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

Número de Radicado	Fecha de Radicado	Fecha de Presentación
1-2024-014781	21/02/2024 11:37	21/02/2024 11:37

Información del contratista del MHCP

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

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

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

º Concepto de cobro : **Monitoreo,diagnóstico,generacion de alertas y recomendaciones,servicios de gestión y análisis de vul**

º Periodo del Servicio:Año **2024** º Mes : **01**

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-MHCO - Nro. contrato: 3.471-2023 - Concepto cobro: Monitoreo,diagnóstico,generacion 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 1.Evidencia de solicitud de pago en el Secop II.pdf

Identificador: 3WR2G0XRvsKv6r1bs9qlODD+LKo=

º 02. Cumplido para pago (Archivo en PDF): Documento adjuntado 2..CUMPLIDO N. 2 CONSORCIO MNEMO SOC-MHCP.pdf

Identificador: FE6RFfmWR88WDfGumHR5Fc5u5RI=

º 03. Informe de Ejecución o acta de entrega (Archivo en PDF): Documento adjuntado 3.Informes de actividades.pdf

Identificador: ufMU0QfGOUQNJtUSInm1+/N8yPE=

º 04. Representación gráfica de la factura (Archivo en PDF): Documento adjuntado 4.FACTURA N. No. FE 3.pdf

Identificador: 4JhrUq15GZHgkntdkeRZQv+gQvo=

º 05.Certificado pago de seguridad social (Archivo en PDF): Documento adjuntado 5.Certificado de seguridad social y parafiscales.pdf

Identificador: QKhqpHQr7SGKyiKYGP17eIzElhg=

Documentos requeridos opcionales adjuntados

º 06. Informe final de actividades (Archivo en PDF): Documento adjuntado 6.SOC Informe de Ejecución y Supervisión de Contrato 3.471-2023 enero 2024_firmado(1).pdf

Identificador: X7ZZYtJLljlsTdcobY3gVYdGmrA=

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 **2**

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 2,313,205,920.00

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: 36,774,600.00 **VALOR PENDIENTE POR EJECUTAR:** 2,276,431,320.00 **% EJECUCIÒN:** 2

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.	FE3	CONDICION DE PAGO	MONITOREO,DIAGNÓSTICO,GENERACIÓN DE ALERTAS Y RECOMENDACIONES MES DE ENERO 2024	74,749,495.80	19 %	14,202,404.20		88,951,900.00
FACTURA NO.	FE3	CONDICION DE PAGO	SERVICIO DE GESTIÓN Y ANÁLISIS DE VULNERABILIDADES ENERO 2024	2,508,067.23	19 %	476,532.77		2,984,600.00
FACTURA NO.	FE3	CONDICION DE PAGO	ANÁLISIS FORENSE (436.440 HORAS) ENERO 2024	9,902,420.17	19 %	1,881,459.83		11,783,880.00
			TOTALES	87,159,983.20		16,560,396.80		

TOTAL A PAGAR 103,720,380.00

Anexos y No. de Folios

Factura	1	Cuenta de Cobro		Declaracion juramentada Seguridad Social	
Otros Anexos o Folios	4	Entrada a Almacen		Constancias de pago de la seguridad social	2
				Total de Folios Anexos	7

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

Firmado digitalmente por Luis Orlando Arenas Ruiz

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

CONTENIDO DEL INFORME

1. CONDICIONES DEL CONTRATO

Número de Contrato: **3.471-2023**
Nombre del Contratista: **CONSORCIO MNEMO SOC-MHCP.**
Periodo informe: **Del 01 al 31 de enero del 2024**
Supervisor: **Luis Orlando Arenas Ruiz**
Área perteneciente: **Dirección del 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

   • Entrega de la documentación de los procesos solicitados del servicio de vigilancia digital.
   • Monitoreo y generación Alertamiento para los servicios de vigilancia digital y Cyber Threat intelligence
   • Entrega de la documentación de la gestión del proyecto (matriz de comunicaciones, matriz de riesgos, plan de trabajo del proyecto y cronograma)
   • Entrega de la documentación técnica (plan de trabajo de implementación y arquitectura.
   • Instalación de appliance en datacenter de MHCP y configuración de puertos e ip de gestión.
   • Configuración inicial de VPN´s solicitadas para los servicios.
   • Capacitaciones para el servicio de vigilancia digital y creación de perfiles de usuario para hacer uso de la plataforma cyberdefense.
   • Ejecución de un análisis Forense y envió del entregable de resultados respectivo.
   • Envió de informes mensuales de la operación de los servicios de vigilancia digita y cyber Threat Intelligence.

Avance: Las actividades anteriormente descritas se desarrollaron satisfactoriamente quedando pendiente otras actividades

Productos del contrato

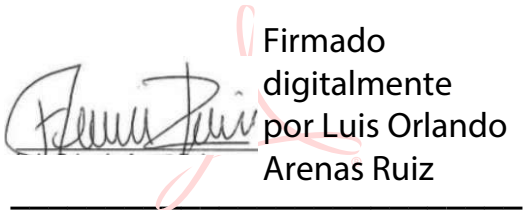
- Sesiones de seguimiento de proyecto
- Envió de documentación contractual
- Mesas de trabajo técnicas

Avance: la realización de las anteriores actividades descritas fue desarrolladas satisfactoriamente

FIRMA CONTRATISTA
Humberto de Jesús Vélez Castro

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.



FIRMA SUPERVISOR

MNEMO

INFORME
Cyber Security Warning - Preventive

ENERO 2024

ELABORADO POR:
EQUIPO CYBER THREAT INTELLIGENCE <CTI>

MNEMO

CYBER THREAT INTELLIGENCE

MNEMO

Enero 2024

INDICADORES GENERALES

Número de alertas

49

Alertas y eventos MISP reportados

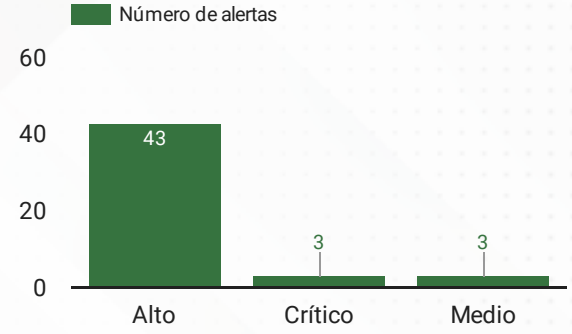
Cantidad

10.957

IoC Reportados

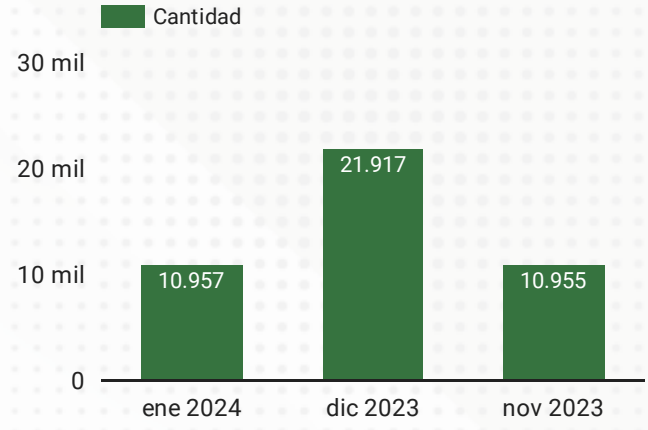
En el presente gráfico, podemos apreciar los datos generales recopilados a lo largo del mes de Enero. En la parte superior izquierda encontramos el gráfico que relaciona el número total de alertas que se podrían verificar en el entorno MISP, mientras que en el gráfico superior derecho veremos el número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

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.



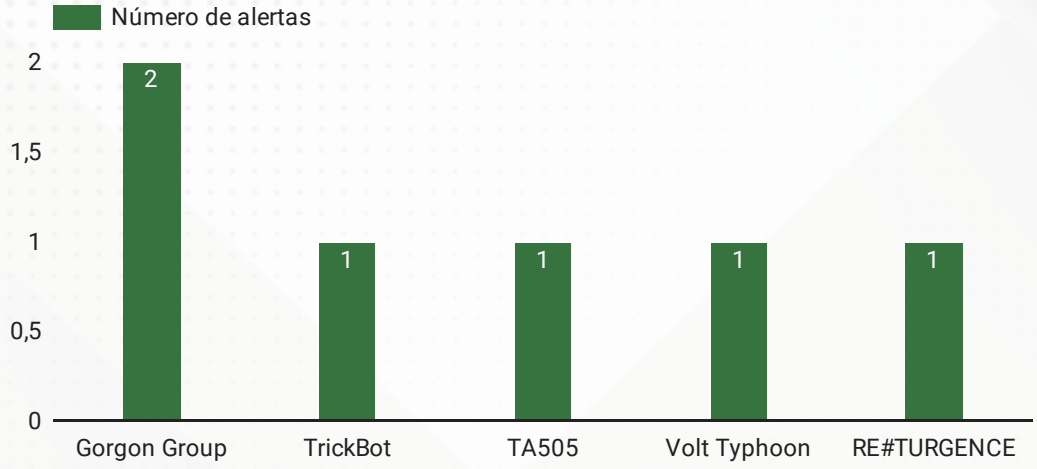
Alertas por criticidad

Comparativa Trimestral IOC



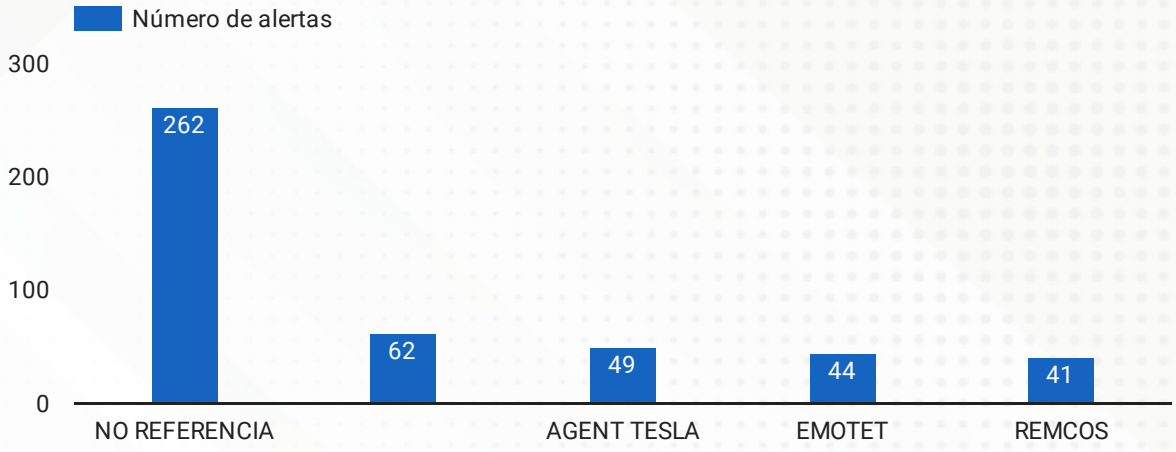
MNEMO

Top 5 actores de amenaza identificados según número de alertas reportadas



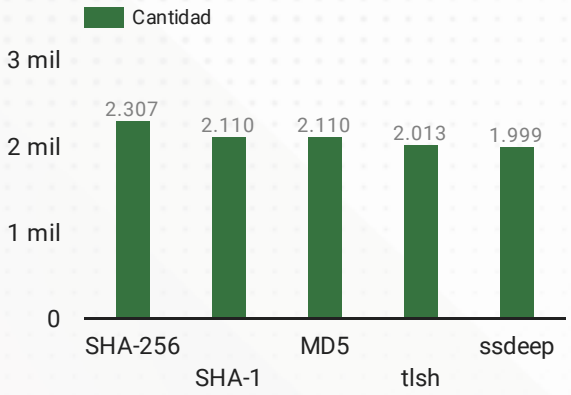
Los gráficos hacen referencia a datos recopilados durante el mes de Enero. En la parte superior, podemos ver los actores de amenazas relacionados por el número de alertas reportadas, siendo estos los cinco principales del mes de Enero. En la parte inferior, se encuentran los gráficos que representan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

