.
Evaluación de amenazas y riesgos: Al analizar las tácticas utilizadas en ataques anteriores o en amenazas específicas, las organizaciones pueden evaluar mejor los riesgos que enfrentan y tomar medidas proactivas para mitigarlos.
Fortalecimiento de defensas: Las tácticas de MITRE ATT&CK ayudan a las organizaciones a identificar posibles puntos débiles en sus sistemas y redes. Esto permite tomar medidas para fortalecer las defensas y prevenir ataques antes de que ocurran.
Comunicación y colaboración: MITRE ATT&CK proporciona un lenguaje común para la comunicación entre profesionales de la ciberseguridad, lo que facilita la colaboración en la identificación y mitigación de amenazas.
Evaluación de soluciones de seguridad: Las organizaciones pueden utilizar las tácticas de MITRE ATT&CK como un marco de referencia para evaluar y comparar soluciones de seguridad, asegurándose de que estén alineadas con las amenazas y tácticas más relevantes.

Top de Fabricantes y su afectación sgsi



MNEMO

CYBER THREAT INTELLIGENCE

by MNEMO

CYBER THREAT INTELLIGENCE

by MNEMO

INFORME
Cyber Security Warning - Preventive

ABRIL 2024

ELABORADO POR:
EQUIPO CYBER THREAT INTELLIGENCE <CTI>

MNEMO

INDICADORES GENERALES ---------- PAG.03

TOP ACTORES Y VECTORES ---------- PAG.04

TOP INDICADORES ---------- PAG.05

TOP TÁCTICAS, TÉCNICAS, MITIGACIONES -------- PAG.06

TOP PRODUCTOS Y SECTORES ---------- PAG.07

TOP PAISES ---------- PAG.08

TOP CAPEC Y DATASOURCE ---------- PAG.09

GLOSARIO ---------- PAG.10

MNEMO

Abril 2024

INDICADORES GENERALES

Número de alertas

52

Cantidad

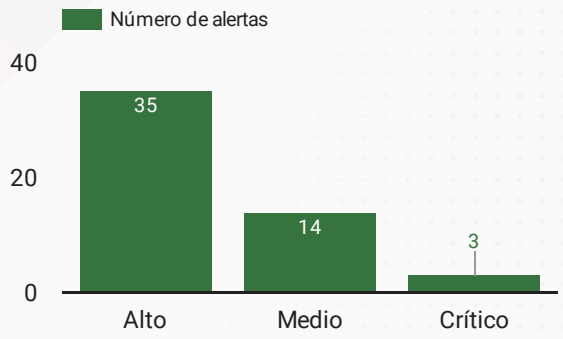
23.863

Alertas y eventos MISP reportados

IoC Reportados

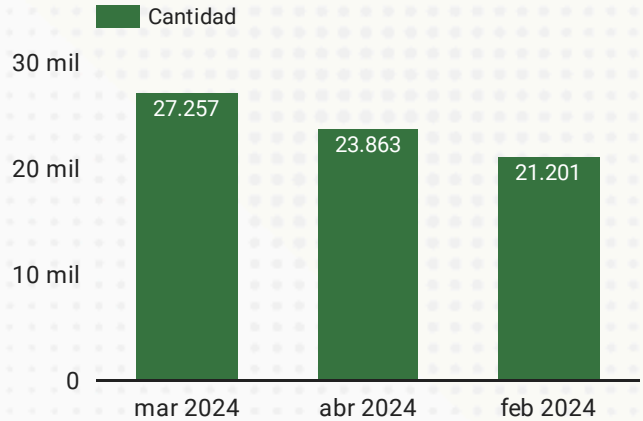
En el presente gráfico, podemos apreciar los datos generales recopilados a lo largo de abril. En la parte superior izquierda encontramos el gráfico que relaciona el número total de alertas que se podrían verificar en el entorno MISP, mientras que en el gráfico superior derecho veremos el número de indicadores de compromiso reportados a lo largo del mismo periodo.

De igual manera, en los gráficos inferiores veremos la relación comparativa de los últimos tres meses. El gráfico de la derecha nos muestra la relación comparativa de IoC (Indicadores de Compromiso) reportados, y en la parte izquierda, los niveles de criticidad de las alertas reportadas en el transcurso del mes.



Alertas por criticidad

Comparativa Trimestral IOC

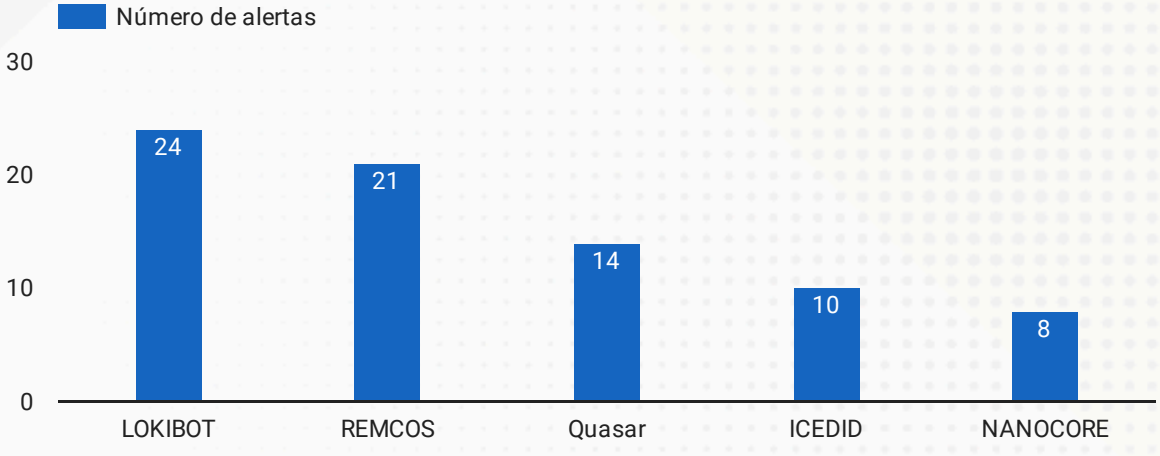


La comparativa superior se realiza en periodos de 1 a 30 de cada mes

Top 5 actores de amenaza identificados según número de alertas reportadas

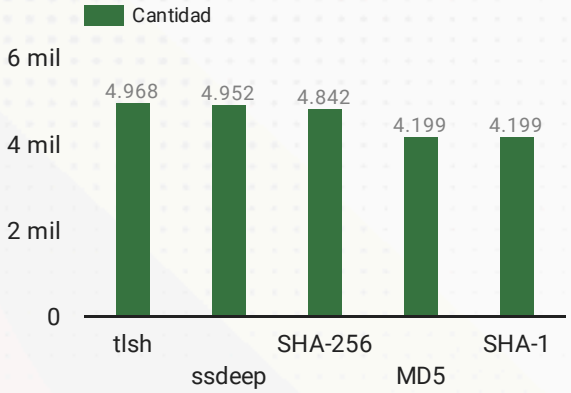
Los gráficos hacen referencia a datos recopilados durante de abril. En la parte superior, podemos ver los actores de amenazas relacionados por el número de alertas reportadas, siendo estos los cinco principales de abril. En la parte inferior, se encuentran los gráficos que representan la recopilación de datos para presentar los cinco tipos de malware reportados durante el mismo periodo. Estos datos son el resultado del número de alertas que hacían referencia a su uso a lo largo de abril.

Top 5 Malware identificados según número de alertas reportadas

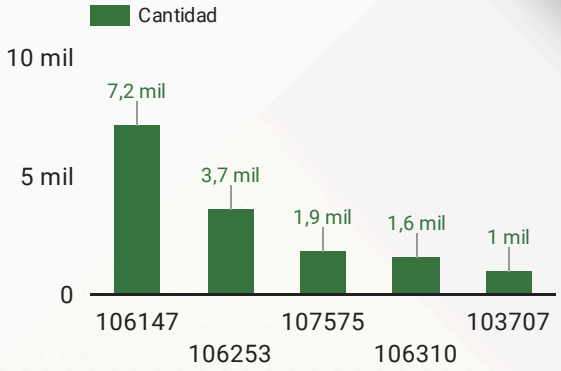


MNEMO

Top 5 de los tipos de indicadores más reportados en el mes



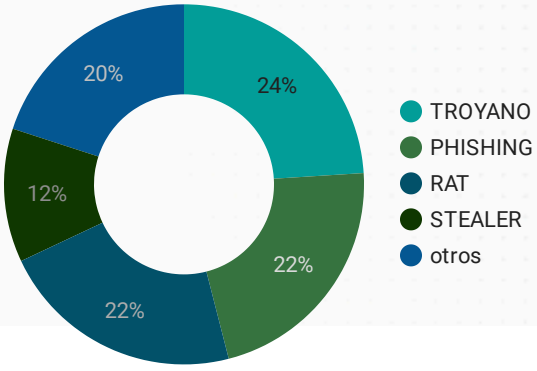
Top 5 de las alertas con mayor número de IoC reportados en el mes



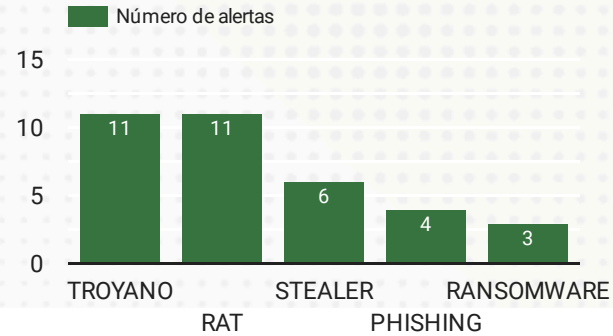
En los siguientes gráficos podemos ver datos recopilados a lo largo de abril. Los dos gráficos superiores son el resultado de la relación del número de IoC (Indicadores de Compromiso) reportados. El gráfico superior izquierdo muestra los tipos de IoC por cantidad reportada, mientras que en el gráfico superior derecho se puede observar el número de IoC reportados en cada alerta, siendo estos los cinco principales.

En la parte inferior izquierda se encuentran los cinco vectores más reportados relacionados en el transcurso del mismo periodo, en términos de porcentaje de uso en las alertas y cantidad reportada. En el gráfico inferior derecho se presenta el mismo resultado, pero esta vez en función del número de veces relacionado a lo largo del mismo periodo.

Top 5 vectores de ataque más relevantes en el transcurso del mes por número de reportes

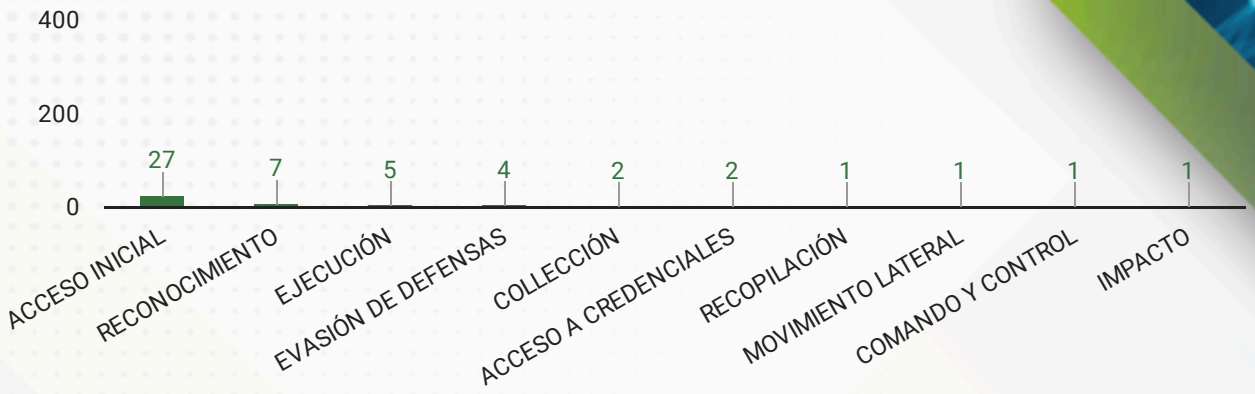


Número de alertas correspondientes al top 5 vectores



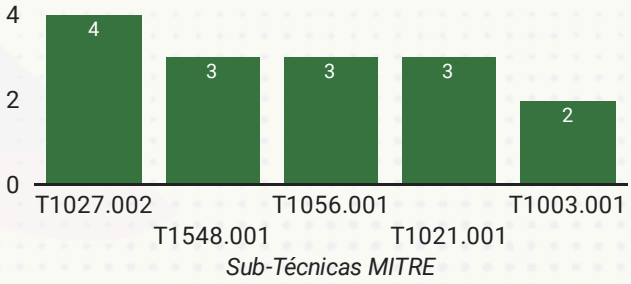
MNEMO

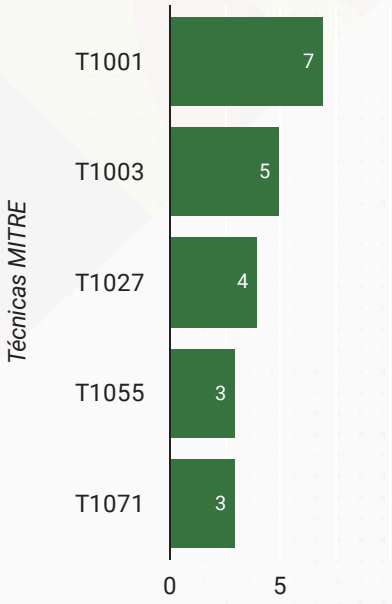
10 Tácticas reportadas en el transcurso del mes



En la parte superior se encuentran las 10 tácticas más reportadas durante de abril, mientras que en la parte inferior izquierda se encuentran las 5 técnicas más reportadas. En la parte inferior derecha, podemos ver las 5 mitigaciones más reportadas en relación con las contramedidas preventivas según el framework Mitre. En la parte inferior central, encontraremos las 5 sub-técnicas más reportadas en el transcurso de abril. Todas las mencionadas anteriormente deben tenerse en cuenta al ser utilizadas para prevenir incidentes derivados de los tipos de malware reportados durante el mismo período.

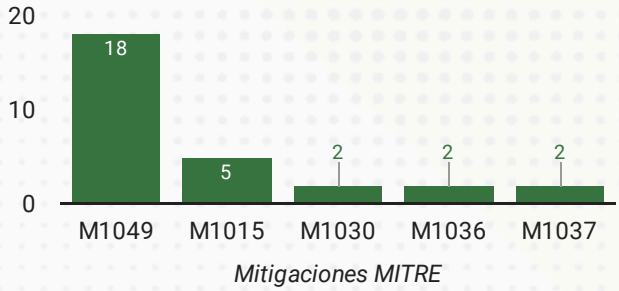
Top 5 de las sub-técnicas más reportados en el mes





Top 5 de las técnicas más reportados en el mes

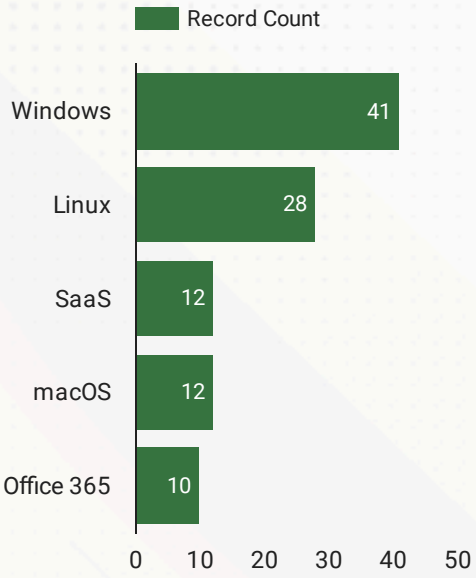
Top 5 de los códigos mitigación más reportados en el mes



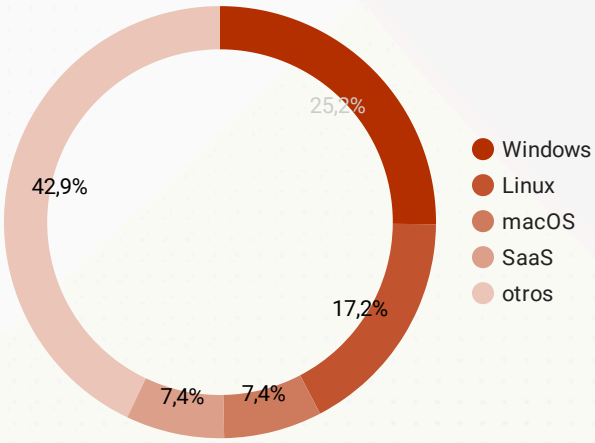
CYBER THREAT INTELLIGENCE

MNEMO

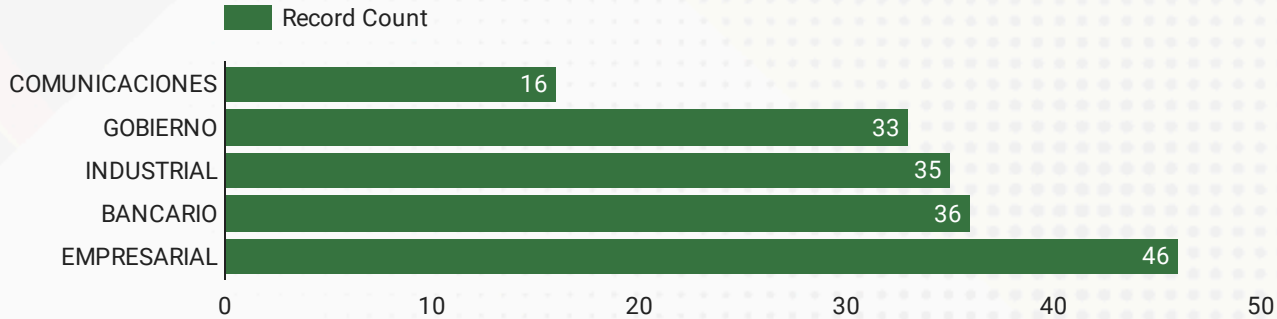
Top 5 productos más afectados en el transcurso del mes

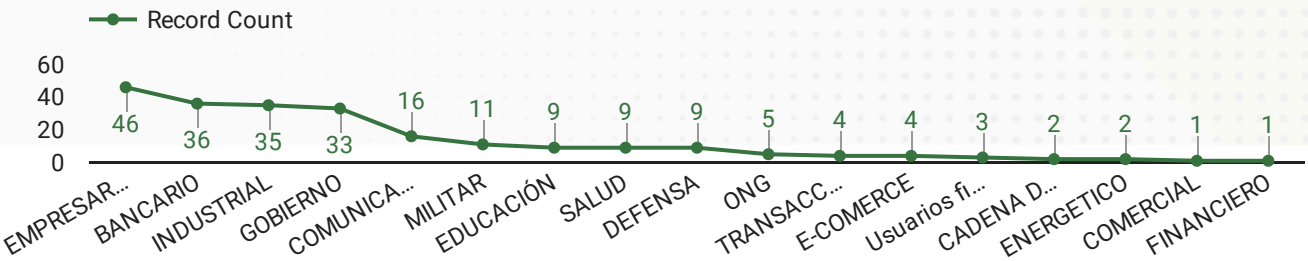


% de participación e incidencia en los productos, en cuanto a las alertas reportadas en el mes

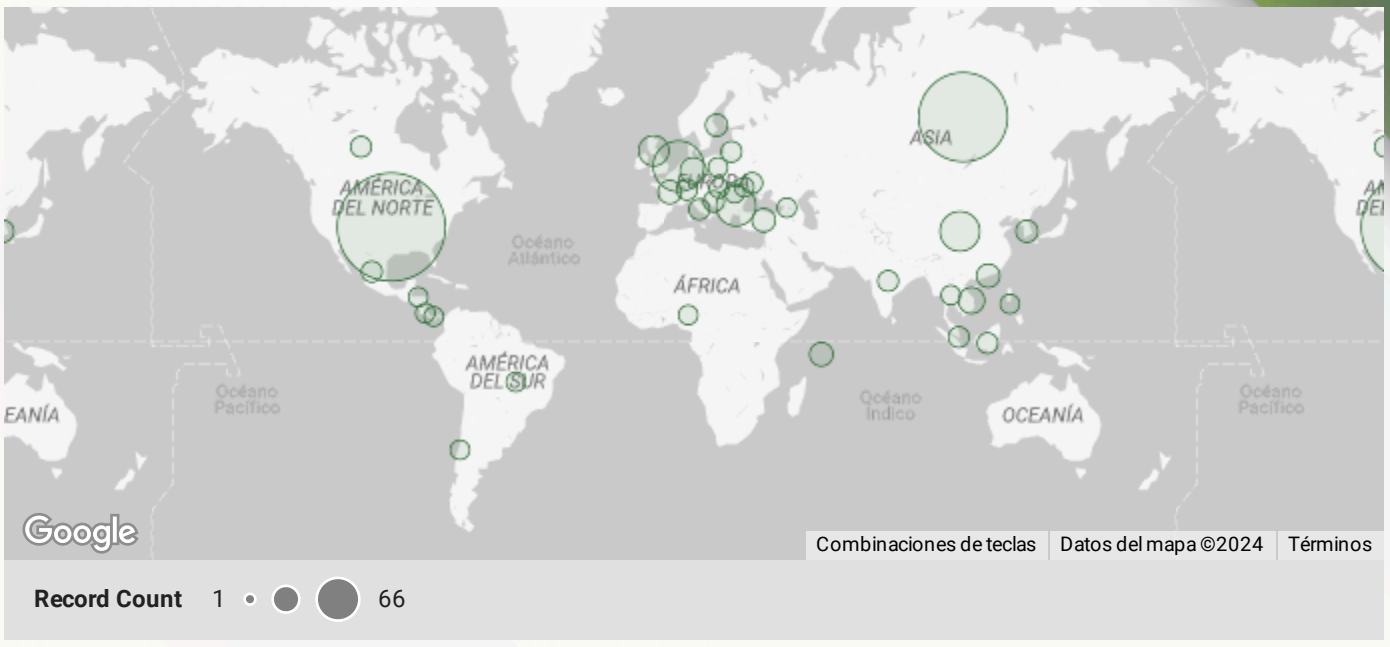


En la parte superior izquierda se muestran los productos más afectados, según lo que muestra el framework de Mitre, en relación a las técnicas reportadas en las alertas de abril. De igual manera, en la parte superior derecha se presenta este mismo resultado, pero en términos de porcentaje de participación con respecto a las alertas reportadas.
En la parte inferior se detallan los sectores que podrían verse afectados en relación a las alertas reportadas y que podrían sufrir los impactos de los malware mencionados. El sector empresarial, que engloba la mayoría de las empresas comerciales, podría ser especialmente vulnerable a los malware durante el transcurso del mismo periodo, debido a su grado de susceptibilidad.





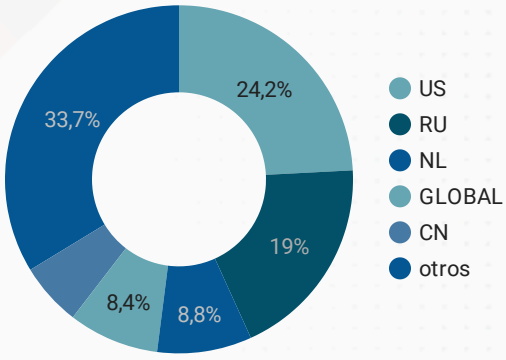
Top 10 países afectados según número de alertas reportadas

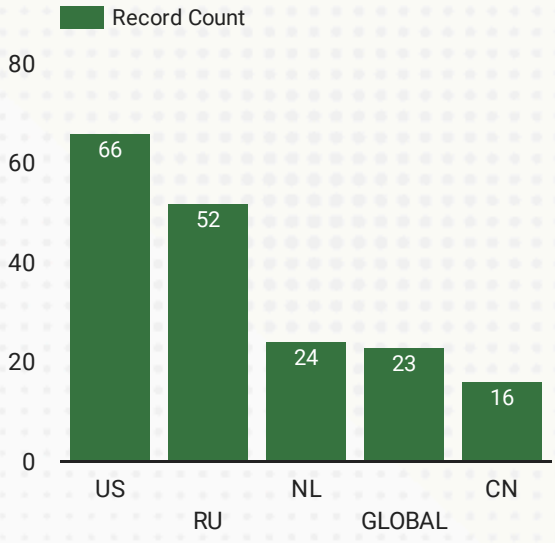


En los gráficos de esta página, podemos observar la afectación de países según el número de alertas reportadas en las que se mencionó su afectación. En la parte superior se encuentra el mapa de calor, donde la intensidad del color representa el nivel de afectación.

En la parte inferior izquierda, encontramos el top 5 de los países afectados, expresado como porcentaje de afectación con respecto a las alertas en las que se reportó su afectación. El gráfico de la derecha muestra el número de alertas en las que se reportó la afectación de estos países.

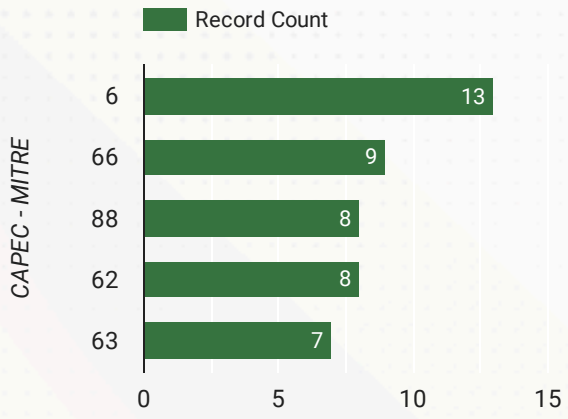
Es importante destacar que, aunque no se muestra gráficamente, Colombia se encuentra en el puesto 4 según nuestro número de alertas reportadas teniendo encuenta la afectacion global.



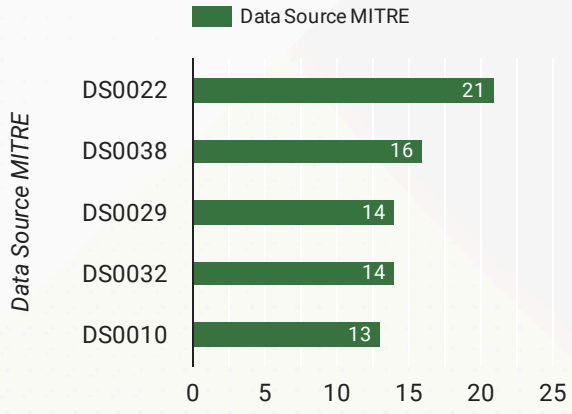


MNEMO

Top 5 Códigos Capec reportados según número de alertas reportadas



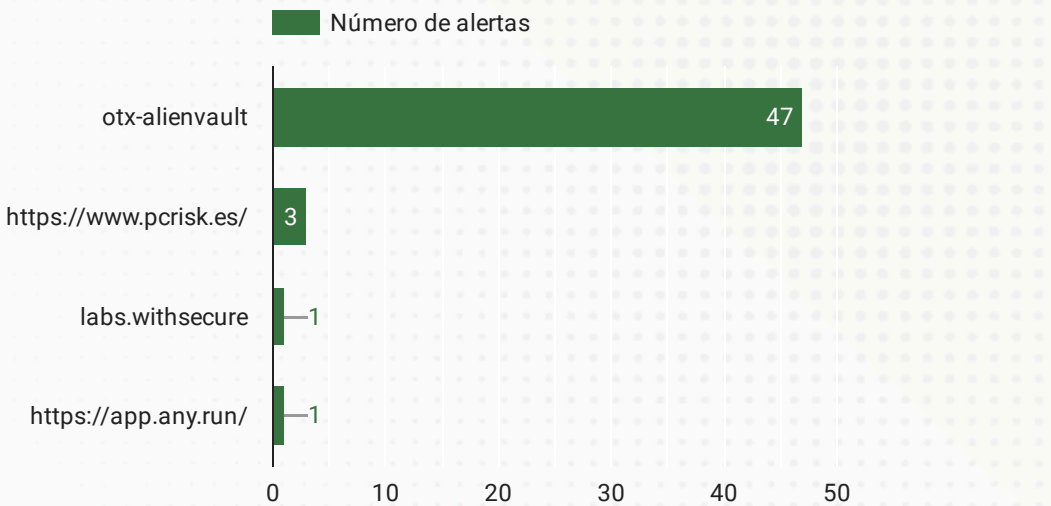
Top 5 Códigos Datasource reportados según número de alertas reportadas



En esta página, se encuentran tres gráficos. En los de la parte superior, se relacionan los cinco principales códigos CAPEC y códigos Datasource, que forman parte del framework de MITRE. Estos dos tipos de códigos se derivan de las técnicas utilizadas y reportadas en las alertas. Es importante señalar que se pueden verificar cada uno de ellos según lo que gestiona y comparte de manera predeterminada cada técnica, lo cual está disponible en la plataforma de MITRE.

En la parte inferior, se presentan las fuentes más utilizadas. Estos gráficos son el resultado del número de veces que se reportaron durante el mes de abril.

Top 5 Fuentes mas usadas tomando el número de alertas reportadas



CYBER THREAT INTELLIGENCE

MNEMO

GLOSARIO

MARCO MITRE ATT & CK:

(Adversarial Tactics, Techniques, and Common Knowledge) es un marco de referencia ampliamente utilizado en ciberseguridad que describe tácticas, técnicas y procedimientos comunes utilizados por ciberdelincuentes en sus ataques. Proporciona un catálogo detallado de comportamientos adversarios, lo que ayuda a las organizaciones a comprender mejor las amenazas y a fortalecer sus defensas cibernéticas al identificar cómo los atacantes pueden comprometer sistemas y redes. Es una herramienta esencial para la detección, respuesta y mitigación de amenazas en el campo de la seguridad informática.

CÓDIGOS MITIGACIÓN:

Las mitigaciones representan conceptos de seguridad y clases de tecnologías que se pueden usar para evitar que una técnica o subtécnica se ejecute con éxito.
En total existen 43 mitigaciones diferentes en el marco de relevancia MITRE.

CÓDIGOS ATT&CK :

MITRE presentó ATT&CK (tácticas, técnicas y conocimiento común de adversarios) en el 2013 como una forma de describir y clasificar los comportamientos adversarios con base en observaciones reales.

CÓDIGOS DETECCIÓN :

Esta la forma alfanumérica en la que la corporación MITRE ha logrado clasificar medidas de control para lograr ejecutar las técnicas de detección que son necesarias para evitar los diferentes ataques que ejercen los grupos de ciberdelincuentes con los diferentes software aplicados para hacer daño a nuestras compañías.

CÓDIGOS CAPEC:

Con sus siglas en ingles: (Common Attack Pattern Enumeration and Classification) es un catálogo de patrones de ataque que se encarga de recolectar información sobre ellos, junto a un esquema de clasificación exhaustiva.

NOTA IMPORTANTE:

Existen en la clasificación de la matriz de MITRE las Técnicas y dentro de ellas las subtécnica, también cabe señalar que la Matriz contiene información para las siguientes plataformas: Windows , macOS , Linux , PRE , Azure AD , Office 365 , Google Workspace , SaaS , IaaS , Network , Containers .

CYBER THREAT INTELLIGENCE

by MNEMO

Colombia

T: (+57) (601) 552 72 10
C: (+57) 318 486 9055
Calle 99 No.10-19
Oficina 502
Trade Center 99 Bogotá D.C

España

T: (+34) 91 417 67 76
Cardenal Marcelo
Spínola 14
Planta 5
28016 Madrid

Panamá

Oceanía Business Plaza
Torre 1000, Piso 23,
Oficina 23C, Punta
Pacífica, Panamá

MNEMO

SECURITY OPERATION CENTER
INFORME EJECUTIVO

1 de Abril al 30 de Abril de 2024

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

Contenido

1 OBJETIVO

2 ALCANCE

3 TIPOS DE FUENTE DE INFORMACIÓN

4 EVENTOS DE SEGURIDAD REPORTADOS

5 GENERALIDADES

6 RECOMENDACIONES Y CONCLUSIONES

7 SLA'S

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.