Top 5 Malware identificados según número de alertas reportadas

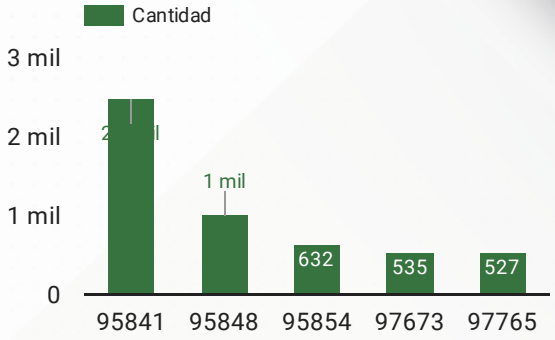


MNEMO

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



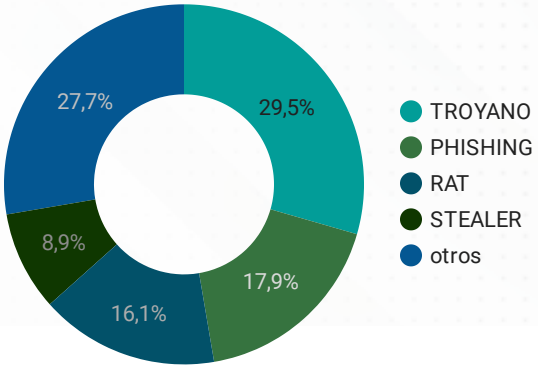
Top 5 de las alertas con mayor número de IoC reportados en el mes



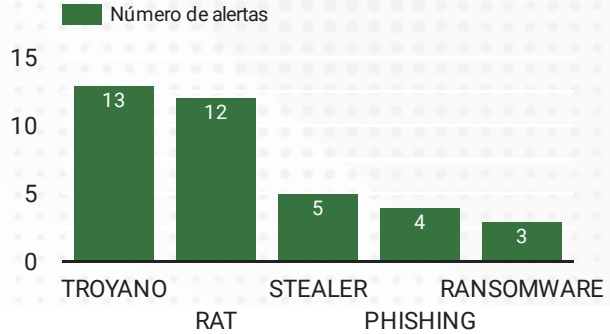
En los siguientes gráficos podemos ver datos recopilados a lo largo del mes de Enero. Los dos gráficos superiores son el resultado de la relación del número de IoC (Indicadores de Compromiso) reportados. El gráfico superior izquierdo muestra los tipos de IoC por cantidad reportada, mientras que en el 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 las alertas del mes de Enero, 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 mes.

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

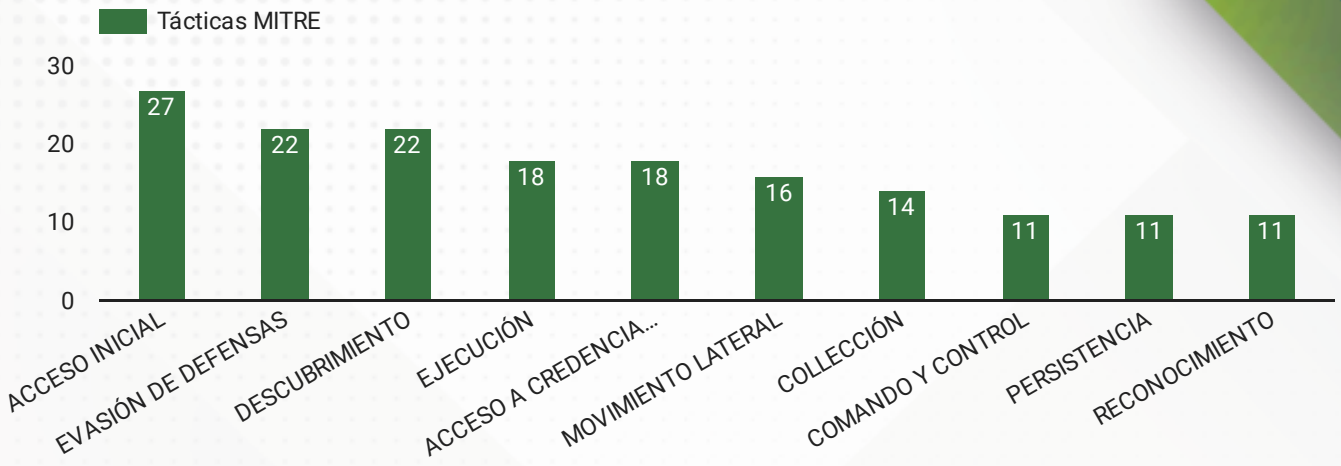


Número de alertas correspondientes al top 5 vectores

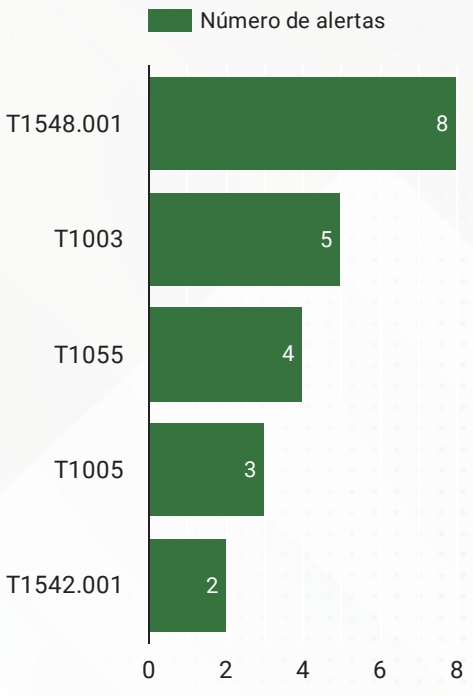


MNEMO

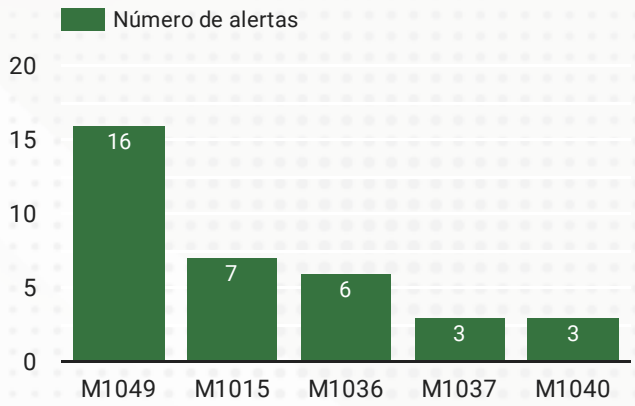
10 Tácticas reportadas en el transcurso del mes



En la parte superior se encuentran las 10 tácticas más reportadas durante el mes de Enero, 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 a las contramedidas preventivas que, según el framework Mitre, se deberían utilizar para prevenir incidentes derivados de los tipos de malware utilizados y reportados durante el mes de Enero.



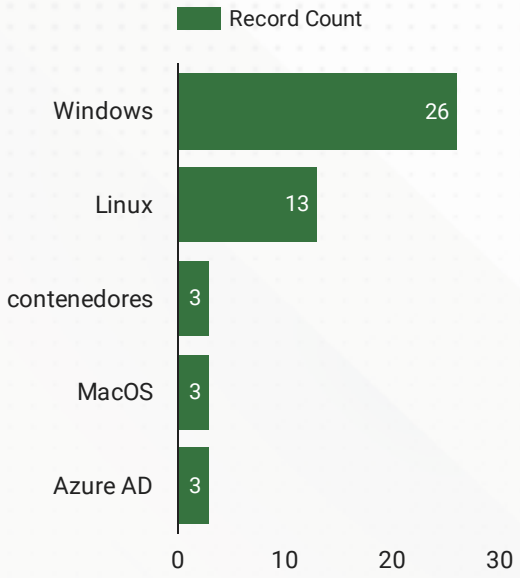
Top 5 de los códigos mitigación más reportados en el mes



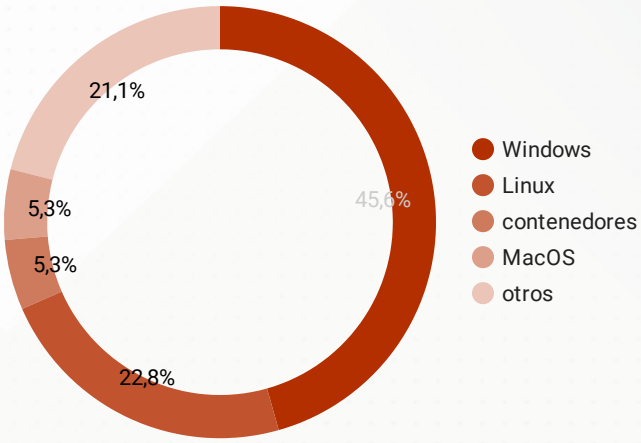
Top 5 de las técnicas más reportados en el mes

MNEMO

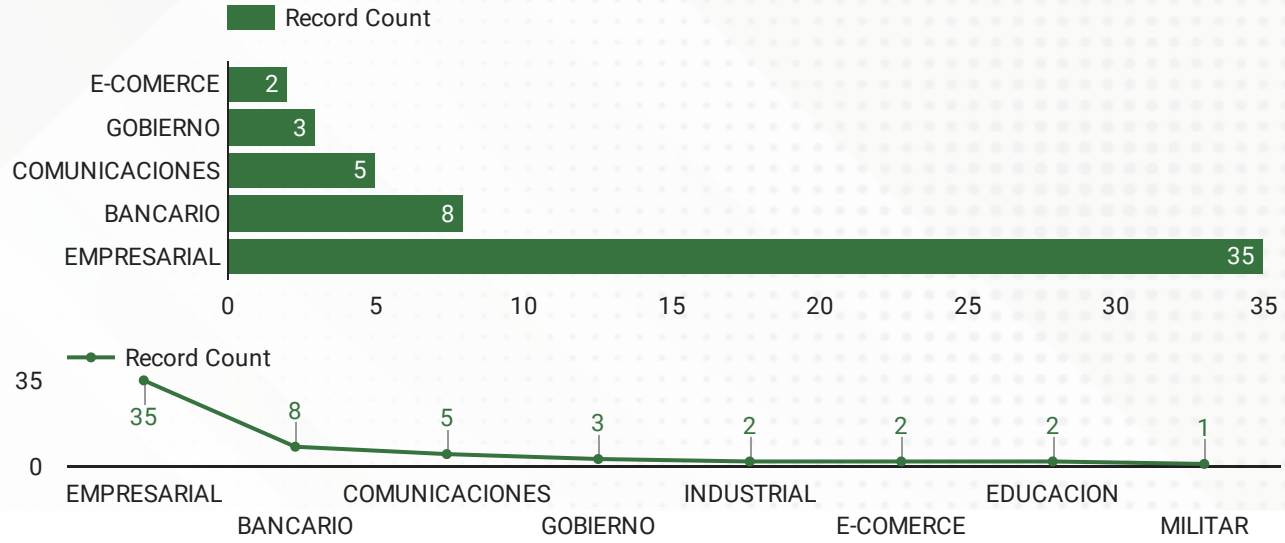
Top 5 productos más afectados en el transcurso del mes



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



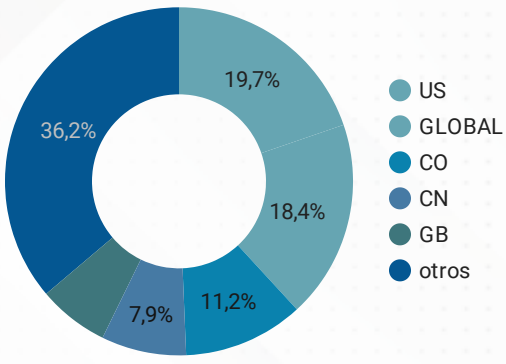
En la parte superior izquierda se muestran los productos más afectados, según lo que muestra el framework de Mitre, en relación a las técnicas reportadas en las alertas del mes de Enero. De igual manera, en la parte superior derecha se presenta este mismo resultado, pero en términos de porcentaje de 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 mes debido a su grado de susceptibilidad.

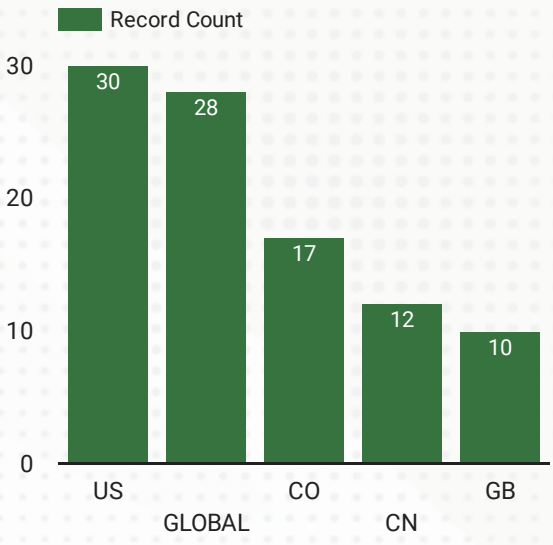


Top 10 países afectados según número de alertas reportadas

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.

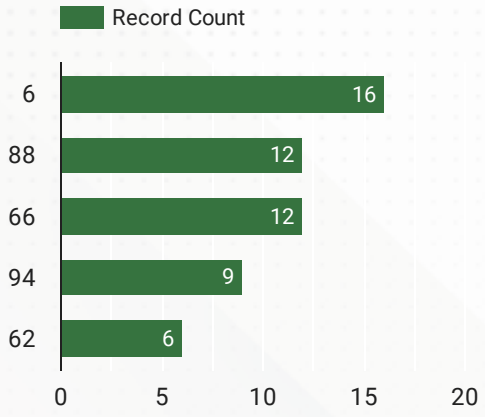
En la parte inferior izquierda, encontramos el top 5 de los países afectados, expresado como porcentaje de afectación con respecto a las alertas en las que se reportó su afectación. El gráfico de la derecha muestra el número de alertas en las que se reportó la afectación de estos países.



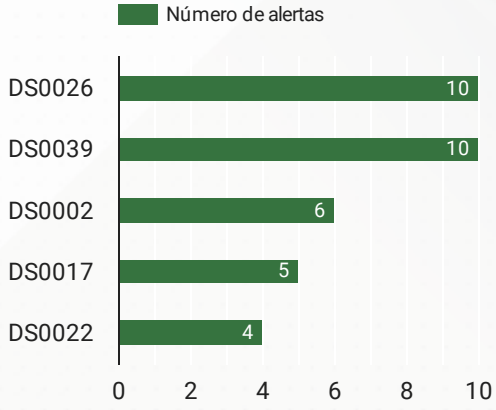


MNEMO

Top 5 Códigos Capec reportados según número de alertas reportadas



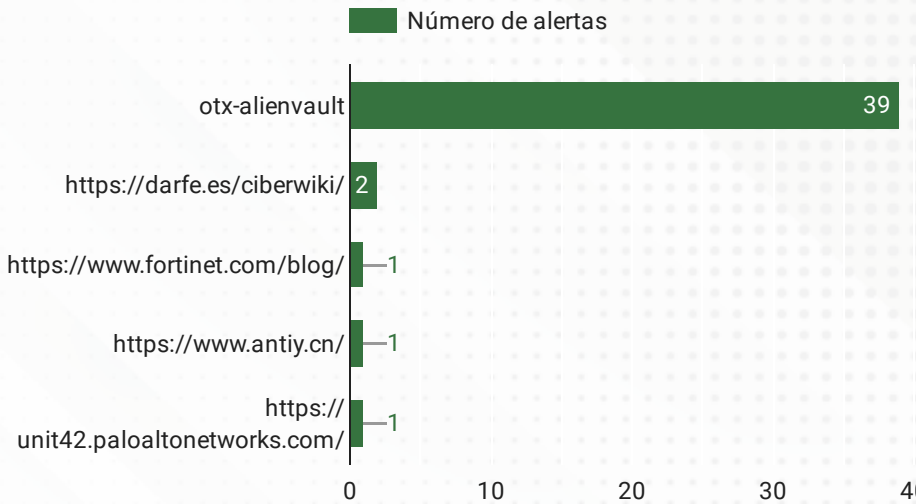
Top 5 Códigos Datasource reportados según número de alertas reportadas



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 Enero.

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 .

MN E MO

MNEMO

INFORME MENSUAL DE VIGILANCIA ENERO 2024

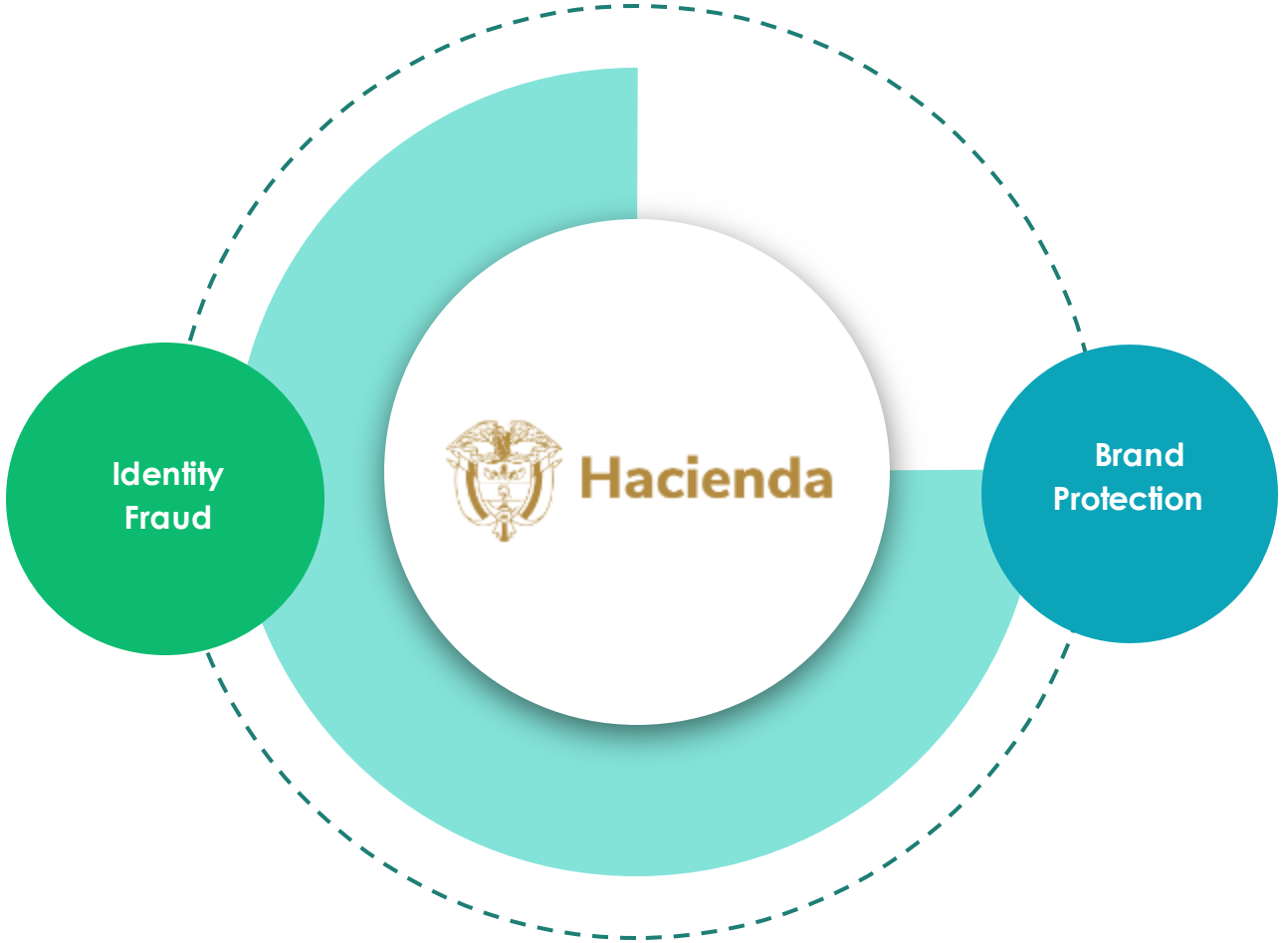
02 FEBRERO 2024

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

2 Dominios.
8 Abusos de marca en RRSS.
1 Suplantación de identidad en RRSS.



3 Menciones de marca.

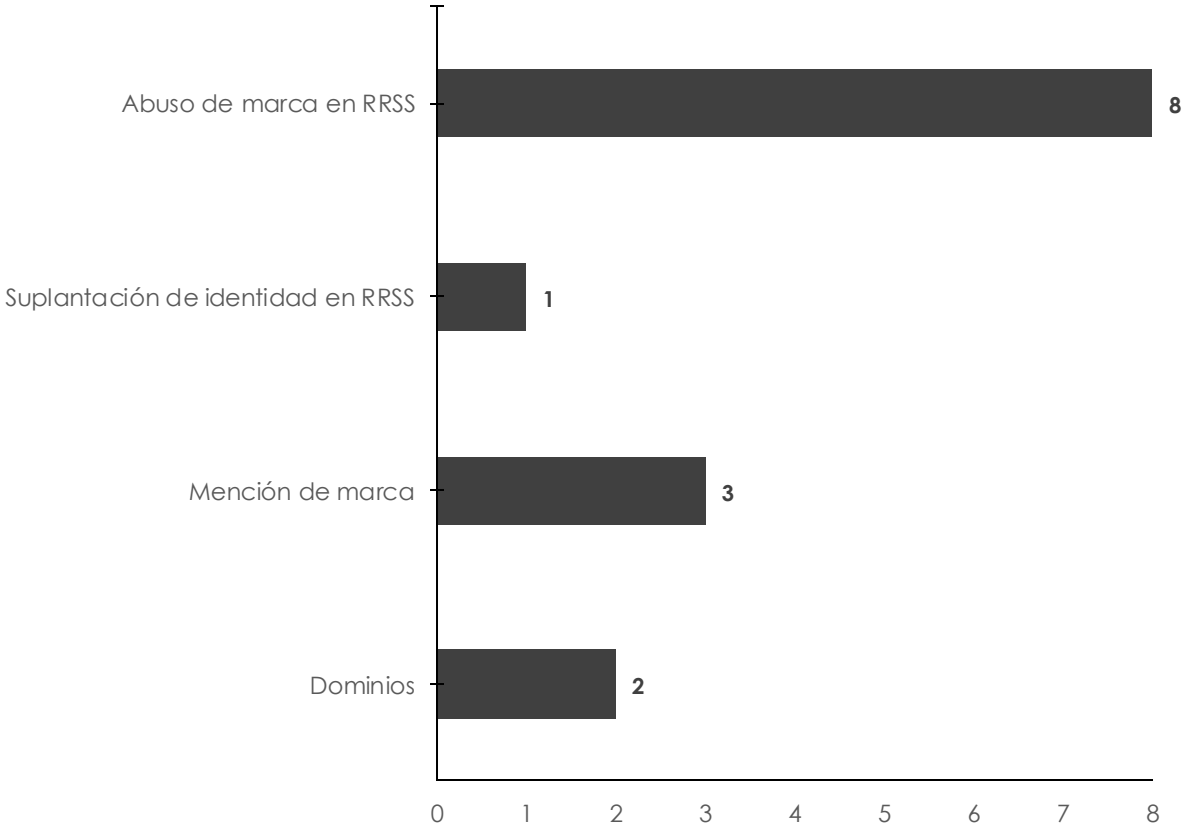
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