MNEMO

OBJETIVO

Presentar los resultados del servicio de correlación, analítica y monitoreo de eventos de seguridad y ciberseguridad, ejecutado por el equipo SOC-CERT de Mnemo Colombia S.A.S., permitiendo contar con la visibilidad de eventos y/o posibles ataques a la infraestructura que soporta los productos, servicios, canales y activos tecnológicos del Ministerio de Hacienda y Crédito Publico (MHCP), correspondiente al periodo entre 01 de Abril al 30 de Abril de 2024, basado en las fuentes de información integradas en la actualidad.

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.

ALCANCE

Exponer los eventos identificados en el servicio de monitorización ejecutado por SOC-CERT de Mnemo Colombia durante el periodo comprendido entre el 01 de Abril al 30 de Abril de 2024. Abarcando los siguientes temas

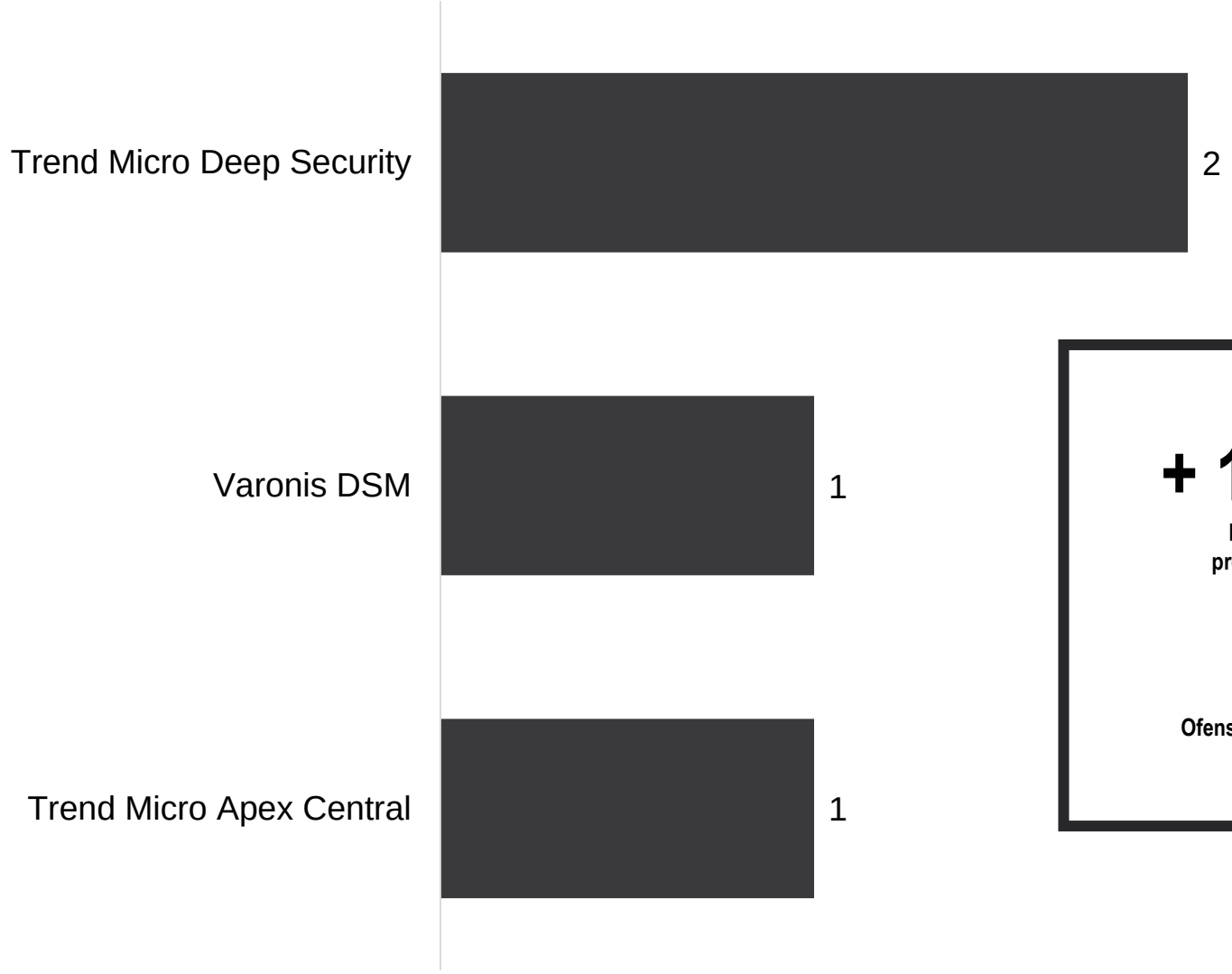
Los temas a tratar sobre este informe son:

- Descripción de fuentes de información
- Taxonomía definida y eventos de casos de uso
- Resumen de incidentes y temas asociados al servicio.
- Recomendaciones.

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.

MNEMO

Tipos de fuentes de información



+ 141M
Eventos procesados

4
Fuentes activas

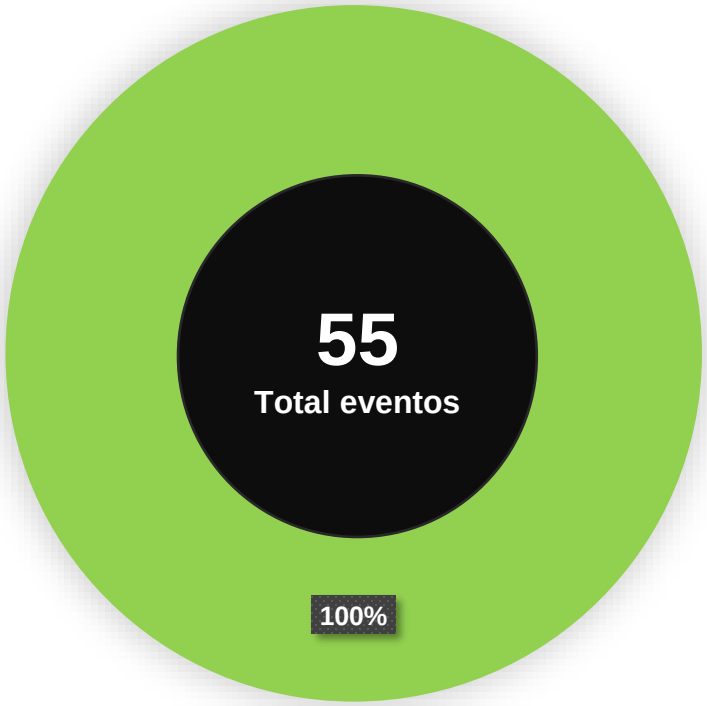
387
Ofensas identificadas

54
EPS

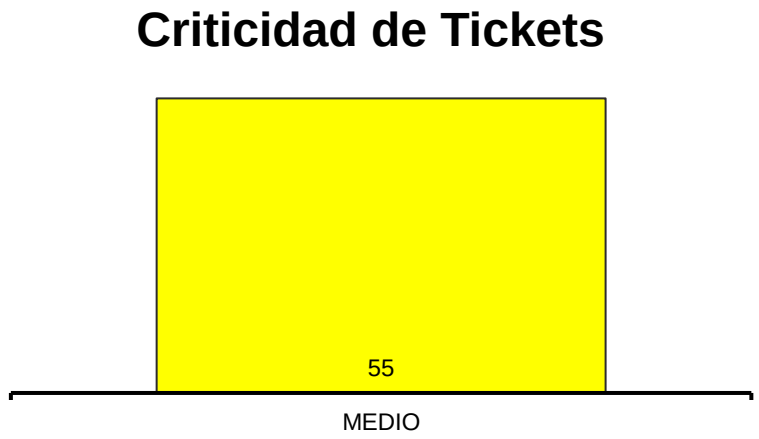
MNEMO

Eventos Reportados

Los tickets que son creados llegan automáticamente pueden ser verificados por la entidad y el personal de SOC de MNEMO queda a espera del procesamiento interno del mismo, el cual debería resultar en una validación del evento y definir si se trata o no de un incidente.



Ninguno de los eventos reportados indican ataques exitosos.

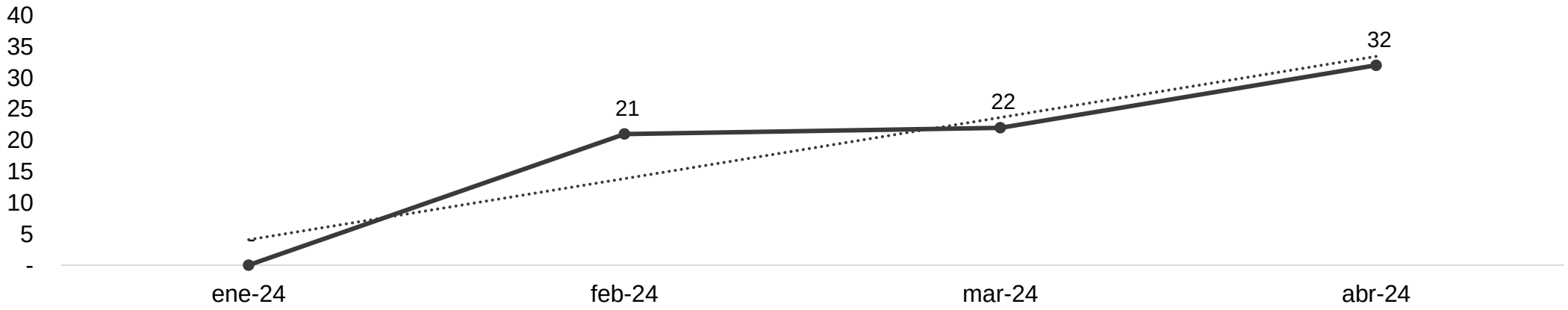


MNEMO

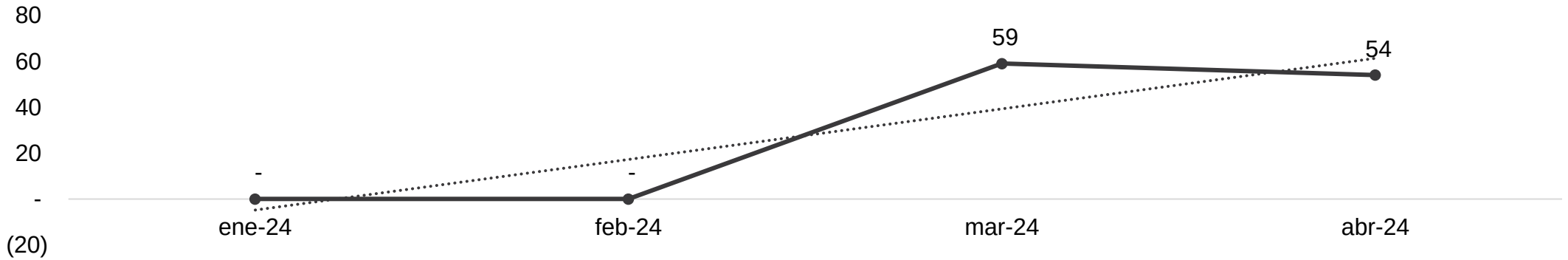
Generalidades

A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología, dando el comportamiento.

Casos de uso mensual

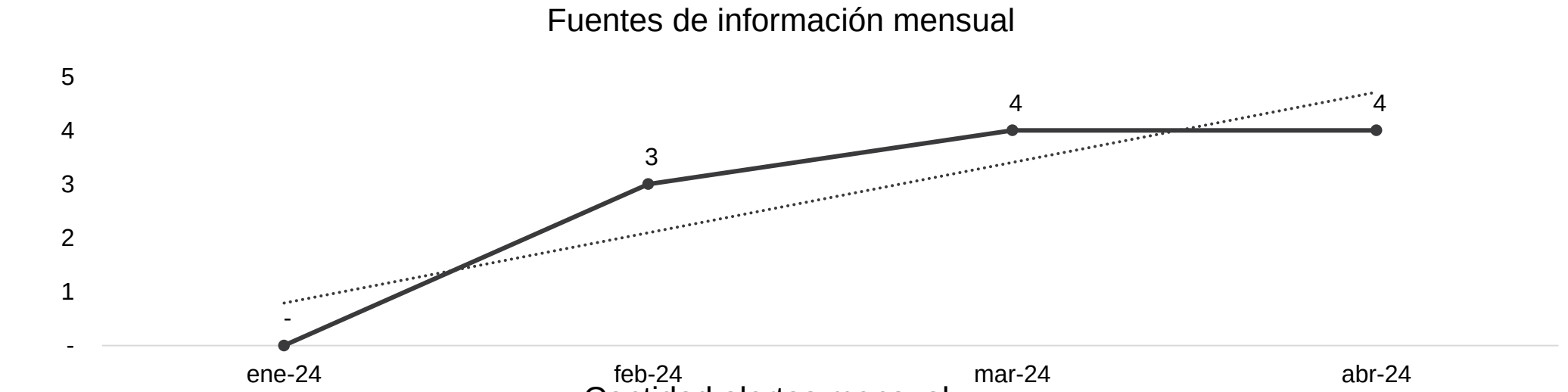


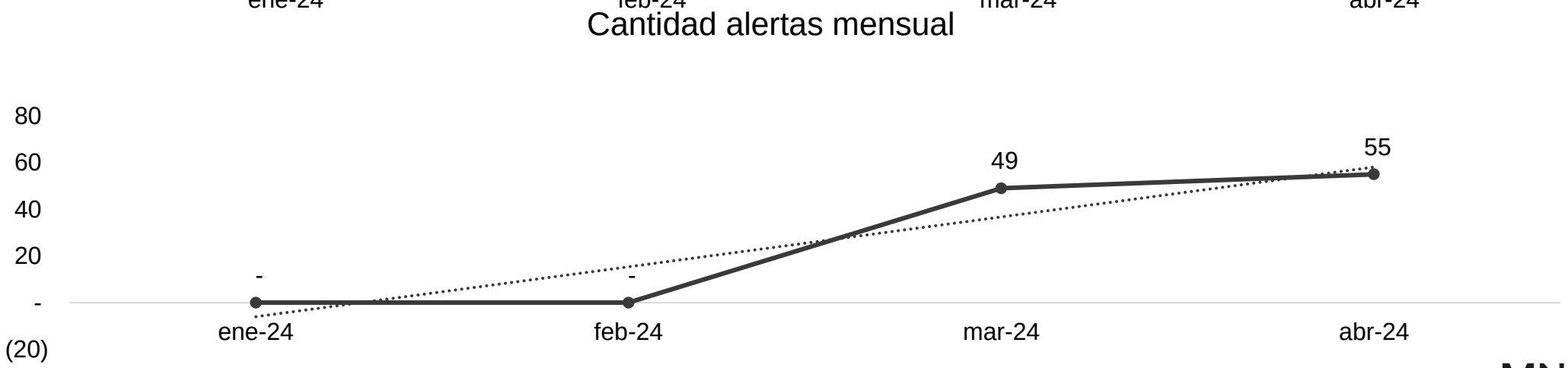
EPS mensual promedio



Generalidades

A continuación, se presentan las estadísticas generales a nivel de servicio y tecnología, dando el comportamiento.





Recomendaciones y conclusiones

- Se recomienda continuar con el constante análisis de los eventos reportadas por el equipo SOC para continuar el seguimiento de alertas y comportamientos que presenten alguna amenaza en la entidad.

- Continuar con la constante validación de los casos de uso durante las sesiones semanales
- Se recomienda reforzar la capacitación del personal perteneciente a la organización respecto a temas de ciberseguridad con el fin de que se evite ser víctima de campañas de phishing.