MNEMO

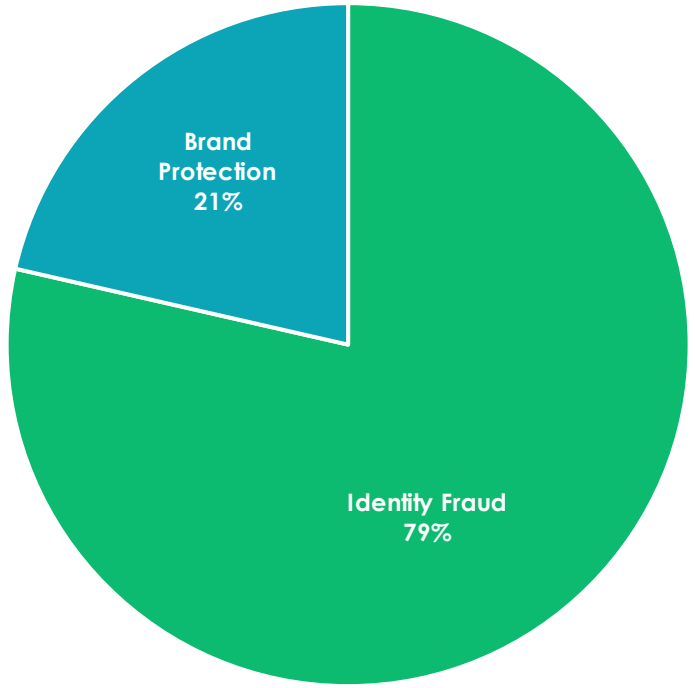
Servicio de Vigilancia

KPIs > Comportamiento del servicio global Vigilancia

Nº Total de Alertas enviadas: 14



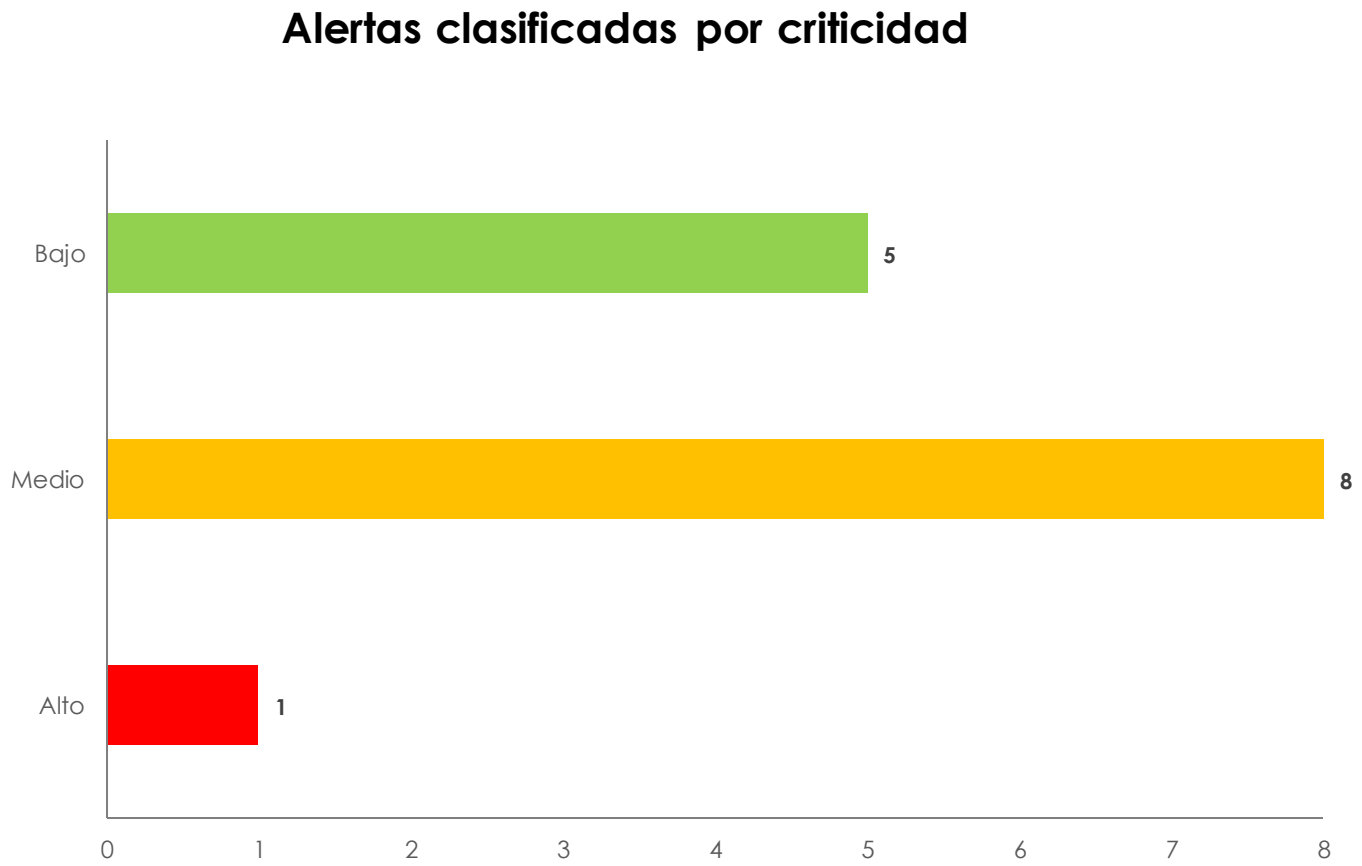
% de afectación por subservicio



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



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 enero de 2024.

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 > Vigilancia de Dominios- Comportamiento Global

Nº Total de Alertas enviadas: 2

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

KPIs > Dominios - Estadística Global

DOMINIO	CLASIFICACIÓN	TICKET
ministeriodehaciendas.com/ ww25.ministeriodehacienda.com/ ministeriodehaciendas.info/	**Parking**	**96911**
ministeriohacienda.com minhacienda.com/	**Parking**	**97023**

Casos detectados:

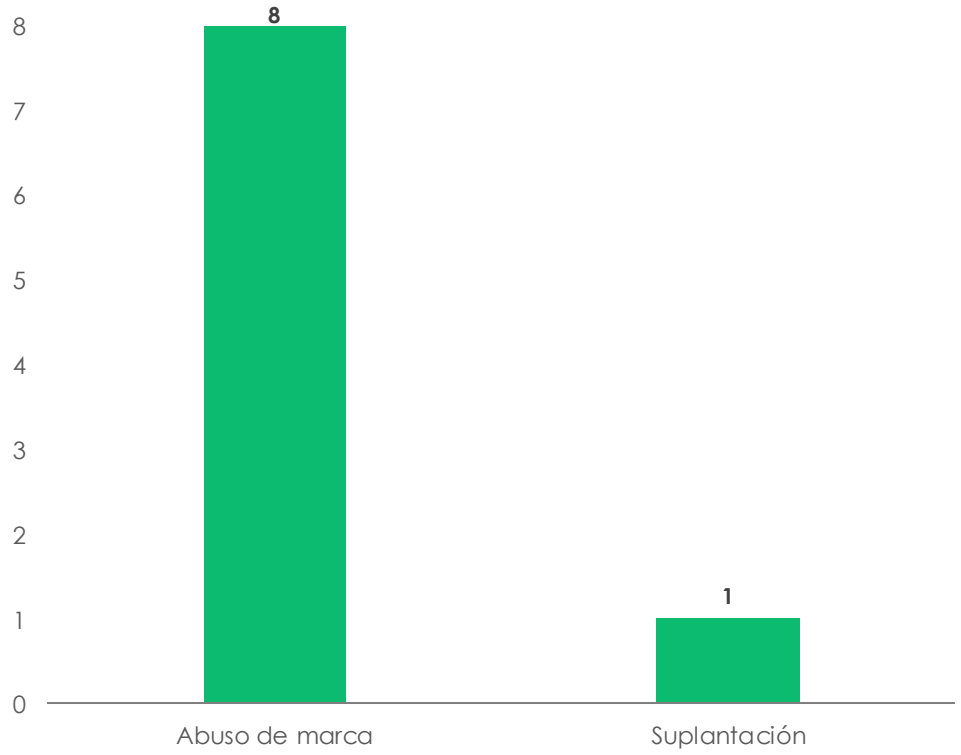
Durante el periodo en mención se reportaron **2 tickets,** los cuales teniendo en cuenta su combinación de registro semejante al dominio oficial del ministerio de hacienda y crédito público, fueron categorizados con una clasificación especifica de dominio.

Servicio de Vigilancia

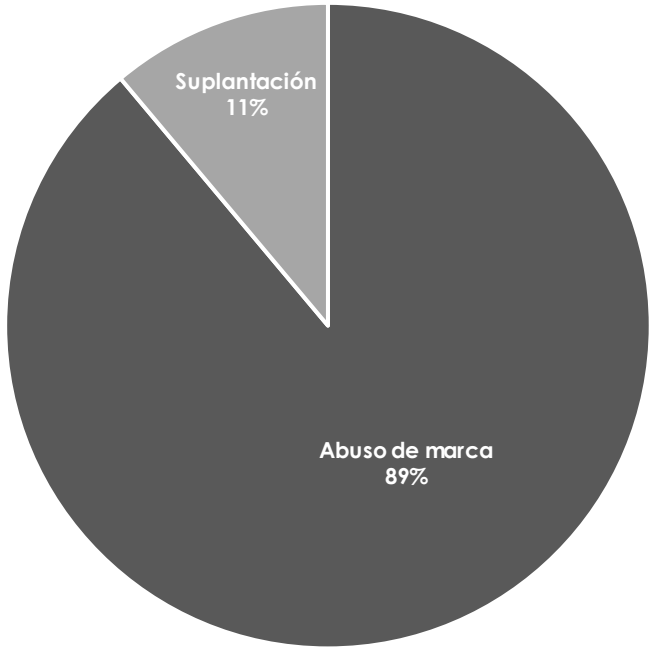
Redes Sociales > **Suplantación / Abuso de marca / Ciberfraude**

Nº de alertas enviadas: 9

Volumetría por tipo de amenaza



% de afectación por tipo de amenaza

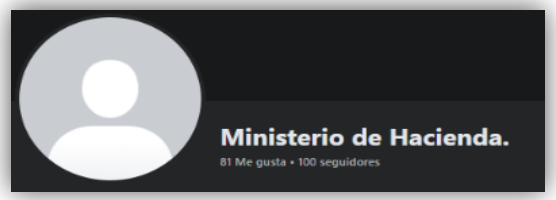


NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

Redes Sociales > **Abuso de marca**

A continuación, se relacionan algunos de los abusos de marca identificados en la red social Facebook, donde las cuentas usan el nombre de la entidad sin autorización, siendo estas catalogadas como "cuentas no legítimas".



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

Servicio de Vigilancia

Redes Sociales > **Suplantación de identidad**

A continuación, se relaciona la suplantación de identidad identificada en la red social de Tik Tok que hace uso de imagen y nombre del ministerio de hacienda y crédito público.

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.

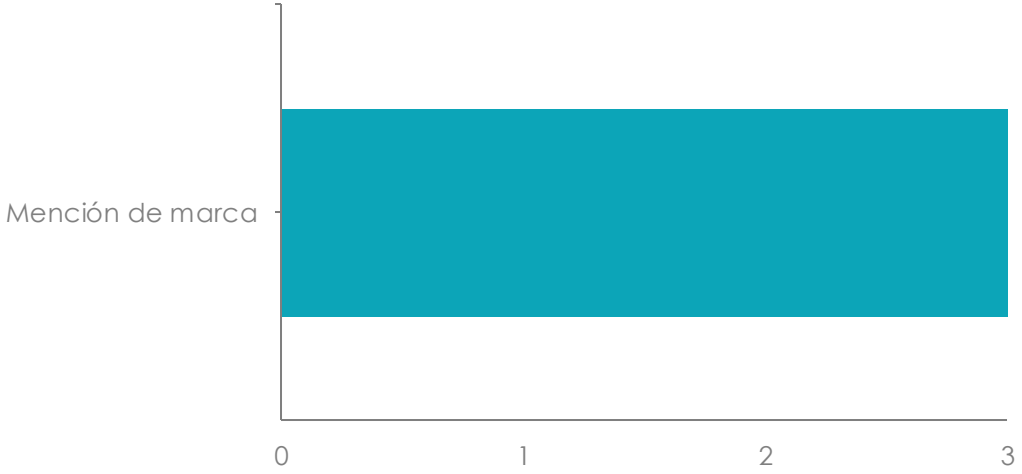
NIVEL DE SEGURIDAD DE ESTE DOCUMENTO: CONFIDENCIAL
No está permitida su reproducción, distribución o comunicación fuera del destinatario.

Servicio de Vigilancia

Brand protection > Ataques a la reputación / Menciones informativas

Nº Total de Alertas enviadas: 3

Volumetría por tipo de amenaza



% de afectación por tipo de amenaza

Mención de marca

Algunos casos:

- Artículo publicado por el medio " larepublica", donde informaron que el Ministerio de Hacienda y Crédito Público, presentó el informe consolidado de la ejecución del "Presupuesto General de la Nación" para el año 2023, detallando el total del presupuesto y el manejo que se le dio al mismo en cuanto a obligaciones, inversiones y deudas del país.
- Artículo publicado por el medio "ambientestereo", donde informaron que en una séptima mesa técnica llevada a cabo el 24 de enero en el Ministerio de Hacienda, los transportadores y el gobierno no lograron llegar a un acuerdo sobre el ajuste del precio del diésel para este año.

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

Servicio de Vigilancia

OBSERVACIONES

- Se sugiere **validar los eventos** que representan riesgo para la entidad y otorgar **retroalimentación al equipo de vigilancia digital** para tomar acciones de mitigación.
- Se sugiere **validar internamente** la posibilidad de comprar los dominios para evitar posibles acciones maliciosas de terceros.
- Las cuentas creadas en las redes sociales causan un **daño reputacional y de credibilidad** frente a la entidad, por lo anterior se sugiere **validar los perfiles que no sean legítimos** y tomar acción.
- Los eventos notificados bajo la tipología de **mención de marca** fueron de **carácter informativo** y **no representan** riesgo para la entidad.
- El **nivel de criticidad** durante el mes de enero se sitúa en **medio - bajo.**

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

CTI

INFORME
CYBER SECURITY WARNING
EARLY

ENERO 2024

EQUIPO DE CYBER THREAT INTELLIGENCE

MIN-HACIENDA

CYBER THREAT INTELLIGENCE

MNEMO

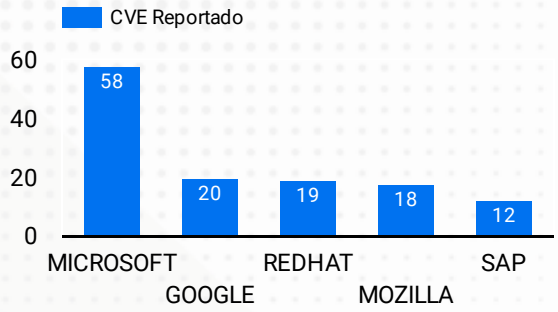
ALERTAS REPORTADAS 29

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

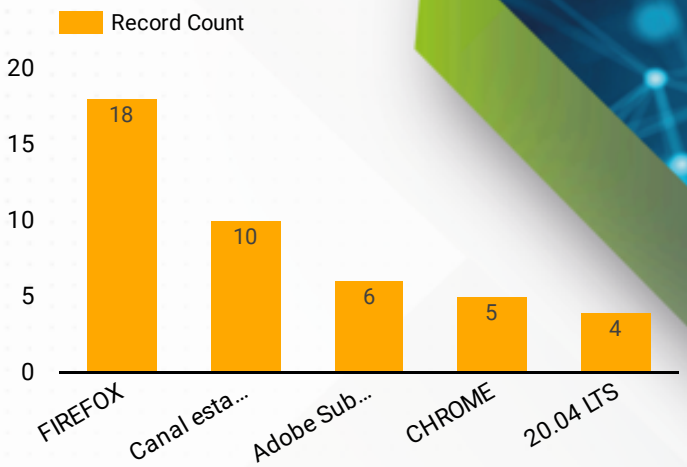
VULNERABILIDADES REPORTADAS 165

CYBER THREAT INTELLIGENCE

MNEMO

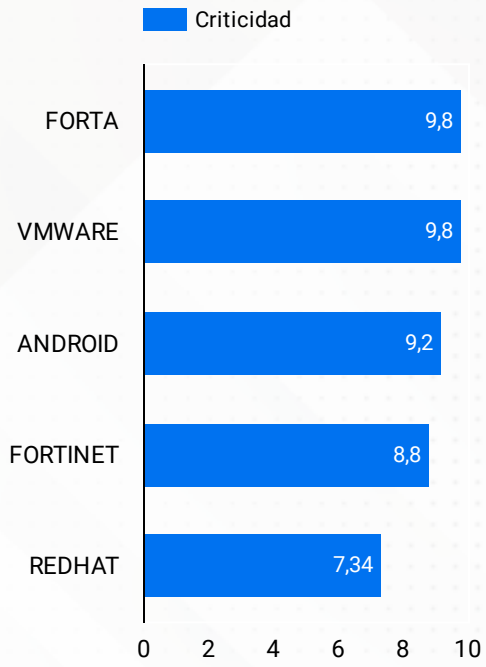


Top 5 fabricantes con mayor número de vulnerabilidades reportadas

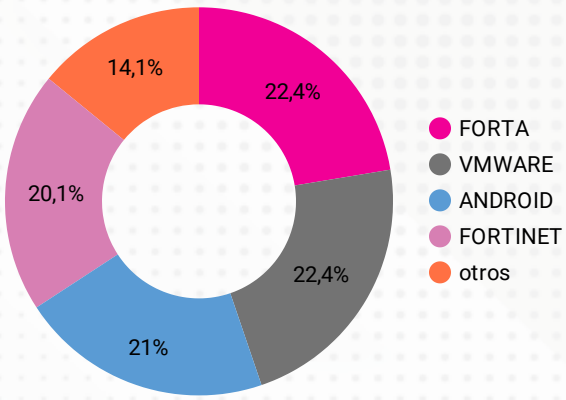


Top 5 productos con mayor número de reportes en el mes

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



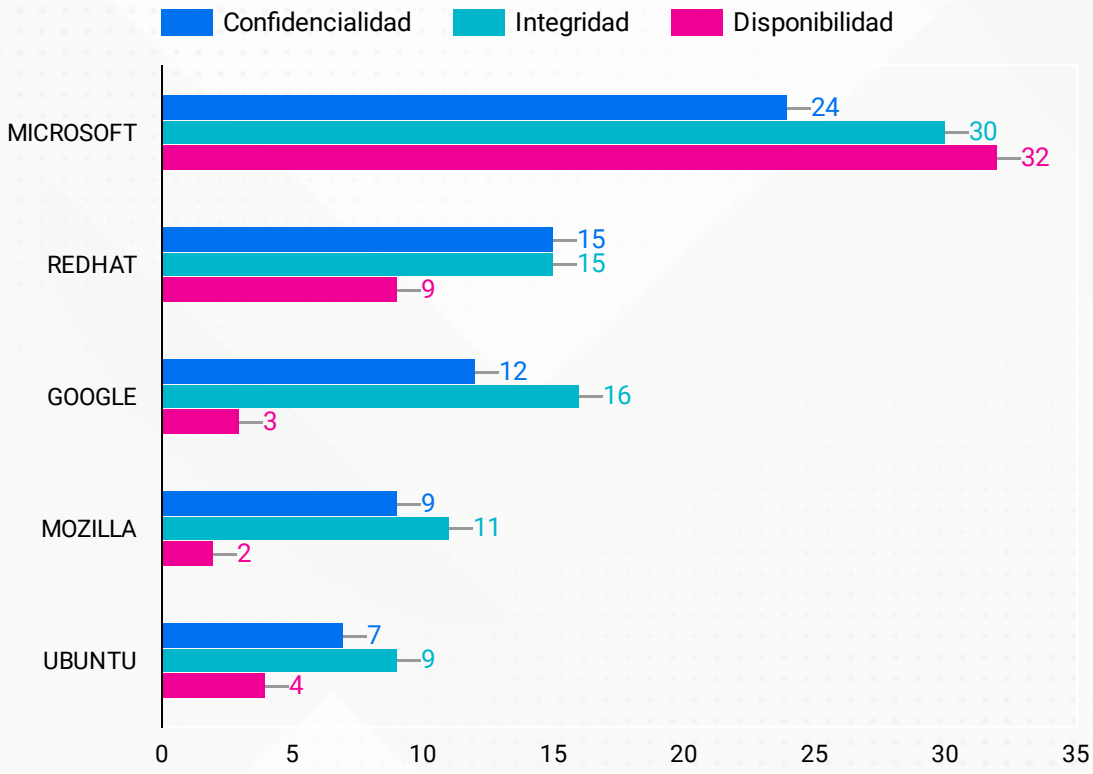
Nivel de criticidad promedio por fabricante, tomando el cvss reportado por cada uno