- Se recomienda reforzar la capacitación del personal perteneciente a la organización para prevenir la instalación de software que viole las leyes de derechos de autor y que contengan posible malware.

Tipos de peticiones SLA'S

A continuación, se presenta las peticiones realizadas:

criticidad	Máx. de diferencia	Promedio de diferencia	Mín. de diferencia
Bajo	00:00:00	00:00:00	00:00:00
Medio	00:58:00	00:26:41	00:05:00
Alto	00:00:00	00:00:00	00:00:00
Total general	00:58:00	00:26:41	00:05:00

CRITICIDAD	CUMPLIMIENTO	SLA	TIEMPO MAX. SLA
Bajo	100%	120 MINUTOS	02:00:00
Medio	100%	60 MINUTOS	01:00:00
Alto	100%	30 MINUTOS	00:30:00

MNEMO

www.mnemo.com

@MNEMO_Colombia

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL.
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Derechos de Propiedad ©Mnemo Colombia S.A.S. Todos los derechos reservados.

MNEMO

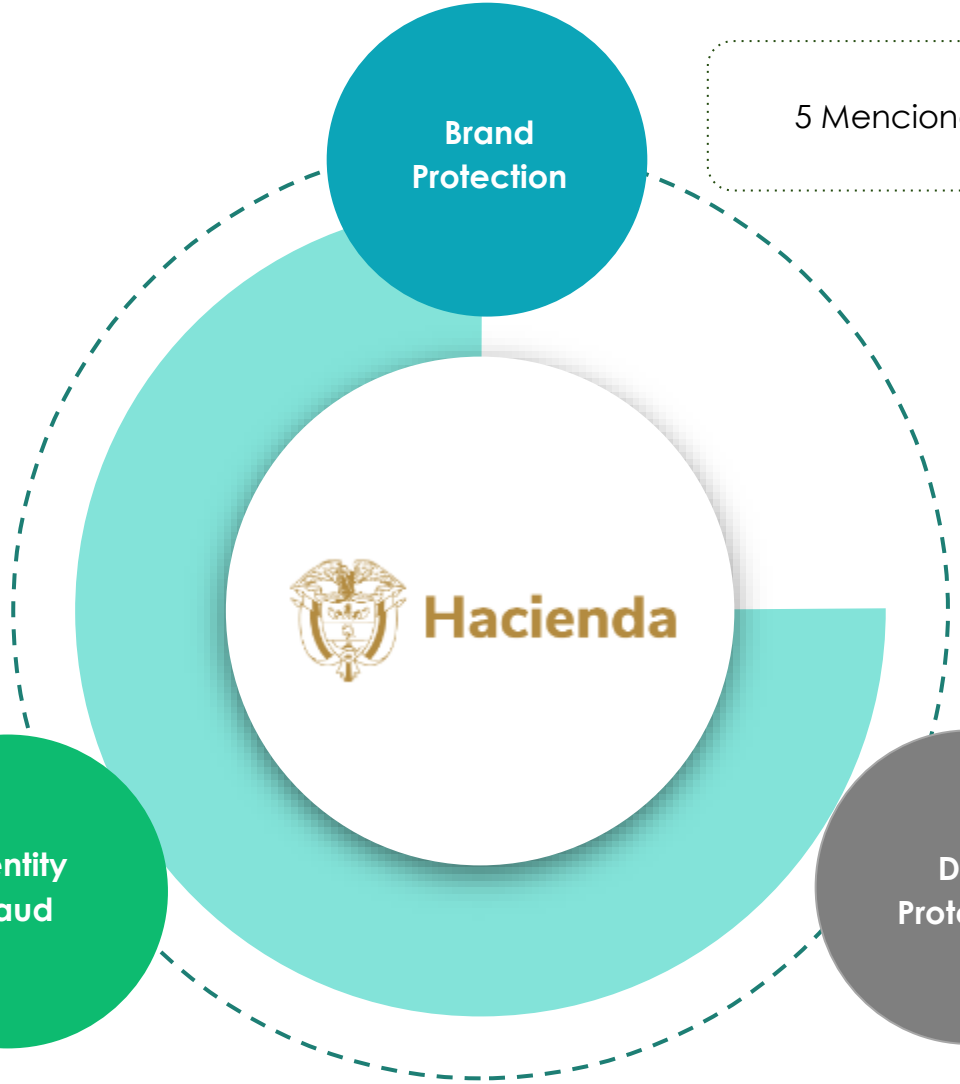
INFORME MENSUAL DE VIGILANCIA ABRIL 2024

03/05/2024

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

KPIs > Resumen de Eventos



5 Menciones de marca

1 Dominio sospechoso
4 Abusos de marca en RRSS

4 Credenciales de terceros
4 Credenciales de empleados

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

MNEMO

Servicio de Vigilancia

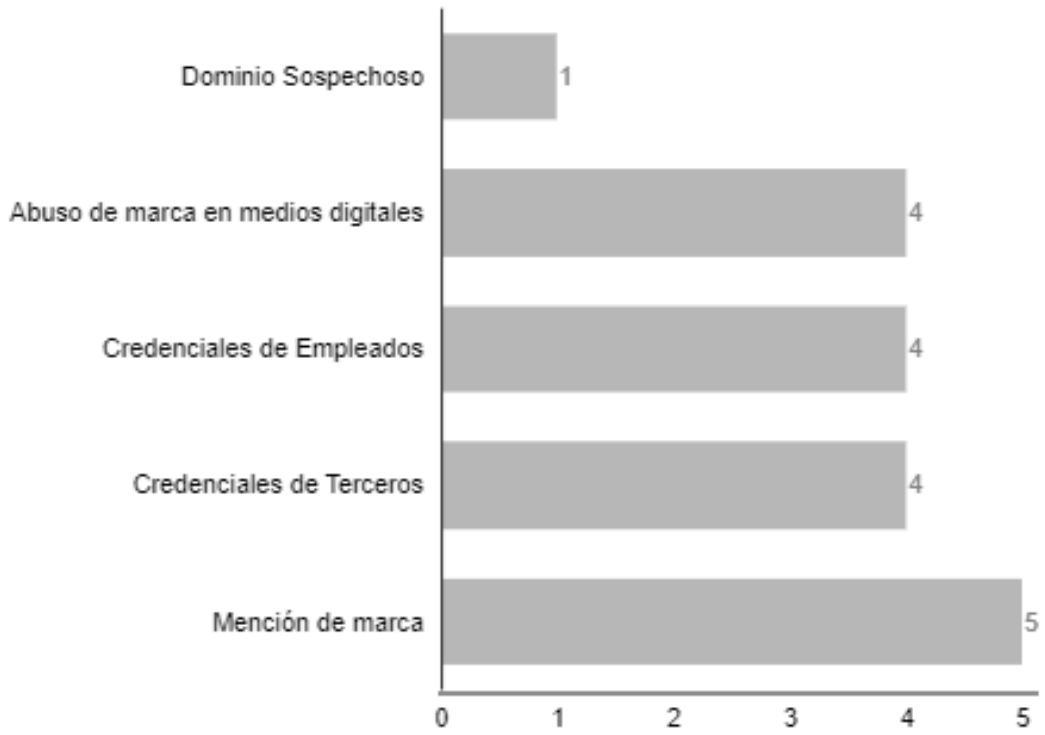
RESUMEN EJECUTIVO

- Se identificaron **4 eventos notificados** bajo la tipología **Abuso de marca** los cuales hacen **uso del nombre de la entidad**.

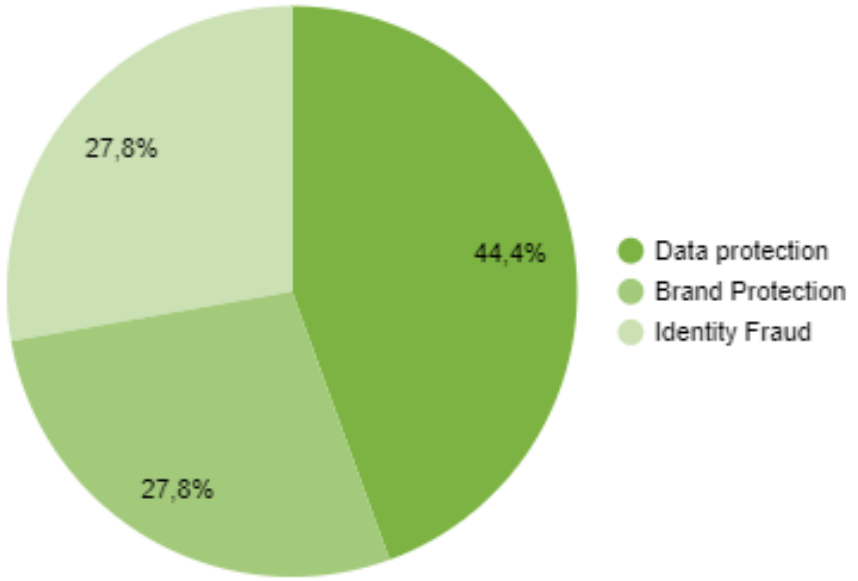
Servicio de Vigilancia

KPIs > Comportamiento del servicio global Vigilancia

Nº Total de Alertas enviadas: 18



% de afectación por subservicio

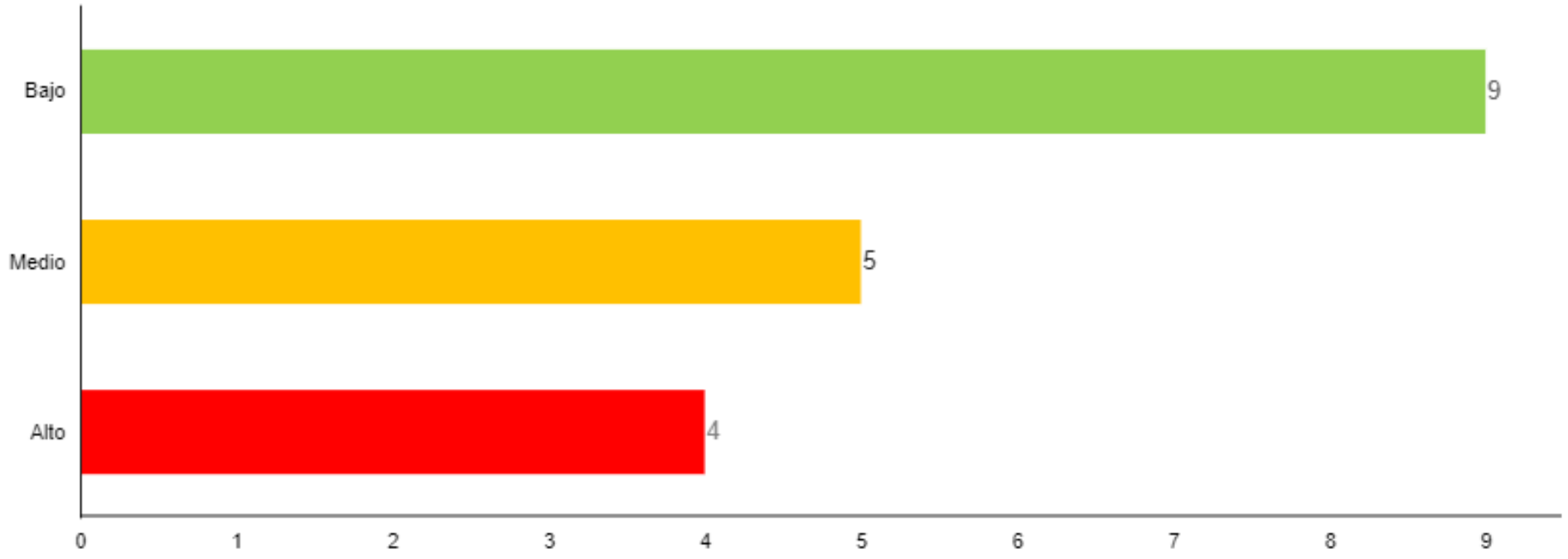


NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

KPIs > Comportamiento del servicio global Vigilancia

Alertas clasificadas por criticidad



NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

SLAs

Criticidad	SLA "Tiempo de respuesta"	
	Cumple	Grado de Cumplimiento
Alta (respuesta <=60 min)	Sí	100%
Media (respuesta <=120 min)	Sí	100%
Baja (respuesta <=240 min)	Sí	100%

Comentarios a los SLAs:

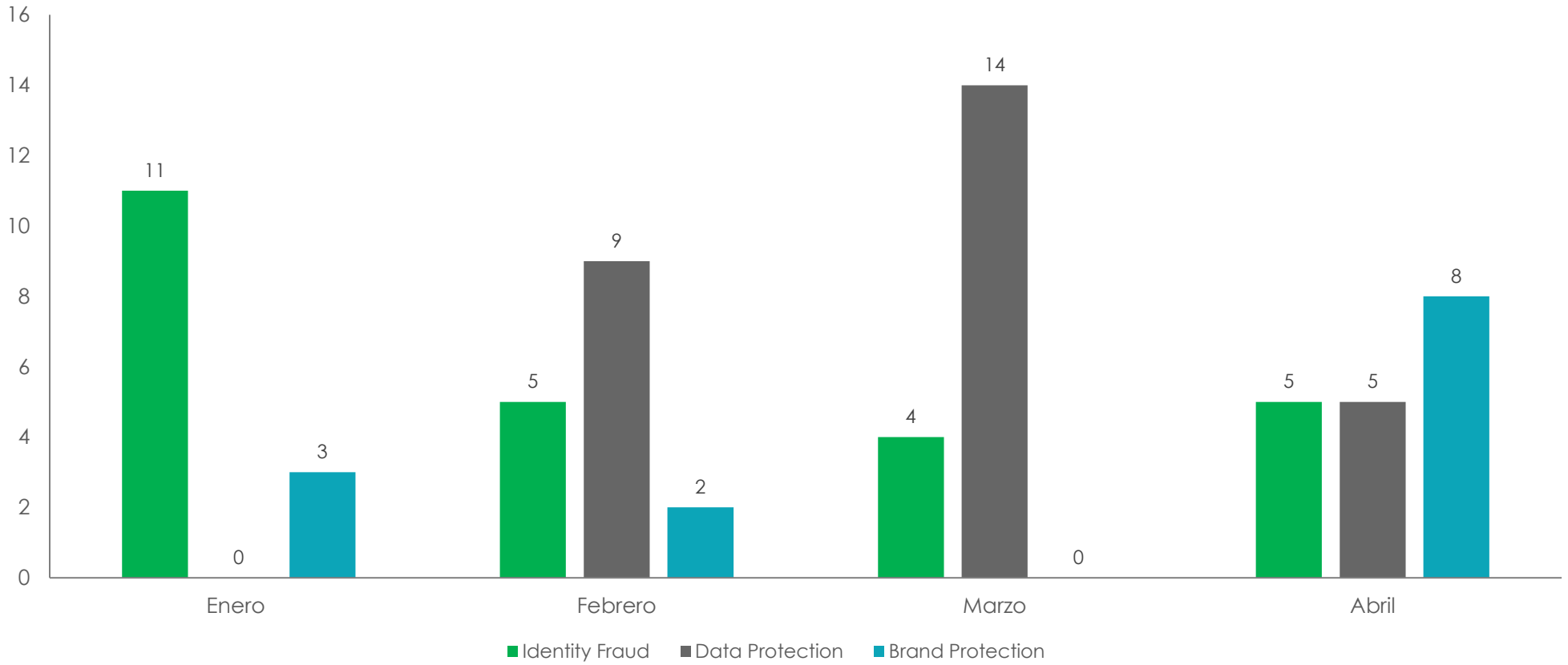
- Sin comentarios para el mes de abril de 2024.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

MNEMO

Servicio de Vigilancia

Histórico > Evolución del servicio a nivel mensual



NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Identity Fraud

Capa de monitorización para la **protección de la identidad digital** frente a usos no autorizados dirigidos a fines delictivos o de aprovechamiento ilegítimo con interés comercial.