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

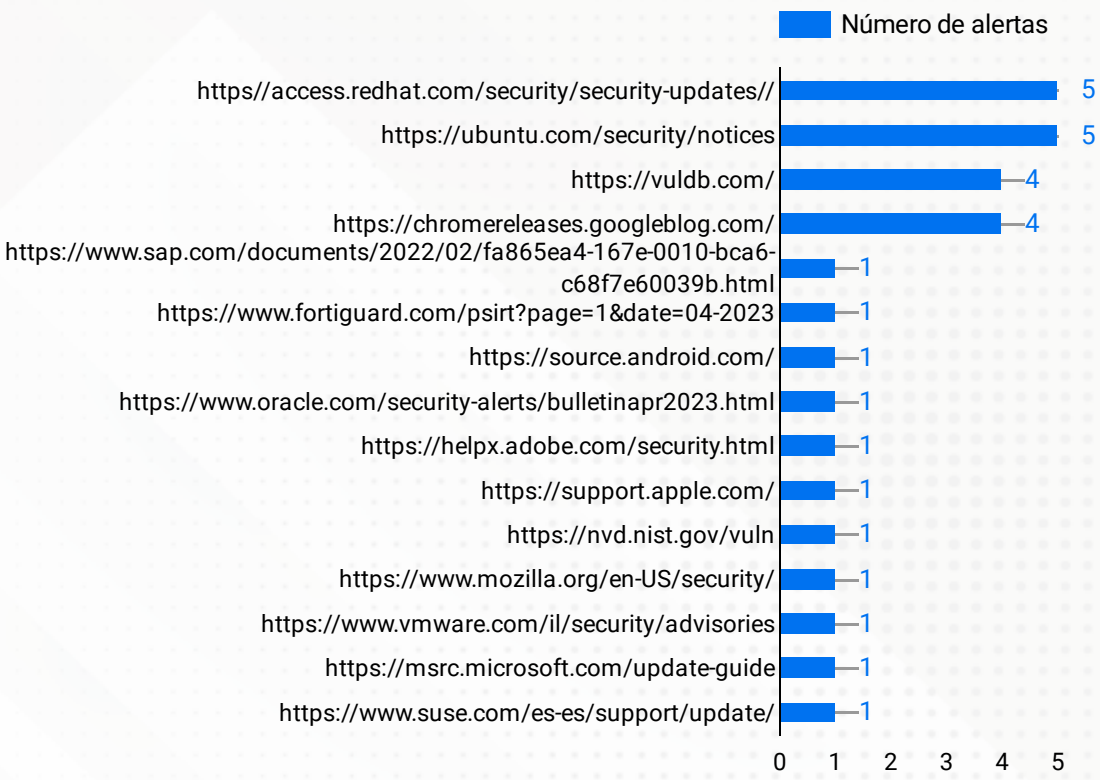
Total productos reportados

160

Total fabricantes reportados

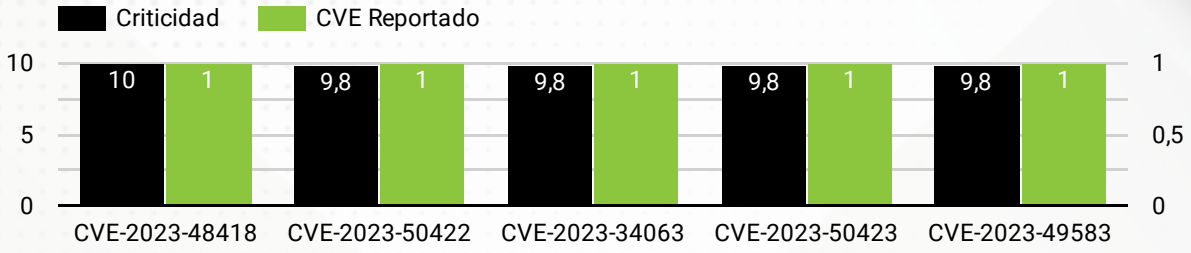
18

Número de CVE reportadas por fuente

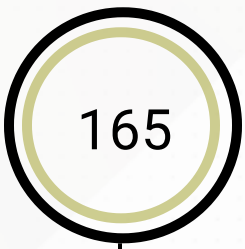


MNEMO

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

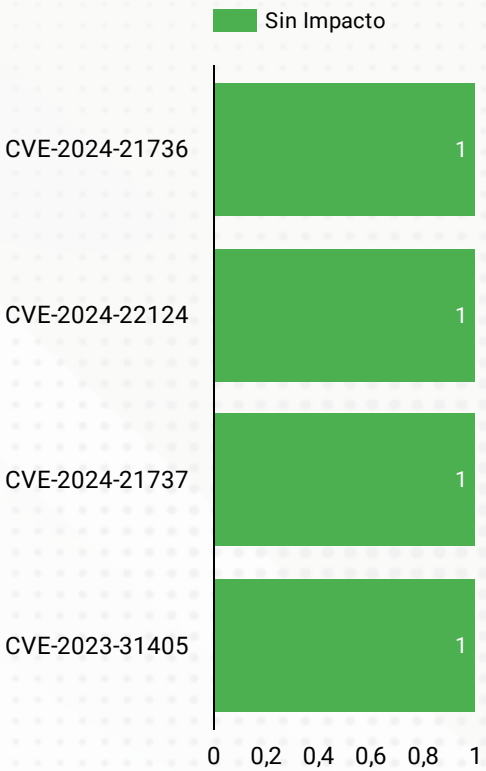


Totlal vulnerabilidades



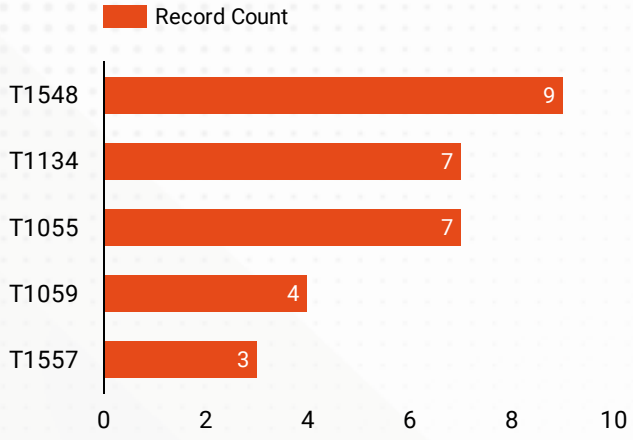
Cantidad general de Indicadores recopilados y reportados en el transcurso del mes.

Vulnerabilidades sin criticidad reportada



MNEMO

Top 5 de técnicas con mayor índice de reporte



NÚMERO DE CÓDIGOS ATT&CK REPORTADOS

76

NÚMERO DE EVENTOS CON CÓDIGOS ATT&CK REPORTADOS

121

Descripción

T1548 - Abuse Elevation Control Mechanism
Los adversarios pueden eludir los mecanismos diseñados para controlar los privilegios elevados para obtener permisos de nivel superior. La mayoría de los sistemas modernos contienen mecanismos nativos de control de elevación cuyo objetivo es limitar los privilegios que un usuario puede ejercer en una máquina.

T1134 - Access Token Manipulation
Los adversarios pueden modificar los tokens de acceso para operar bajo un contexto de seguridad de sistema o usuario diferente para realizar acciones y eludir los controles de acceso. Windows utiliza tokens de acceso para determinar la propiedad de un proceso en ejecución.

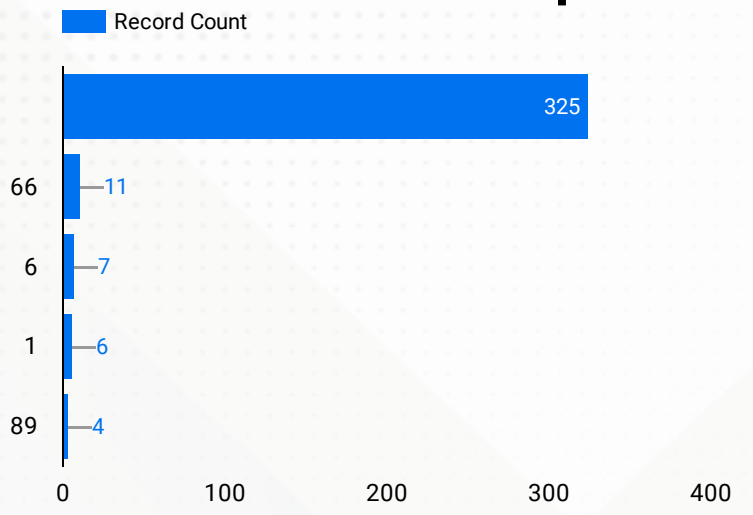
T1055 - Process Injection
Los adversarios pueden inyectar código en los procesos para evadir las defensas basadas en procesos y posiblemente elevar los privilegios. La inyección de proceso es un método para ejecutar código arbitrario en el espacio de direcciones de un proceso en vivo separado. Ejecutar código en el contexto de otro proceso puede permitir el acceso a la memoria del proceso, al sistema

T1059 - Command and Scripting Interpreter
Los adversarios pueden abusar de los intérpretes de comandos y scripts para ejecutar comandos, scripts o archivos binarios. Estas interfaces y lenguajes proporcionan formas de interactuar con sistemas informáticos y son una característica común en muchas plataformas diferentes.

T1557 - Adversary-in-the-Middle
Los adversarios pueden intentar posicionarse entre dos o más dispositivos en red utilizando una técnica de adversario en el medio (AiTM) para respaldar comportamientos de seguimiento como rastreo de red, manipulación de datos transmitidos o ataques de repetición (explotación para acceso a credenciales).

MNEMO

Top 5 de Códigos Capec con mayor índice de reporte



NÚMERO DE CÓDIGOS CAPEC REPORTADOS

82

NÚMERO DE EVENTOS CON CÓDIGOS CAPEC REPORTADOS

143

Descripción

CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
En las aplicaciones, particularmente en las aplicaciones web, el acceso a la funcionalidad está mitigado por un marco de autorización. Este marco asigna listas de control de acceso (ACL) a elementos de la funcionalidad de la aplicación; particularmente URL para aplicaciones web.

CAPEC - 6: Argument Injection
Un atacante cambia el comportamiento o el estado de una aplicación objetivo mediante la inyección de datos o sintaxis de comandos mediante el uso del objetivo de argumentos no validados y no filtrados de servicios o métodos expuestos.

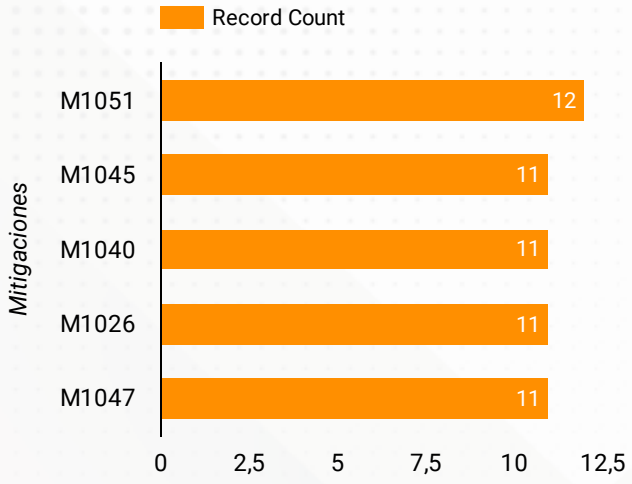
CAPEC-27: Leveraging Race Conditions via Symbolic Links
Este ataque aprovecha el uso de enlaces simbólicos (Symlinks) para escribir en archivos confidenciales. Un atacante puede crear un enlace simbólico a un archivo de destino al que no podría acceder de otro modo. Cuando el programa privilegiado intenta crear un archivo temporal con el mismo nombre que el enlace simbólico, en realidad escribirá en el archivo de destino al que apunta el enlace simbólico de los atacantes.

CAPEC - 66: SQL Injection
Este ataque explota el software de destino que construye declaraciones SQL basadas en la entrada del usuario. Un atacante crea cadenas de entrada de modo que cuando el software de destino construye declaraciones SQL basadas en la entrada, la declaración SQL resultante realiza acciones distintas a las previstas por la aplicación. La inyección SQL resulta de una falla de la aplicación al validar adecuadamente la entrada.

CAPEC-89: Pharming
Un ataque de pharming ocurre cuando se engaña a la víctima para que ingrese datos confidenciales en ubicaciones supuestamente confiables, como el sitio de un banco en línea o una plataforma comercial. Un atacante puede hacerse pasar por estos sitios supuestamente confiables y hacer que la víctima sea dirigida a su sitio en lugar del originalmente previsto. Pharming no requiere la inyección de scripts ni hacer clic en enlaces maliciosos para que el ataque tenga éxito.

MNEMO

Top 5 de Mitigaciones con mayor índice de reporte



NÚMERO DE CÓDIGOS ATT&CK REPORTADOS

38

NÚMERO DE EVENTOS CON CÓDIGOS ATT&CK REPORTADOS

188

Descripción

M1045 - Code Signing
Haga cumplir la integridad binaria y de las aplicaciones con verificación de firma digital para evitar que se ejecute código que no sea de confianza.

M1040 - Behavior Prevention on Endpoint
Utilice capacidades para evitar que se produzcan patrones de comportamiento sospechosos en los sistemas de endpoints. Esto podría incluir comportamientos sospechosos de procesos, archivos, llamadas API, etc.

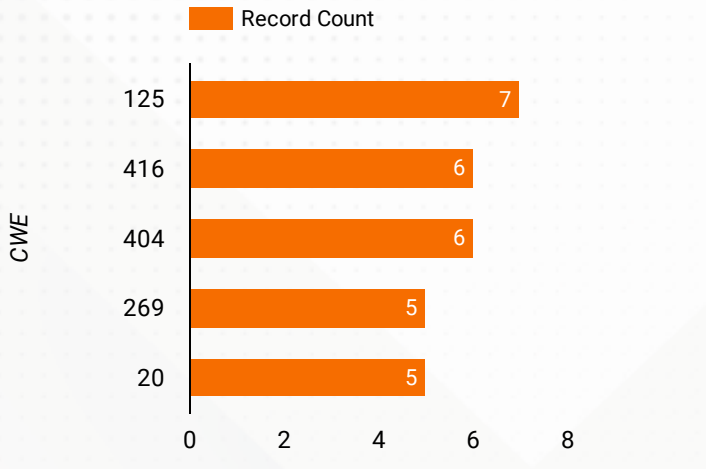
M1026 - Privileged Account Management
Administre la creación, modificación, uso y permisos asociados a cuentas privilegiadas, incluidas SISTEMA y raíz.

M1051: Update Software
Realice actualizaciones periódicas de software para mitigar el riesgo de explotación.

M1047 - Audi
Realizar auditorías o escaneos de sistemas, permisos, software inseguro, configuraciones inseguras, etc. para identificar posibles debilidades.

Las mitigaciones de MITRE son medidas de seguridad que se utilizan para reducir el riesgo de un ataque cibernético. Estas medidas se basan en la matriz de tácticas, técnicas y procedimientos (TTP) de MITRE ATT&CK y se centran en reducir la efectividad de las técnicas de ataque. Ejemplos de mitigaciones comunes incluyen la autenticación multifactor y la detección y respuesta de amenazas

Top 5 de Códigos CWE con mayor índice de reporte



NÚMERO DE CÓDIGOS ATT&CK REPORTADOS

27

NÚMERO DE EVENTOS CON CÓDIGOS ATT&CK REPORTADOS

68

Descripción

CWE-125: Out-of-bounds Read
El producto lee datos más allá del final o antes del comienzo del búfer previsto.

CWE-416: Use After Free
Hacer referencia a la memoria después de haberla liberado puede provocar que un programa falle, utilice valores inesperados o ejecute código.

CWE-269: Improper Privilege Management
El producto no asigna, modifica, rastrea ni verifica adecuadamente los privilegios de un actor, lo que crea una esfera de control no deseada para ese actor.

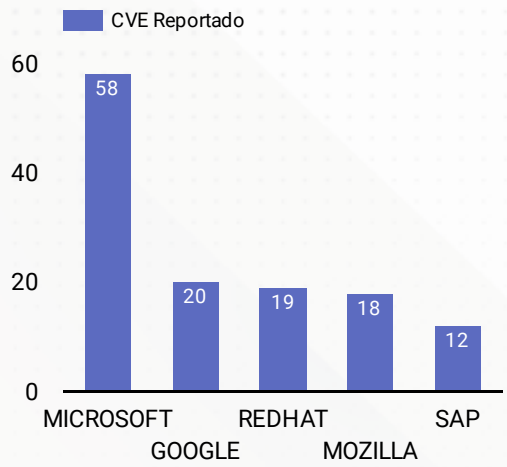
CWE-404: Improper Resource Shutdown or Release
El producto no libera o libera incorrectamente un recurso antes de que esté disponible para su reutilización.

CWE-20: Improper Input Validation
El producto recibe entradas o datos, pero no valida o valida incorrectamente que la entrada tiene las propiedades necesarias para procesar los datos de forma segura y correcta.

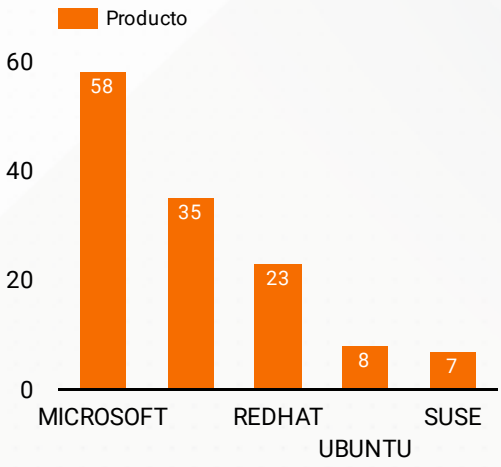
Los códigos CWE (Common Weakness Enumeration) se utilizan para identificar y categorizar debilidades comunes de seguridad en software y sistemas. Estos códigos son una lista numérica y alfanumérica que asigna un identificador único a cada tipo de debilidad o vulnerabilidad de seguridad conocida. CWE 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

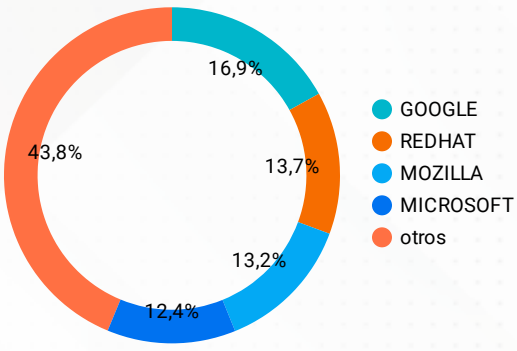
Top 5 de fabricantes con base en CVE reportados



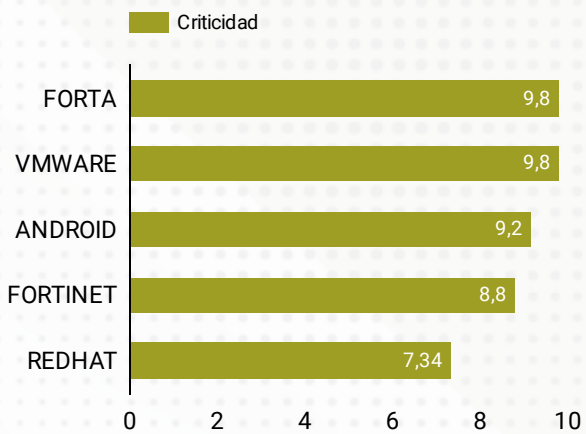
Top 5 de fabricantes con base en Productos reportados



TOP de fabricantes promedio con mayor índice de criticidad reportado



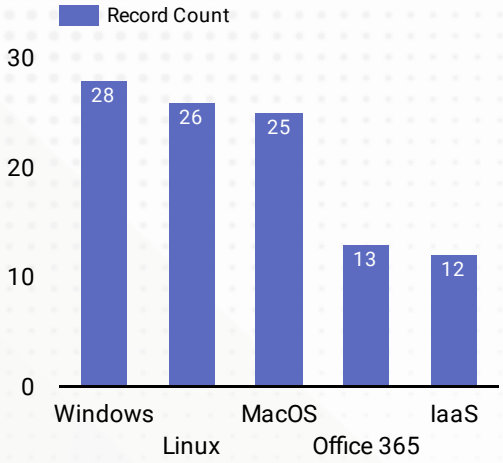
Promedio de participación

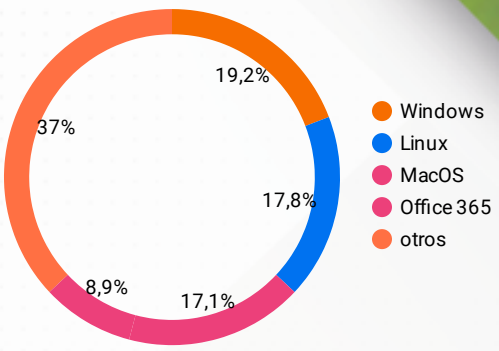


CYBER THREAT INTELLIGENCE

MNEMO

Top 5 de plataformas afectadas

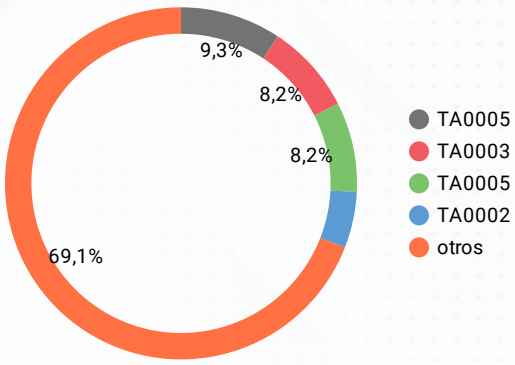


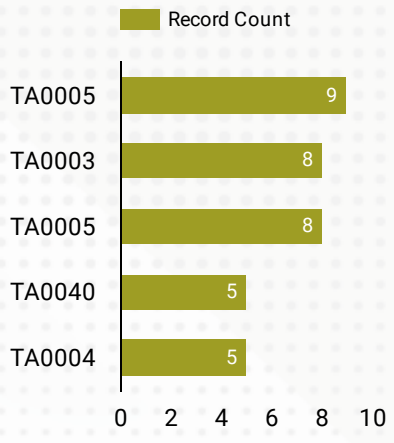


Tener en cuenta las tácticas de MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es fundamental en ciberseguridad por varias razones:

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 5 de tácticas usadas





MNEMO

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 3

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	16/02/2024, 16:00
Expedición	16/02/2024, 16:51
Vencimiento	17/03/2024

Ítem	Descripción	Cantidad	Vr. Total
1	Monitoreo,Diagnóstico,generación de alertas y recomendaciones. Contrato: 3.471-2023 Periodo de facturación:01-01-2024 al 31/01/2024	1.00	88,951,900.00
2	Servicio de gestión y análisis de vulnerabilidades. Contrato: 3.471-2023 Periodo de facturación:01-01-2024 al 31/01/2024	1.00	2,984,600.00
3	Análisis Forense(436.440 Horas) Contrato: 3.471-2023 Periodo de facturación:01-01-2024 al 31/01/2024	1.00	11,783,880.00

Total items: 3

Valor en Letras:
Ciento tres millones setecientos veinte mil trescientos ochenta pesos m/cte

Condiciones de Pago:
Crédito - Cuota No. 001 vence el 2024-03-17 por $ 103,720,380.00

Total Bruto	87,159,983.20
IVA 19%	16,560,396.80
Total a Pagar	**103,720,380.00**

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 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: 17c1616b49e38ccc2fc764a1d91dccbaf3ae1f2c97cbf9a5e9186f9c531a926a1b9e3ceb2db45aa989bd0dfc4b2af87c

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

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 septiembre de 2023 al 2 de febrero 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 **JOSE IGNACIO SALAZAR GOMEZ**, 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 febrero de 2024.

At.

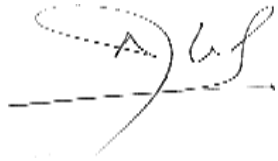
JOSE IGNACIO SALAZAR GOMEZ
Revisor Fiscal T.P. 27.398-T
C.C. 14.239.581 de Ibagué – Cel. 3158889246 joseignaciosago@hotmail.com

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 dieciséis (16) días del mes de Febrero 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

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	
2024-01	2024-02		9462991562	E	2024/02/19			0		

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	Dias	Codigo	Días	Tarifa	Días	Exonerado SENA e ICBF
SUCURSAL: PRINCIPAL (96 Afiliados)																															
Centro de Trabajo: ACTIVIDADES EN CLIIENTE VISITA / TRASLADOS (19 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (19 Afiliados)																															
1	CC	1023002210	ACEVEDO VARGAS OSCAR IVAN																		23020 1	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
2	CC	93387321	ARANA REYES JAMES GUSTAVO																		25-14	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	No
3	CC	67016350	BOCANEGRA VALBUENA ANA MARIA																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	No
4	CC	1122651302	CARO ROA JONATHAN																		23030 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
5	CC	79136413	CASTRO CORREDOR HECTOR EDISSON																		23030 1	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
6	CC	1013592039	EMBUS IPIA JULIAN ANDRES																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
7	CC	52794429	LEGUIZAMON TARAZONA NINI LIZETH																		25-14	30	EPS001	30	CCF24	30	14-25	30	1.044%	30	Si
8	CC	1073163243	ORTIZ RUBIANO WILSON LEONARDO																		23100 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
9	CC	1033687848	POMPEYO MARTINEZ VICTOR ALFONSO																		23030 1	30	EPS008	30	CCF24	30	14-25	30	1.044%	30	Si
10	CC	79865487	PUENTES CASTRO DAVID EDUARDO																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
11	CC	79717549	RODRIGUEZ JOHN FERNANDO																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
12	CC	52824814	RODRIGUEZ MURCIA NIDIA ESPERANZA																		23030 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
13	CC	80791790	ROJAS ARIAS RICARDO																		23020 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
14	CC	80066361	ROMERO ARCHILA DANIEL DARIO																		23020 1	30	MIN001	30	CCF24	30	14-25	30	1.044%	30	Si
15	CC	1032439248	SANCLEMENTE RAMIREZ SERGIO GIOVANI																		23100 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	Si
16	CC	24659147	VALDES RAMIREZ ALBA LIBIA																			0	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
17	CC	79950164	VARGAS HINCAPIE FERNANDO													X					23030 1	1	EPS002	1	CCF24	1	14-25	1	0.000%	1	Si
18	CC	79950164	VARGAS HINCAPIE FERNANDO																		23030 1	29	EPS002	29	CCF24	29	14-25	29	1.044%	29	Si
19	CC	1032410736	VARGAS HINCAPIE HENRY																		23090 1	30	EPS005	30	CCF24	30	14-25	30	1.044%	30	No
20	CC	1022411758	VARGAS LEON MARIA CAMILA													X					23030 1	14	EPS008	14	CCF24	14	14-25	14	0.000%	14	Si
21	CC	1022411758	VARGAS LEON MARIA CAMILA																		23030 1	16	EPS008	16	CCF24	16	14-25	16	1.044%	16	Si
Centro de Trabajo: ADMINISTRACION (73 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (73 Afiliados)																															
22	CC	1014306151	ABRIL MONTES SERGIO LEONARDO																		23020 1	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
23	CC	1019151775	ACOSTA MURILLO JUAN CAMILO																		25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
24	CC	93128242	ALDANA RODRIGUEZ TITO FERNANDO																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si