Actividades globales de Identificación de:

- Dominios fraudulentos y/o sospechosos.
- Dominios en parking y/o a la venta.
- Fraude, suplantación y/o Abuso de marca en Redes sociales
- Aplicaciones móviles en markets de terceros.
- Gestión de Bajas

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

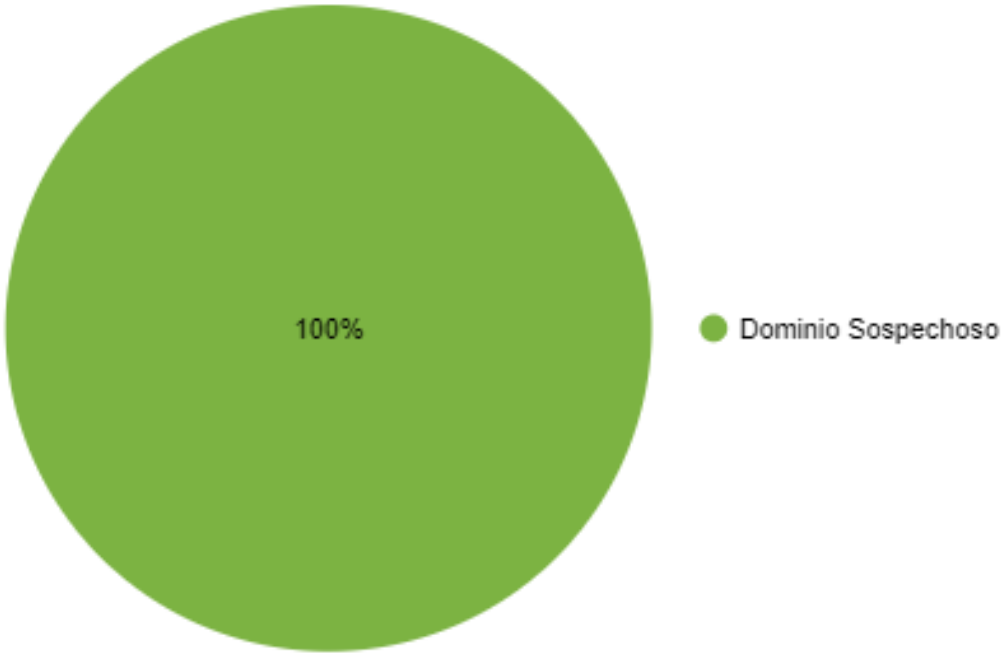
Servicio de Vigilancia

KPIs > **Dominios – Estadística Global**

Nº de alertas enviadas: 1

Volumetría por tipo de dominio

% de afectación por tipo de dominio



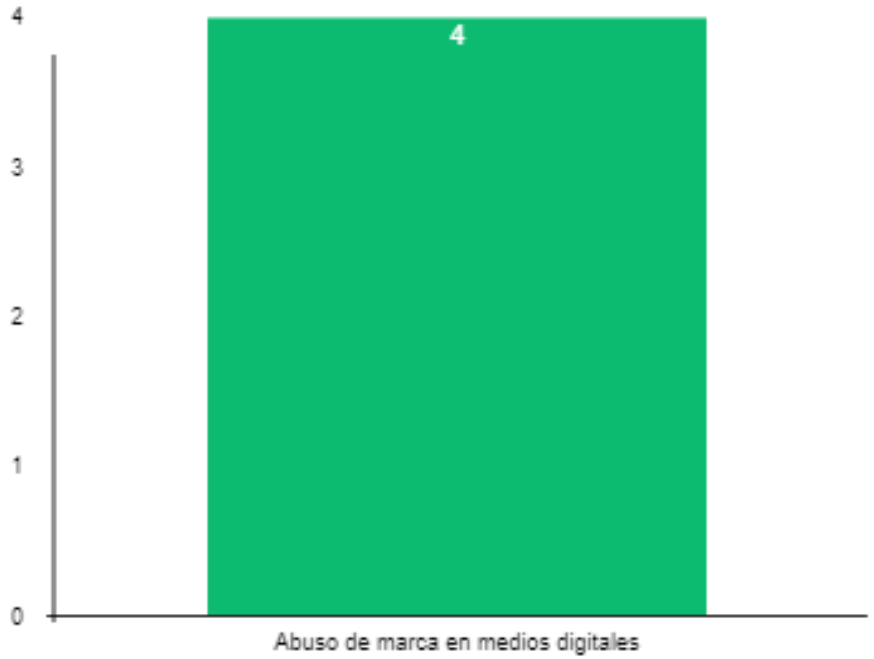
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

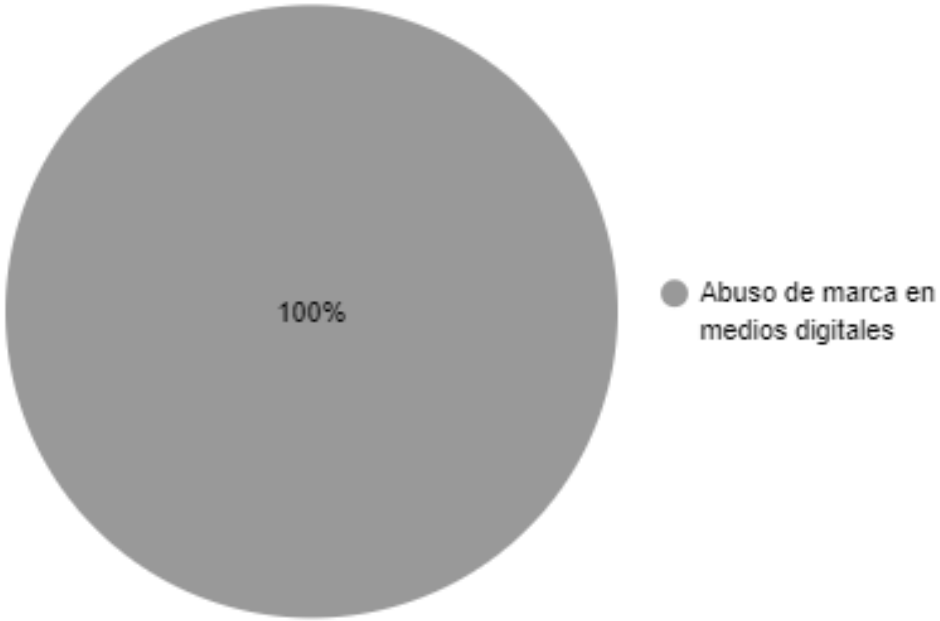
Redes Sociales > **Abuso de marca / Oferta laboral no autorizada**

Nº de alertas enviadas:4

Volumetría por tipo de amenaza



% de afectación por tipo de amenaza

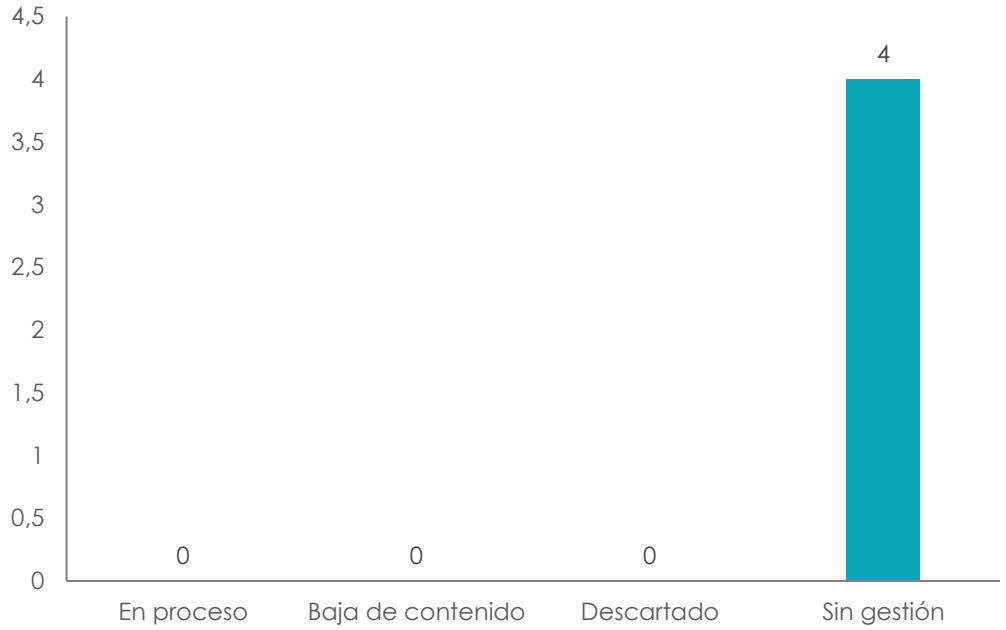


NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

Gestión de baja mensual

A continuación, se presenta el estado actual de las gestiones de baja realizadas para el mes de febrero



En Proceso: Continúan las gestiones para el cierre.

Baja de contenido: Cerrado. Amenaza eliminada

Descartado: No se continúan con las acciones de cierre por circunstancias ajenas al servicio.

Sin gestión: Eventos sin gestionar. Pendientes de la solicitud del cliente.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

No está permitida su reproducción, distribución o comunicación fuera del destinatario.

MNEMO

Data Protection

Capa de monitorización para **protección de la información** corporativa frente a fugas documentales que exponen a la organización a riesgo legal y daños derivados de la reputación; así como los impactos sobre el negocio derivados de la pérdida del secreto.

Actividades globales de Identificación de:

- Credenciales filtradas en la Red.
- Credenciales puestas a la venta en los markets cibercriminales.
- Credenciales recopiladas por los C2.
- Documentación expuesta.
- Gestión de baja.

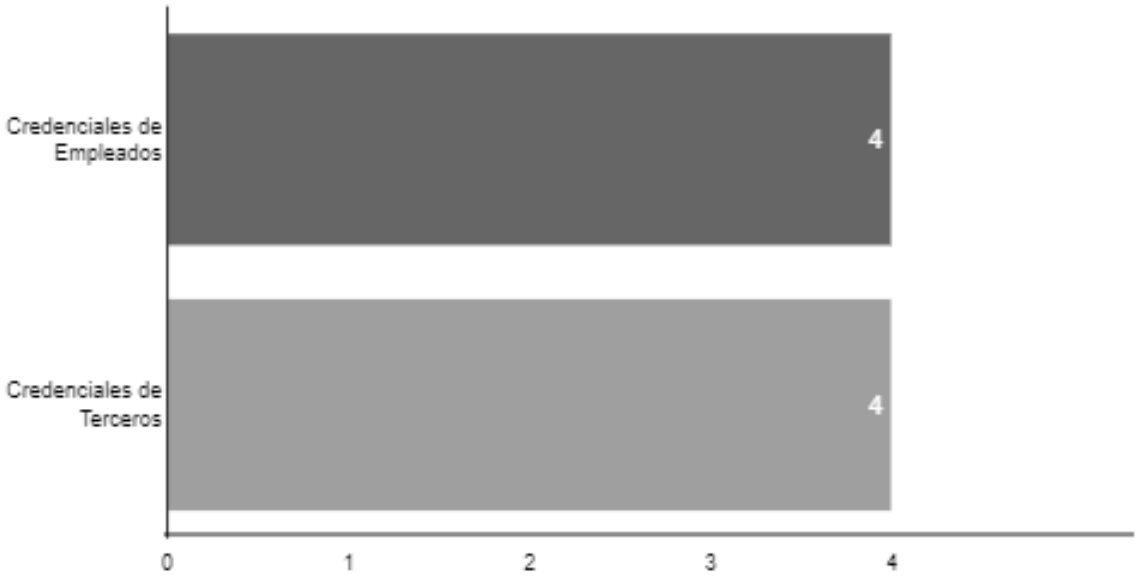
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

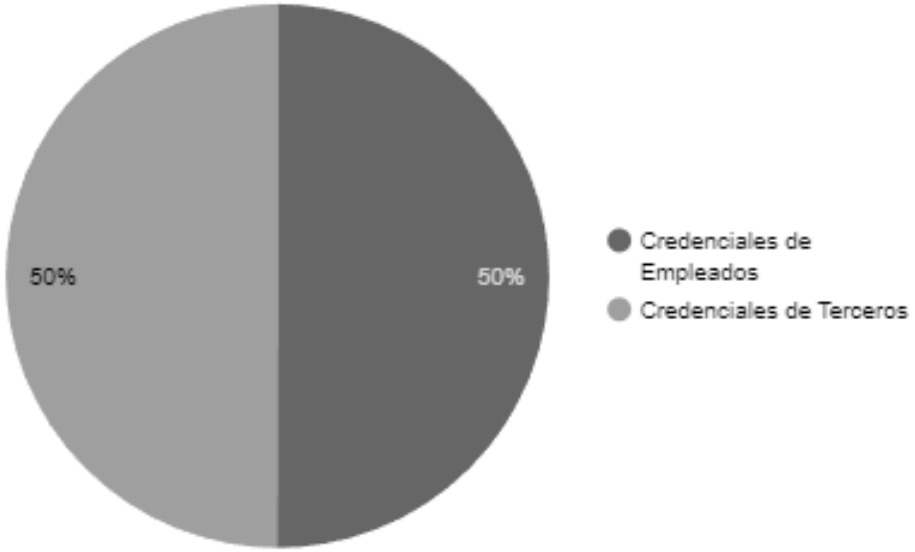
KPIs > Fuga de información

Volumetría por tipo de fuga

Nº Total de Alertas enviadas: 8



% de afectación por tipo de fuga

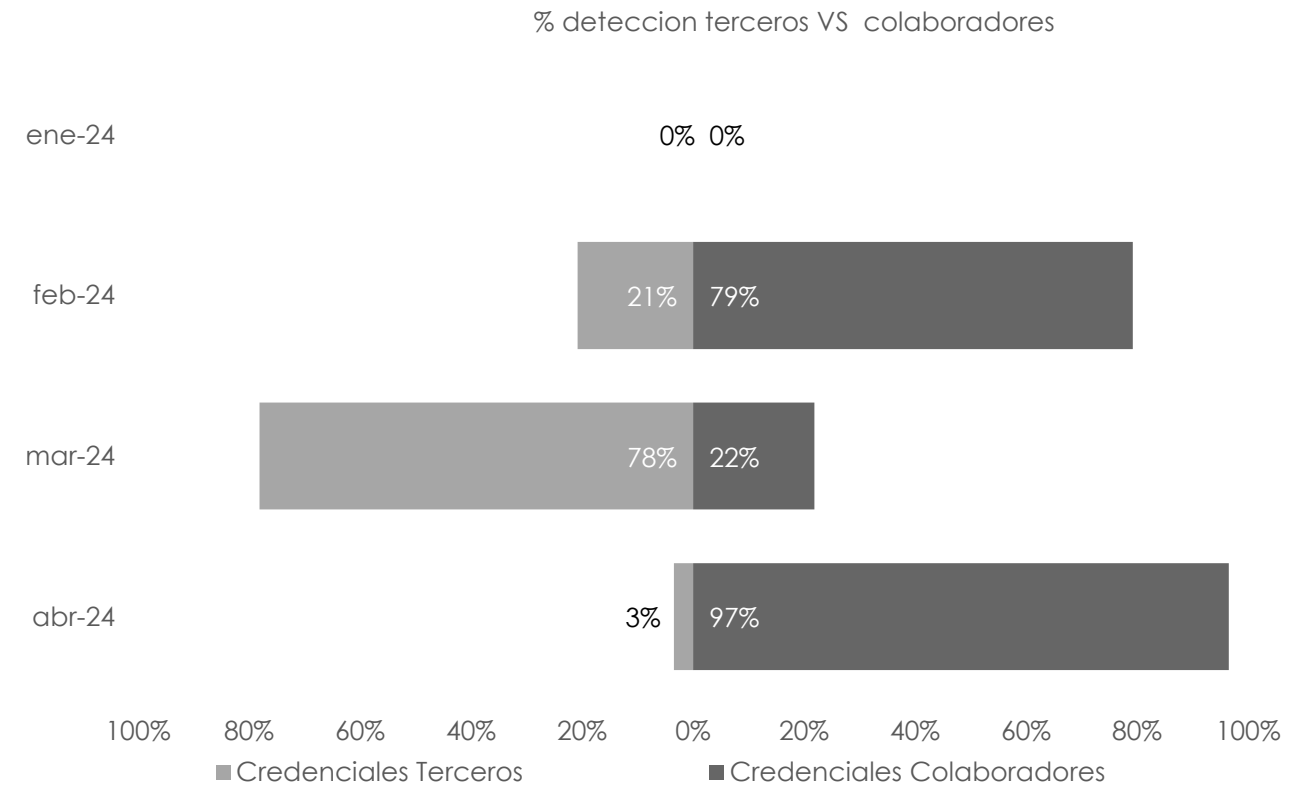


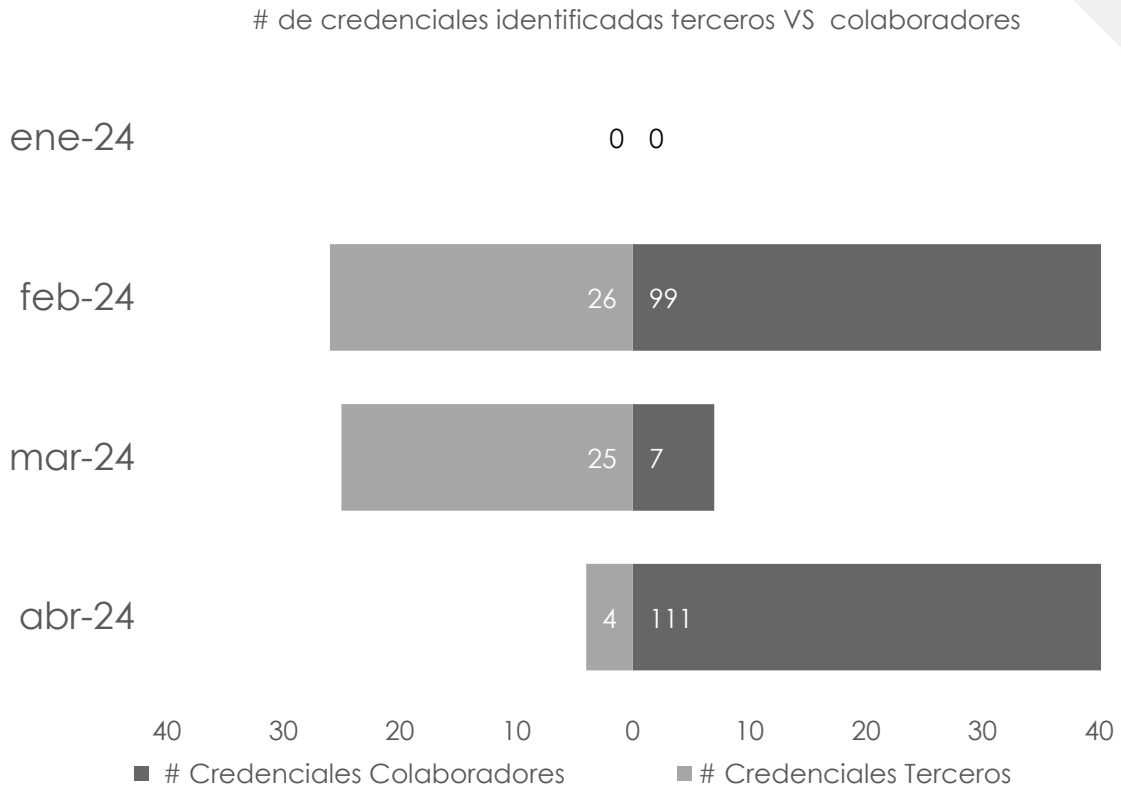
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

Histórico > Evolución del servicio a nivel mensual

Volumetría total de eventos identificados





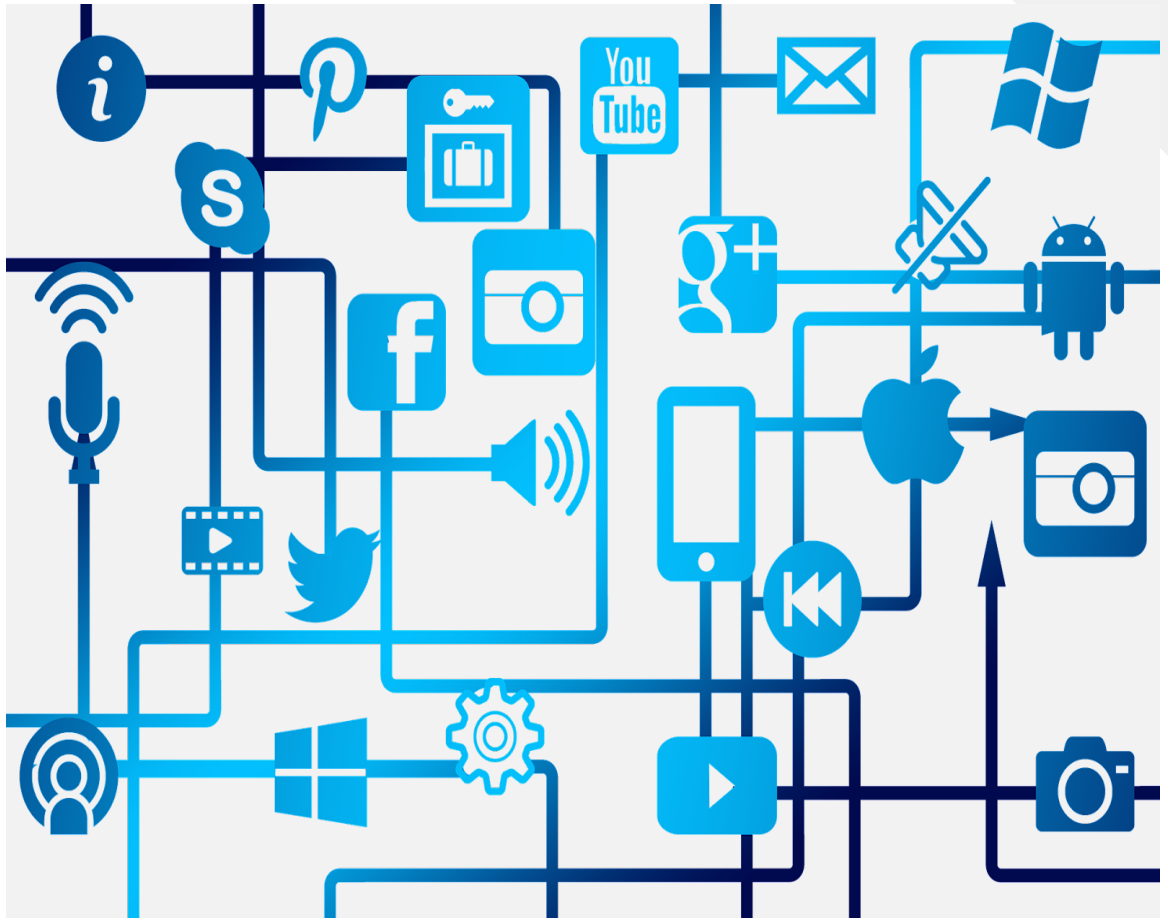
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Brand Protection

Capa de monitorización para la **protección de la marca** frente a intentos de ataque organizado con la intención de dañar la reputación mediante acciones de alto impacto.

Actividades globales de identificación de:

- Hacktivismo y movilizaciones sociales.
- Ataques Organizados.
- Ataques a VIP y/o POI
- Menciones de marca.



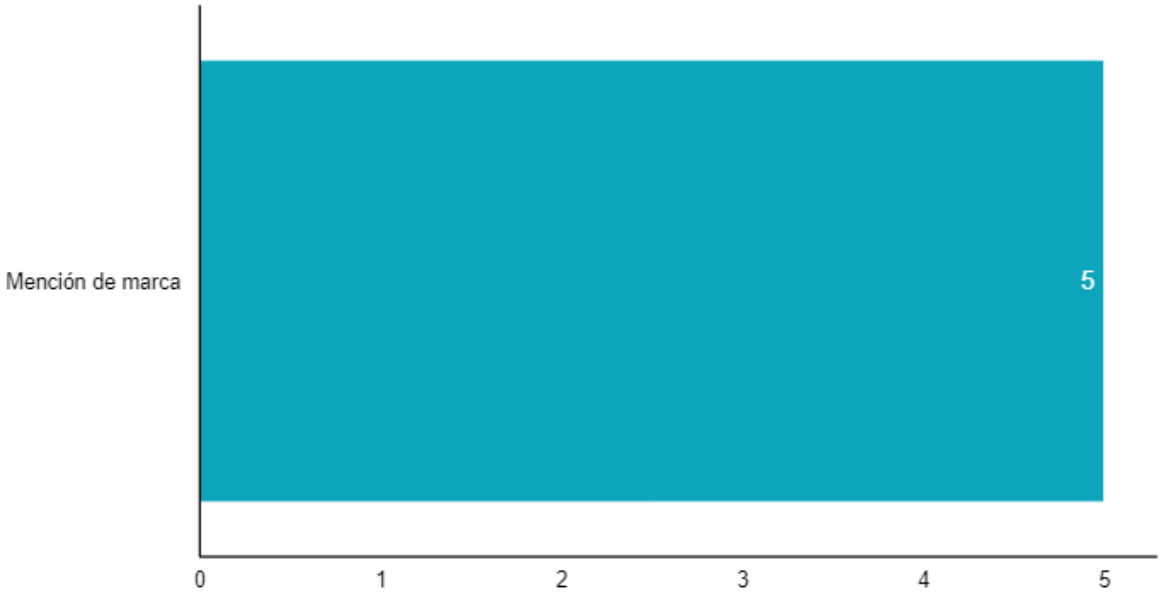
MNEMO

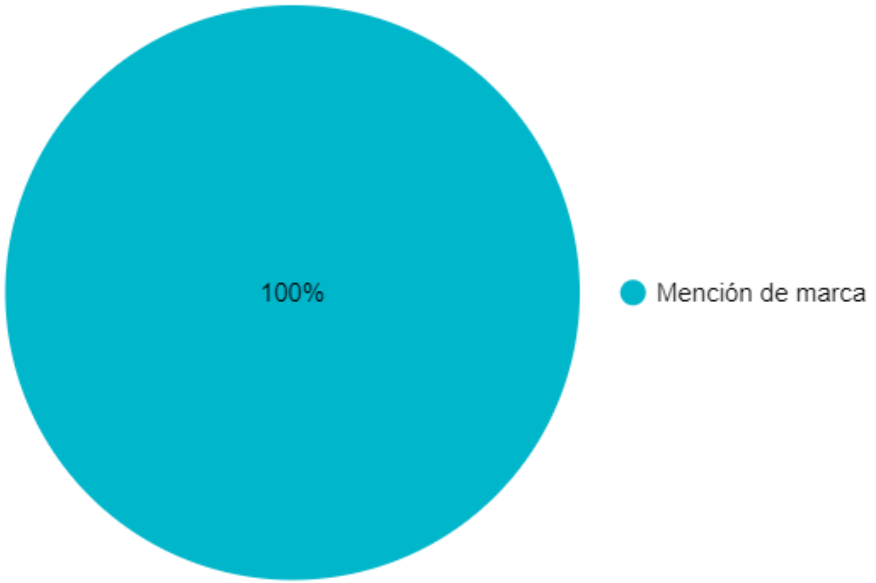
Servicio de Vigilancia

Brand protection > Ataques a la reputación / Menciones informativas

Nº de alertas enviadas: 5

% de afectación por tipo de amenaza





NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL

No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

OBSERVACIONES y RECOMENDACIONES

- **Observación:** Se identificaron **4 eventos** notificados bajo la **tipología Abuso de marca** los cuales hacen **uso del nombre de la entidad.**

  Recomendación: **Validar** a nivel interno si **los eventos reportados** están **relacionados con la entidad** y **retroalimentar al equipo de vigilancia** digital en caso de que sea requerido **gestionar la baja del contenido**, o registrar el evento **como perfil legitimo**.

MNEMO

Servicio de Vigilancia

ANEXOS

- A continuación, se adjuntan el resumen de los tickets sin gestión para el periodo presentado

Fecha de Notificación	Ticket	Asunto de la Alerta	Tipología
07/04/2024	106691	[VIGL] [MEDIA] Medio Digital - Abuso de marca	Abuso de marca
12/04/2024	107428	[VIGL] [MEDIA] Medio Digital - Abuso de marca	Abuso de marca
19/04/2024	109353	[VIGL] [MEDIA] Medio Digital - Abuso de marca	Abuso de marca
23/04/2024	109896	[VIGL] [MEDIA] Medio Digital - Abuso de marca	Abuso de marca

MNEMO

MNEMO

Hacienda

GRACIAS

MNEMO_Colombia

T: (+57) 318 335 44 47
Calle 99 No. 10 – 19 of 502

Todos los derechos reservados.

NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCI

No está permitida su reproducción, distribución o comunicación fuera del d

MNEMO

CERTIFICACIÓN DE CUMPLIMIENTO ARTÍCULO 50 LEY 789 DE 2002 Y LEY 828 DE 2003 - PERSONA JURÍDICA.

HUMBERTO DE JESUS VELEZ CASTRO, identificado con cédula de ciudadanía No.**8.770.446** de Soledad - Atlántico, y con Tarjeta Profesional No. 61.061-T de la JuntaCentral de Contadores de Colombia, en mi condición de Revisor Fiscal de la sociedad extranjera con sucursal en Colombia MNEMO EVOLUTION & INTEGRATION SERVICES SA, identificada con NIT 901.306.687-2, debidamente inscrito en la Cámara de Comercio de Bogotá D.C., luego de examinar de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, los estados financieros de la compañía, certifico que la sucursal en mención **NO CUENTA CON PERSONAL VINCULADO EN COLOMBIA** por lo que no tiene obligaciones pendientes durante los últimos seis (6) meses calendario legalmente exigibles a la fecha de presentación de la propuesta para el presente proceso de selección, por los conceptos de salud, pensiones, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA).

Lo anterior, en cumplimiento de lo dispuesto en el Artículo 50 de la Ley 789 de 2002.
Dada en Bogotá D.C., a los catorce (14) días del mes de Mayo de 2024.

HUMBERTO DE JESUS VELEZ CASTRO
C.C. 8.770.446 de Soledad – Atlántico
T.P. No. 61.061-T de la Junta Central de Contadores de Colombia

CEDULA DE CIUDADANIA
REPÚBLICA DE COLOMBIA
NUIP 8.770.446
VELEZ CASTRO
HUMBERTO DE JESUS
COL
1.70
M
26 JUL 1970
B+
BARRANQUILLA (ATLANTICO)
15 SEPT 1988, SOLEDAD
29 DIC 2030

0000163555
REGISTRADOR NACIONAL
ICCOL0000163550030 52<<<<<<<<<<<
7007282M3012291COL8770446<<<<8
VELEZ<CASTRO<<HUMBERTO<DE<JESU

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

61061-T

HUMBERTO DE JESUS
VELEZ CASTRO
C.C. 8770446
RES. INSCRIPCION 98 DEL 20/06/1998
UNIVERSIDAD AUTONOMA DEL CARIBE

OSCAR EDUARDO FUENTES PEÑA
DIRECTOR GENERAL

251625 69149

UNIDAD ADMINISTRATIVA ESPECIAL | JUNTA CENTRAL DE CONTADORES

Esta tarjeta es el único documento que lo acredita como Contador Público de acuerdo con lo establecido en la Ley 43 de 1990. Es personal e intransferible.

Agradecemos a quien encuentre esta tarjeta comunicarse al PBX: (57)(1) 6444450 o devolverla a la UAE – Junta Central de Contadores a la Calle 96 No. 9 A – 21 Bogotá D.C

FIRMA

EL SUSCRITO REVISOR FISCAL

C E R T I F I C A

Que para efectos de la norma establecida en el artículo 50 de la Ley 789 de 2002, modificado por el artículo 9 de la Ley 828 de 2003, la empresa **MNEMO COLOMBIA S.A.S., con NIT 900.396.176-1**, legalmente constituida, cuyo domicilio principal se encuentra en la CL 99 10 19 OF 502, de la ciudad de Bogotá, D.C., dedicada a la actividad de desarrollo de sistemas informáticos CIIU 6201, durante el período de los **ÚLTIMO SEIS MESES**, comprendido entre el 1 de diciembre de 2023 al 1 de mayo de 2024, presentó el pago de los aportes al sistema de seguridad social y parafiscales y se pudo verificar que la administración ha cumplido con lo establecido en norma.

Que los registros presentados se encuentran debidamente soportados con los documentos internos y externos que respaldan los pagos a la seguridad social y parafiscales.

Esta certificación se expide por el Revisor Fiscal **JOSÉ IGNACIO SALAZAR GÓMEZ**, identificado C.C. 14.239.581 de Ibagué y T.P. 27.398-T, para el único fin consagrado en la norma mencionada anteriormente.

En constancia de lo anterior, firmo en la ciudad de Bogotá, D.C., a los (2) dos días del mes de mayo de 2024.

At.

JOSE IGNACIO SALAZAR GOMEZ
Revisor Fiscal T.P. 27.398-T
C.C. 14.239.581 de Ibagué – Cel. 3158889246 joseignaciosago@hotmail.com

aportes en línea

Planilla Resumen

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si

DATOS GENERALES DE LA LIQUIDACION

Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-03	2024-04	580106838	9465650819	E	2024/04/17	2024/04/16	BANCO BBVA COLOMBIA S.A.	0	$147,390,400

LIQUIDACION DETALLADA DE APORTES

EMPLEADO			NOVEDADES																PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Días	Codigo	Dias	Codigo	Días	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (97 Afiliados)																													

Planilla Resumen

Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (21 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (21 Afiliados)																															
1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN													X					23020 1	15	EPS008	15	CCF24	15	14-25	15	0.000%	15	Si
2	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																	X	23020 1	15	EPS008	15	CCF24	15	14-25	15	1.044%	15	Si
3	CC	93387321	ARANA REYES JAMES GUSTAVO																		25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No
4	CC	67016350	BOCANEGRA VALBUENA ANA MARIA											X							25-14	3	EPS001	3	CCF24	0	14-25	3	0.000%	0	No
5	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																		25-14	27	EPS001	27	CCF24	27	14-25	27	1.044%	27	No
6	CC	1122651302	CARO ROA JONATHAN													X					23030 1	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
7	CC	1122651302	CARO ROA JONATHAN																		23030 1	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	Si
8	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																		23030 1	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
9	CC	1013592039	EMBUS IPIA JULIAN ANDRES																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
10	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
11	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO													X					23100 1	11	EPS005	11	CCF24	11	14-25	11	0.000%	11	Si
12	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO																		23100 1	19	EPS005	19	CCF24	19	14-25	19	1.044%	19	Si
13	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																		23030 1	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
14	CC	79865487	PUENTES CASTRO DAVID EDUARDO																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
15	CC	79717549	RODRIGUEZ JOHN FERNANDO											X							23020 1	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	Si
16	CC	79717549	RODRIGUEZ JOHN FERNANDO																		23020 1	28	EPS005	28	CCF24	28	14-25	28	1.044%	28	Si
17	CC	52824814	RODRIGUEZ MURCIA NIDIA ESPERANZA																		23030 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
18	CC	80791790	ROJAS ARIAS RICARDO											X							23020 1	10	EPS005	10	CCF24	0	14-25	10	0.000%	0	No
19	CC	80791790	ROJAS ARIAS RICARDO																		23020 1	20	EPS005	20	CCF24	20	14-25	20	1.044%	20	No
20	CC	80066361	ROMERO ARCHILA DANIEL DARIO																		23020 1	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
21	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI													X					23100 1	13	EPS005	13	CCF24	13	14-25	13	0.000%	13	No
22	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																	X	23100 1	17	EPS005	17	CCF24	17	14-25	17	1.044%	17	No
23	CC	24659147	VALDES RAMIREZ ALBA LIBIA																			0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
24	CC	79950164	VARGAS HINCAPIE FERNANDO								X										23030 1	30	EPS002	30	CCF24	30	14-25	30	1.044%	30	Si
25	CC	1032410736	VARGAS HINCAPIE HENRY																		23090 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
26	CC	1000349377	VARGAS ALVAREZ MARIA ANTONIA											X							23030 1	2	EPS037	2	CCF24	0	14-25	2	0.000%	0	Si
27	CC	1000349377	VARGAS ALVAREZ MARIA ANTONIA																		23030 1	28	EPS037	28	CCF24	28	14-25	28	1.044%	28	Si
28	CC	1022411758	VARGAS LEON MARIA CAMILA																		23030 1	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
29	CC	1025525887	ZABALA MAHECHA DANIEL STEVEN																			0	EPS017	30		0		0	0.000%	0	No
Centro de Trabajo: ADMINISTRACION (72 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (72 Afiliados)																															
30	CC	1014306151	ABRIL MONTES SERGIO LEONARDO								X										23020 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	1019151775	ACOSTA MURILLO JUAN CAMILO								X										25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
32	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO													X					25-14	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si

PLANILLA PAGADA

33	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO															25-14	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
34	CC	1031162097	ARISTIZABAL ANGEL LAURA VANESSA								X							230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
35	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER															231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
36	CC	1019077197	BELEÑO BUELVAS CHARLES JAVIER								X							230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
37	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER															230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
38	CC	1012437249	BOCANEGRA MORALES LUIS FELIPE									X						230301	4	EPS008	4	CCF24	0	14-25	4	0.000%	0	Si
39	CC	1012437249	BOCANEGRA MORALES LUIS FELIPE								X							230301	26	EPS008	26	CCF24	26	14-25	26	0.522%	26	Si
40	CC	1004268659	BONILLA ZUÑIGA ANDERSON															231001	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
41	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN															230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
42	CC	1024467791	CARDENAS VARON KEVIN ANDRES																0	EPS010	30		0	14-25	30	0.522%	0	No
43	CC	13870244	CARRILLO ALVAREZ OSCAR															25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
44	CC	1012322665	CASTAÑEDA MESA ANDREA KATHERINE												X			231001	11	EPS008	11	CCF24	11	14-25	11	0.000%	11	Si
45	CC	1012322665	CASTAÑEDA MESA ANDREA KATHERINE															231001	19	EPS008	19	CCF24	19	14-25	19	0.522%	19	Si
46	CC	1034397473	CASTILLO IDROBO JHON FABER																0	EPS002	30		0	14-25	30	0.522%	0	No
47	CC	1020809969	CASTILLO MENDOZA JOHN ALEXANDER								X							230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
48	CC	1070590173	CASTRO CALDERON JUAN GUILLERMO																0	EPS005	30		0	14-25	30	0.522%	0	No
49	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID								X							230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
50	CC	1022418490	DIAZ MONCALEANO JOSE MANUEL								X							230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
51	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER												X			25-14	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
52	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER															25-14	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
53	CC	1023957895	GIL MURILLO JAVIER EDUARDO								X							230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
54	CC	1019009180	GOMEZ ROJAS YENNY PAOLA										X					230301	1	EPS037	1	CCF24	0	14-25	1	0.000%	0	Si
55	CC	1019009180	GOMEZ ROJAS YENNY PAOLA										X		X			230301	3	EPS037	3	CCF24	1	14-25	3	0.000%	1	Si
56	CC	1019009180	GOMEZ ROJAS YENNY PAOLA															230301	26	EPS037	26	CCF24	26	14-25	26	0.522%	26	Si
57	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO												X			230201	13	EPS005	13	CCF24	13	14-25	13	0.000%	13	Si
58	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO															230201	17	EPS005	17	CCF24	17	14-25	17	0.522%	17	Si
59	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN										X						0	EPS005	1		0	14-25	1	0.000%	0	No
60	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN																0	EPS005	29		0	14-25	29	0.522%	0	No
61	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL								X							230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
62	CC	1000689679	GUARIN PINZON MATEO								X							230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	1076663845	GUAYAZAN CORTES JONATHAN STIVEN								X							230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
64	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES												X			230201	2	EPS005	2	CCF24	2	14-25	2	0.000%	2	Si
65	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES															230201	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si

66	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																	230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
67	CC	1099374748	LEAL GOMEZ DANIELA												X					230201	1	EPS037	1	CCF24	1	14-25	1	0.000%	1	Si
68	CC	1099374748	LEAL GOMEZ DANIELA																	230201	29	EPS037	29	CCF24	29	14-25	29	0.522%	29	Si
69	CC	52953219	LEON CERON MARIA ALEXANDRA										X							231001	3	EPS005	3	CCF24	0	14-25	3	0.000%	0	Si
70	CC	52953219	LEON CERON MARIA ALEXANDRA																	231001	27	EPS005	27	CCF24	27	14-25	27	0.522%	27	Si
71	CC	1069769484	LOPEZ ZAMORA JUAN DAVID	X																230301	20	EPS002	20	CCF24	20	14-25	20	0.522%	20	Si
72	CC	79992827	MARROQUIN GUTIERREZ DIDIER																	230201	30	MIN002	30	CCF24	30	14-25	30	0.522%	30	Si
73	CC	1000032122	MARTIN GARCES JUAN DAVID																	230301	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
74	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																	230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
75	CC	1000719172	MARTINEZ BECERRA MARIA JOSE								X									230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
76	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
77	CC	1000717997	MELO MOSQUERA DANIEL RENE								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
78	CC	98632570	MESA MENDEZ CARLOS MANUEL												X					230201	2	MIN001	2	CCF24	2	14-25	2	0.000%	2	Si
79	CC	98632570	MESA MENDEZ CARLOS MANUEL																	230201	28	MIN001	28	CCF24	28	14-25	28	0.522%	28	Si
80	CC	1022947945	MOLANO JIMENEZ JESUS RICARDO								X									230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
81	CC	1110173553	MORA TABARES MIGUEL ANGEL								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
82	CC	1033711407	MURCIA TORRES JHON FREDY																	230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
83	CC	1023907046	OCHOA ROJAS ROGER JULIAN								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
84	CC	1032479763	ORJUELA CALDERON PAULA NATALIA										X							231001	2	EPS005	2	CCF24	0	14-25	2	0.000%	0	Si
85	CC	1032479763	ORJUELA CALDERON PAULA NATALIA								X									231001	28	EPS005	28	CCF24	28	14-25	28	0.522%	28	Si
86	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
87	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN																	230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
88	CC	1023886752	PATARROYO JIMENEZ JHON JAIRO								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
89	CC	1019127504	PERDOMO GUZMAN JESSICA LILIANA								X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
90	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO																	230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
91	CC	1030618626	PINZON ROJAS ANDRES CAMILO												X					230201	3	EPS005	3	CCF24	3	14-25	3	0.000%	3	Si
92	CC	1030618626	PINZON ROJAS ANDRES CAMILO																	230201	27	EPS005	27	CCF24	27	14-25	27	0.522%	27	Si
93	CC	1023972445	PRIETO SILVA NICOL																	230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
94	CC	1014201989	QUIROGA PERALTA EDWIN FERNANDO																	230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
95	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN								X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
96	CC	1032486411	RINCON HILARION EDWARD MAURICIO								X									231001	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
97	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES								X									25-14	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
98	CC	1003712217	RODRIGUEZ PENAGOS JOAN SEBASTIAN	X																230301	20	EPS008	20	CCF24	20	14-25	20	0.522%	20	Si
99	CC	52505417	ROJAS PEÑA NILSA YAMILE																	25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
100	CC	1030697447	ROJAS PEREZ VALENTINA								X									230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si

101	CC	1030666489	SALAZAR ARCILA JOHN SEBASTIAN		X							X								X	230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
102	CC	1010180437	SANCHEZ ROMERO CARLOS ANDRES									X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
103	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO													X					230201	13	EPS008	13	CCF24	13	14-25	13	0.000%	13	Si
104	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO																	X	230201	17	EPS008	17	CCF24	17	14-25	17	0.522%	17	Si
105	CC	1030539604	TAMAYO RIVERA FABIO ANDRES											X							231001	30	EPS005	30	CCF24	0	14-25	30	0.000%	0	Si
106	CC	1020808701	TIBADUIZA CALDERON SEBASTIAN																		231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
107	CC	1032394709	TOLEDO SALAMANCA WALTER OSWALDO																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
108	CC	1018408876	TOVAR LOZANO JAIRO DAVID																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
109	CC	1031172873	TRUJILLO ALVAREZ VALENTINA											X							231001	2	EPS008	2	CCF24	0	14-25	2	0.000%	0	Si
110	CC	1031172873	TRUJILLO ALVAREZ VALENTINA																		231001	28	EPS008	28	CCF24	28	14-25	28	0.522%	28	Si
111	CC	1014279176	URBANO ARDILA SEBASTIAN									X									25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
112	CC	1019136138	VANEGAS CAMARGO DIEGO ALEJANDRO									X									230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
113	CC	80247522	VARGAS HINCAPIE CARLOS																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
114	CC	1075280531	VARGAS POLANIA JAIRO ALEXANDER													X					230201	3	EPS005	3	CCF24	3	14-25	3	0.000%	3	Si
115	CC	1075280531	VARGAS POLANIA JAIRO ALEXANDER																		230201	27	EPS005	27	CCF24	27	14-25	27	0.522%	27	Si
116	CC	1014197302	VELASQUEZ RAMOS JOHAN SEBASTIAN																		25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
117	CC	8770446	VELEZ CASTRO HUMBERTO DE JESUS																		230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	No
118	CE	667352	VICENT FERNANDEZ CARLOS																			0	EPS005	30	CCF24	30	14-25	30	0.522%	30	No
Centro de Trabajo: CENTRO TRABAJO 2 (1 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																															
119	CC	1019024746	MUÑOZ OROZCO BERTHA JUDITH																		25-14	30	EPS017	30	CCF24	30	14-25	30	1.044%	30	Si
Centro de Trabajo: MENSAJERIA (3 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (3 Afiliados)																															
120	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS													X					230201	5	EPS008	5	CCF24	5	14-25	5	0.000%	5	Si
121	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS																		230201	25	EPS008	25	CCF24	25	14-25	25	4.350%	25	Si
122	CC	79840394	RODRIGUEZ ANGARITA ELKIN																		230301	30	EPS008	30	CCF24	30	14-25	30	4.350%	30	Si
123	CC	91462884	SERRANO BONILLA JILMER																		230301	30	MIN001	30	CCF24	30	14-25	30	4.350%	30	Si

LIQUIDACION DETALLADA DE APORTES

EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: FAMISANAR (1 Afiliados)																														
Centro de Trabajo: FAMISANAR - ADMINISTRATIVO (1 Afiliados)																														
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																														
124	CC 80155666	CHAVES MARTINEZ JORGE ANDRES									X									230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si

LIQUIDACION DETALLADA DE APORTES

EMPLEADO			NOVEDADES																	PENSION		SALUD		CCF		RIESGOS			PARAFISCALES	
No.	Identificación	Nombre	ing	ret	tde	tae	tdp	tap	vsp	cor	vst	sln	ige	lma	vac	avp	vct	irl	vip	Codigo	Dias	Codigo	Dias	Codigo	Dias	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF

PLANILLA PAGADA

Planilla Resumen

SUCURSAL: OTROS (1 Afiliados)														
Centro de Trabajo: OTROSCAL (1 Afiliados)														
Ciudad: CALI Depto: VALLE (1 Afiliados)														
125	CC	14701875	CASTRO LOPEZ JULIAN ANDRES	X	230201	6	EPS010	6	CCF56	6	14-25	6	0.522%	6	Si
Total	Afiliados(99)													

DATOS GENERALES DEL APORTANTE

Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono	Exonerado SENA e ICBF
NIT 900396176	1	MNEMO COLOMBIA SAS	B - MENOS DE 200 COTIZANTES	PRINCIPAL	CLL 99 10 19 OF 502	BOGOTA-BOGOTA D.E.	5527210	Si

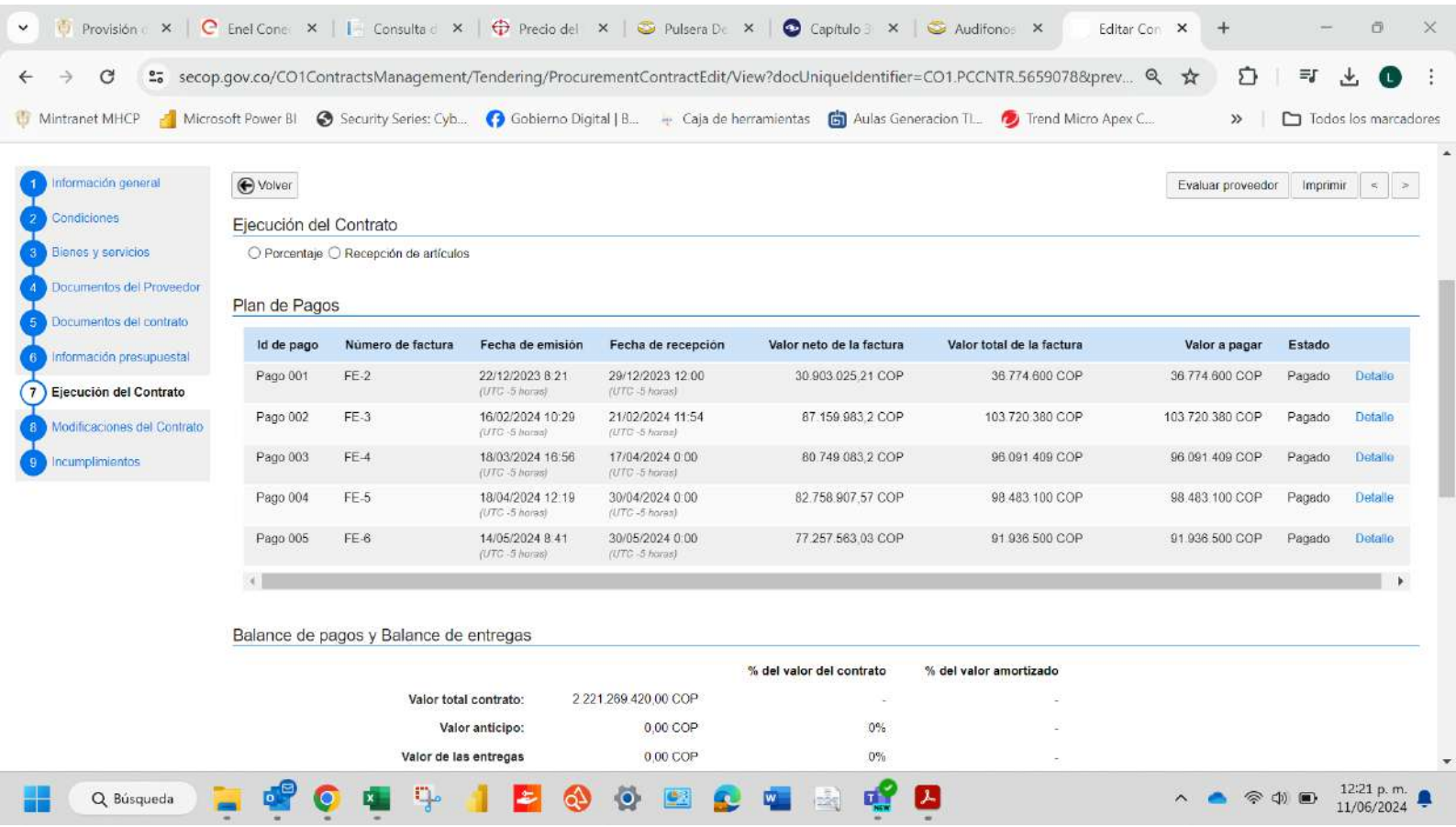
DATOS GENERALES DE LA LIQUIDACION

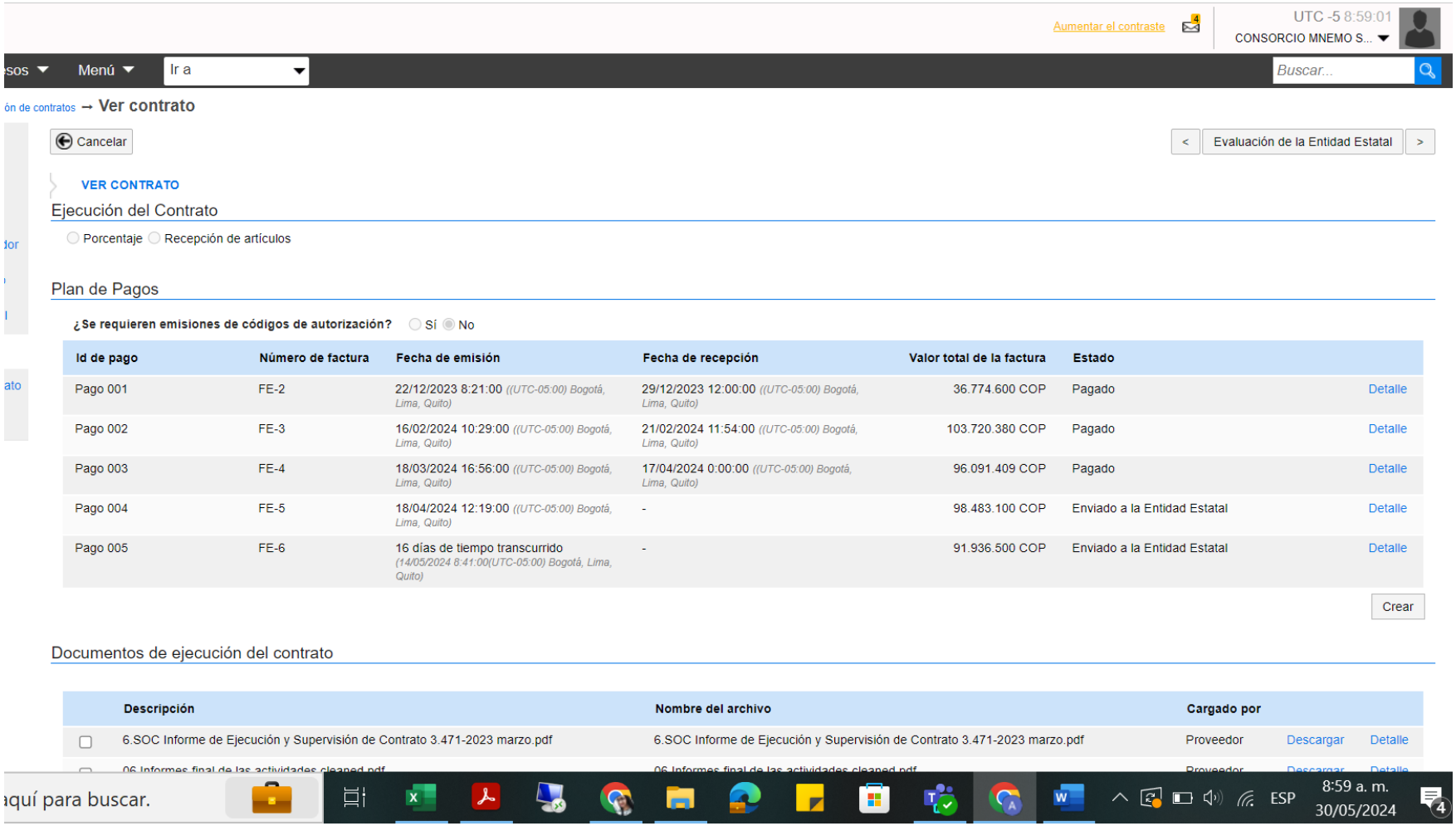
Periodo		Clave		Tipo	Fecha		Pago		
Pensión	Salud	Pago	Planilla	Planilla	Limite	Pago	Banco	Dias Mora	Valor
2024-03	2024-04	580106838	9465650819	E	2024/04/17	2024/04/16	BANCO BBVA COLOMBIA S.A.	0	$147,390,400

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				92	$80,342,000	$0	$0	$80,342,000
COLFONDOS	231001	800,227,940	6	11	$12,650,200	$0	$0	$12,650,200
COLPENSIONES	25-14	900,336,004	7	13	$13,518,900	$0	$0	$13,518,900
PORVENIR	230301	800,224,808	8	37	$24,354,800	$0	$0	$24,354,800
PROTECCION	230201	800,229,739	0	30	$27,676,100	$0	$0	$27,676,100
SKANDIA	230901	800,253,055	2	1	$2,142,000	$0	$0	$2,142,000
ARL (ADMINISTRADORAS: 1)				98	$3,880,700	$0	$0	$3,880,700
COLMENA	14-25	800,226,175	3	98	$3,880,700	$0	$0	$3,880,700
CCF (ADMINISTRADORAS: 2)				94	$20,917,700	$0	$0	$20,917,700
COMFENALCO VALLE	CCF56	890,303,093	5	1	$13,600	$0	$0	$13,600
COMPENSAR	CCF24	860,066,942	7	93	$20,904,100	$0	$0	$20,904,100
EPS (ADMINISTRADORAS: 10)				99	$34,823,200	$0	$0	$34,823,200
ALIANSALUD EPS (ANTES COLMEDICA)	EPS001	830,113,831	0	2	$1,795,000	$0	$0	$1,795,000
CAPITAL SALUD	EPSC34	900,298,372	9	1	$104,200	$0	$0	$104,200
COMPENSAR	EPS008	860,066,942	7	19	$5,059,900	$0	$0	$5,059,900
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	6	$760,600	$0	$0	$760,600
FAMISANAR	EPS017	830,003,564	7	13	$2,028,200	$0	$0	$2,028,200
FOSYGA	MIN001	901,037,916	1	7	$3,280,600	$0	$0	$3,280,600
FOSYGA RÉGIMEN DE EXCEPCIÓN	MIN002	901,037,916	1	1	$154,000	$0	$0	$154,000
NUEVA E.P.S.	EPS037	900,156,264	2	6	$879,300	$0	$0	$879,300
SALUD TOTAL	EPS002	800,130,907	4	9	$1,209,000	$0	$0	$1,209,000
SANITAS	EPS005	800,251,440	6	35	$19,552,400	$0	$0	$19,552,400
ICBF (ADMINISTRADORAS: 1)				10	$4,456,100	$0	$0	$4,456,100
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	10	$4,456,100	$0	$0	$4,456,100
SENA (ADMINISTRADORAS: 1)				10	$2,970,700	$0	$0	$2,970,700
SENA	PASENA	899,999,034	1	10	$2,970,700	$0	$0	$2,970,700
TOTAL				99	$147,390,400	$0	$0	$147,390,400

PLANILLA PAGADA


Provisión
Enel Cone
Consulta
Precio del
Pulsera De
Capítulo 3
Audífonos
Editar Con
secop.gov.co/CO1ContractsManagement/Tendering/ProcurementContractEdit/View?docUniqueIdentifier=CO1.PCCNTR.5659078&prev...
Mintranet MHCP
Microsoft Power BI
Security Series: Cyb...
Gobierno Digital | B...
Caja de herramientas
Aulas Generacion TI...
Trend Micro Apex C...
Todos los marcadores
1 Información general
2 Condiciones
3 Bienes y servicios
4 Documentos del Proveedor
5 Documentos del contrato
6 Información presupuestal
7 Ejecución del Contrato
8 Modificaciones del Contrato
9 Incumplimientos
Volver
Evaluar proveedor
Imprimir
Ejecución del Contrato
Porcentaje
Recepción de artículos
Plan de Pagos
Id de pago
Número de factura
Fecha de emisión
Fecha de recepción
Valor neto de la factura
Valor total de la factura
Valor a pagar
Estado
Pago 001 FE-2 22/12/2023 8:21 (UTC -5 horas) 29/12/2023 12:00 (UTC -5 horas) 30.903.025,21 COP 36.774.600 COP 36.774.600 COP Pagado Detalle
Pago 002 FE-3 16/02/2024 10:29 (UTC -5 horas) 21/02/2024 11:54 (UTC -5 horas) 87.159.983,2 COP 103.720.380 COP 103.720.380 COP Pagado Detalle
Pago 003 FE-4 18/03/2024 16:56 (UTC -5 horas) 17/04/2024 0:00 (UTC -5 horas) 80.749.083,2 COP 96.091.409 COP 96.091.409 COP Pagado Detalle
Pago 004 FE-5 18/04/2024 12:19 (UTC -5 horas) 30/04/2024 0:00 (UTC -5 horas) 82.758.907,57 COP 98.483.100 COP 98.483.100 COP Pagado Detalle
Pago 005 FE-6 14/05/2024 8:41 (UTC -5 horas) 30/05/2024 0:00 (UTC -5 horas) 77.257.563,03 COP 91.936.500 COP 91.936.500 COP Pagado Detalle
Balance de pagos y Balance de entregas
% del valor del contrato
% del valor amortizado
Valor total contrato: 2.221.269.420,00 COP - -
Valor anticipo: 0,00 COP 0% -
Valor de las entregas 0,00 COP 0% -
Búsqueda
12:21 p. m.
11/06/2024


Aumentar el contraste
UTC -5 8:59:01
CONSORCIO MNEMO S...
sos
Menú
Ir a
Buscar...
ón de contratos → Ver contrato
Cancelar
< Evaluación de la Entidad Estatal >
VER CONTRATO
Ejecución del Contrato
Porcentaje Recepción de artículos
Plan de Pagos
¿Se requieren emisiones de códigos de autorización? Sí No
Id de pago | Número de factura | Fecha de emisión | Fecha de recepción | Valor total de la factura | Estado
Pago 001 | FE-2 | 22/12/2023 8:21:00 ((UTC-05:00) Bogotá, Lima, Quito) | 29/12/2023 12:00:00 ((UTC-05:00) Bogotá, Lima, Quito) | 36.774.600 COP | Pagado | Detalle
Pago 002 | FE-3 | 16/02/2024 10:29:00 ((UTC-05:00) Bogotá, Lima, Quito) | 21/02/2024 11:54:00 ((UTC-05:00) Bogotá, Lima, Quito) | 103.720.380 COP | Pagado | Detalle
Pago 003 | FE-4 | 18/03/2024 16:56:00 ((UTC-05:00) Bogotá, Lima, Quito) | 17/04/2024 0:00:00 ((UTC-05:00) Bogotá, Lima, Quito) | 96.091.409 COP | Pagado | Detalle
Pago 004 | FE-5 | 18/04/2024 12:19:00 ((UTC-05:00) Bogotá, Lima, Quito) | - | 98.483.100 COP | Enviado a la Entidad Estatal | Detalle
Pago 005 | FE-6 | 16 días de tiempo transcurrido (14/05/2024 8:41:00(UTC-05:00) Bogotá, Lima, Quito) | - | 91.936.500 COP | Enviado a la Entidad Estatal | Detalle
Crear
Documentos de ejecución del contrato
Descripción | Nombre del archivo | Cargado por
6.SOC Informe de Ejecución y Supervisión de Contrato 3.471-2023 marzo.pdf | 6.SOC Informe de Ejecución y Supervisión de Contrato 3.471-2023 marzo.pdf | Proveedor | Descargar | Detalle
aquí para buscar.
ESP
8:59 a. m.
30/05/2024