25	CC	1031162097	ARISTIZABAL ANGEL LAURA VANESSA																230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
26	CC	1032381933	AVILA BERMUDEZ WILLIAM ALEXANDER																231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
27	CC	1019077197	BELEÑO BUELVAS CHARLES JAVIER																230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
28	CC	3034118	BELTRAN CAMACHO CARLOS JAVIER																230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
29	CC	1012437249	BOCANEGRA MORALES LUIS FELIPE																230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
30	CC	1004268659	BONILLA ZUÑIGA ANDERSON																231001	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
31	CC	1000161032	CALLEJAS PATARROYO DAVID STEVEN																230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
32	CC	1007854099	CAMACHO MORALES SANTIAGO																230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
33	CC	1024467791	CARDENAS VARON KEVIN ANDRES						X											0	EPS010	30		0		0	0.000%	0	No
34	CC	13870244	CARRILLO ALVAREZ OSCAR																25-14	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
35	CC	1012322665	CASTAÑEDA MESA ANDREA KATHERINE																231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
36	CC	1034397473	CASTILLO IDROBO JHON FABER																	0	EPS002	30		0	14-25	30	0.522%	0	No
37	CC	1020809969	CASTILLO MENDOZA JOHN ALEXANDER																230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
38	CC	1014263133	DE SALVADOR PEÑA OSCAR DAVID																230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
39	CC	1022418490	DIAZ MONCALEANO JOSE MANUEL																230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
40	CC	79503458	GARZON RODRIGUEZ CARLOS JAVIER																25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
41	CC	1023957895	GIL MURILLO JAVIER EDUARDO																230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
42	CC	1032496477	GOMEZ LIZARAZO BRAYAN ANDRES																230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
43	CC	1019009180	GOMEZ ROJAS YENNY PAOLA																230301	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
44	CC	1110457150	GONZALEZ RUIZ JIMMY ALEJANDRO																230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
45	CC	1021665609	GRANADA VILLANUEVA JOHAN STIVEN						X											0	EPS005	30		0	14-25	30	0.522%	0	No
46	CC	1076657683	GRANADOS ROCHA MIGUEL ANGEL																230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
47	CC	1000689679	GUARIN PINZON MATEO																230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
48	CC	1076663845	GUAYAZAN CORTES JONATHAN STIVEN																230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
49	CC	1033738924	GUZMAN PEÑA CARLOS ANDRES																230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
50	CC	1075658745	HERNANDEZ PUIN ANGELA PATRICIA																230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
51	CC	1099374748	LEAL GOMEZ DANIELA																230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
52	CC	52953219	LEON CERON MARIA ALEXANDRA																231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
53	CC	79992827	MARROQUIN GUTIERREZ DIDIER																230201	30	MIN002	30	CCF24	30	14-25	30	0.522%	30	Si
54	CC	1000032122	MARTIN GARCES JUAN DAVID																230301	30	EPSC34	30	CCF24	30	14-25	30	0.522%	30	Si
55	CC	79836643	MARTINEZ RODRIGUEZ JHON BAIRON																25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
56	CC	1023951729	MARTINEZ VASQUEZ MAIKOL ESTIVEN																230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
57	CC	1000719172	MARTINEZ BECERRA MARIA JOSE																230301	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si

58	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE											X							230301	5	EPS017	5	CCF24	0	14-25	5	0.000%	0	Si
59	CC	1000940557	MEDINA GUEVARA ANDRES FELIPE																		230301	25	EPS017	25	CCF24	25	14-25	25	0.522%	25	Si
60	CC	1000717997	MELO MOSQUERA DANIEL RENE																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
61	CC	98632570	MESA MENDEZ CARLOS MANUEL																		230201	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
62	CC	1022947945	MOLANO JIMENEZ JESUS RICARDO																		230201	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
63	CC	1110173553	MORA TABARES MIGUEL ANGEL																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
64	CC	1033711407	MURCIA TORRES JHON FREDY																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
65	CC	1023907046	OCHOA ROJAS ROGER JULIAN																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
66	CC	1032479763	ORJUELA CALDERON PAULA NATALIA																		231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
67	CC	1000179818	PACAVITA GONZALEZ BRAYAN ALEXANDER																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
68	CC	1030555370	PARAMO CALDERON CRISTIAN ADRIAN																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
69	CC	1023886752	PATARROYO JIMENEZ JHON JAIRO																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
70	CC	1019127504	PERDOMO GUZMAN JESSICA LILIANA																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
71	CC	1016059950	PINTO GONZALEZ CESAR ORLANDO																		230201	30	EPS037	30	CCF24	30	14-25	30	0.522%	30	Si
72	CC	1030618626	PINZON ROJAS ANDRES CAMILO																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
73	CC	1023972445	PRIETO SILVA NICOL																		230301	30	EPS002	30	CCF24	30	14-25	30	0.522%	30	Si
74	CC	1014201989	QUIROGA PERALTA EDWIN FERNANDO																		230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
75	CC	1013618432	QUIROGA LOZANO OSCAR FABIAN																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
76	CC	1032486411	RINCON HILARION EDWARD MAURICIO																		231001	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
77	CC	1033792754	RODRIGUEZ SOTO DANIEL ANDRES																		25-14	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
78	CC	52505417	ROJAS PEÑA NILSA YAMILE																		25-14	30	MIN001	30	CCF24	30	14-25	30	0.522%	30	Si
79	CC	1030697447	ROJAS PEREZ VALENTINA																		230301	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
80	CC	1030666489	SALAZAR ARCILA JOHN SEBASTIAN																		230201	30	EPS010	30	CCF24	30	14-25	30	0.522%	30	Si
81	CC	1010180437	SANCHEZ ROMERO CARLOS ANDRES																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
82	CC	1023033607	SANCLEMENTE PEÑA DIEGO ALEJANDRO																		230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
83	CC	1030539604	TAMAYO RIVERA FABIO ANDRES																		231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
84	CC	1020808701	TIBADUIZA CALDERON SEBASTIAN																		231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	No
85	CC	1032394709	TOLEDO SALAMANCA WALTER OSWALDO																		230201	30	EPS017	30	CCF24	30	14-25	30	0.522%	30	Si
86	CC	1018408876	TOVAR LOZANO JAIRO DAVID																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
87	CC	1031172873	TRUJILLO ALVAREZ VALENTINA																		231001	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
88	CC	1014279176	URBANO ARDILA SEBASTIAN																		25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
89	CC	1019136138	VANEGAS CAMARGO DIEGO ALEJANDRO																		230301	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
90	CC	80247522	VARGAS HINCAPIE CARLOS																		25-14	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
91	CC	1075280531	VARGAS POLANIA JAIRO ALEXANDER																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	No
92	CC	1000178261	VELANDIA CHITIVA LIZETT YAMILE																		231001	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si

PLANILLA SIN PAGAR

93	CC	1014197302	VELASQUEZ RAMOS JOHAN SEBASTIAN																		25-14	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	Si
94	CC	8770446	VELEZ CASTRO HUMBERTO DE JESUS																		230201	30	EPS008	30	CCF24	30	14-25	30	0.522%	30	No
95	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)																															
96	CC	1019024746	MUÑOZ OROZCO BERTHA JUDITH													X					25-14	2	EPS017	2	CCF24	2	14-25	2	0.000%	2	Si
97	CC	1019024746	MUÑOZ OROZCO BERTHA JUDITH																		25-14	28	EPS017	28	CCF24	28	14-25	28	1.044%	28	Si
Centro de Trabajo: MENSAJERIA (3 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (3 Afiliados)																															
98	CC	79214078	PENAGOS CIFUENTES JIMMY ALEXIS																		230201	30	EPS008	30	CCF24	30	14-25	30	4.350%	30	Si
99	CC	79840394	RODRIGUEZ ANGARITA ELKIN																		230301	30	EPS008	30	CCF24	30	14-25	30	4.350%	30	Si
100	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	Días	Codigo	Dias	Codigo	Dias	Codigo	Dias	Tarifa	Dias	Exonerado SENA e ICBF
SUCURSAL: FAMISANAR (1 Afiliados)																															
Centro de Trabajo: FAMISANAR - ADMINISTRATIVO (1 Afiliados)																															
Ciudad: BOGOTA Depto: BOGOTA D.E. (1 Afiliados)																															
101	CC	80155666	CHAVES MARTINEZ JORGE ANDRES																		230201	30	EPS005	30	CCF24	30	14-25	30	0.522%	30	Si
Total		**Afiliados(97)**																													

PLANILLA SIN PAGAR

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
2024-01	2024-02		9462991562	E	2024/02/19			0	

RESUMEN DE PAGO

RIESGO	CODIGO	NIT	DV	AFILIADOS	VALOR LIQUIDADO	INTERESES MORA	SALDOS E INCAPACIDADES	VALOR A PAGAR
AFP (ADMINISTRADORAS: 5)				92	$72,795,000	$0	$0	$72,795,000
COLFONDOS	231001	800,227,940	6	12	$12,159,600	$0	$0	$12,159,600
COLPENSIONES	25-14	900,336,004	7	14	$13,294,300	$0	$0	$13,294,300
PORVENIR	230301	800,224,808	8	35	$19,702,500	$0	$0	$19,702,500
PROTECCION	230201	800,229,739	0	30	$25,496,600	$0	$0	$25,496,600
SKANDIA	230901	800,253,055	2	1	$2,142,000	$0	$0	$2,142,000
ARL (ADMINISTRADORAS: 1)				96	$3,764,800	$0	$0	$3,764,800
COLMENA	14-25	800,226,175	3	96	$3,764,800	$0	$0	$3,764,800
CCF (ADMINISTRADORAS: 1)				94	$19,444,700	$0	$0	$19,444,700
COMPENSAR	CCF24	860,066,942	7	94	$19,444,700	$0	$0	$19,444,700
EPS (ADMINISTRADORAS: 10)				97	$34,578,900	$0	$0	$34,578,900
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	$94,000	$0	$0	$94,000
COMPENSAR	EPS008	860,066,942	7	19	$5,556,300	$0	$0	$5,556,300
EPS SURA (ANTES SUSALUD)	EPS010	800,088,702	2	5	$684,500	$0	$0	$684,500
FAMISANAR	EPS017	830,003,564	7	12	$1,530,100	$0	$0	$1,530,100
FOSYGA	MIN001	901,037,916	1	7	$3,239,000	$0	$0	$3,239,000
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	5	$662,000	$0	$0	$662,000
SALUD TOTAL	EPS002	800,130,907	4	9	$1,162,600	$0	$0	$1,162,600
SANITAS	EPS005	800,251,440	6	36	$19,701,400	$0	$0	$19,701,400
ICBF (ADMINISTRADORAS: 1)				12	$5,165,200	$0	$0	$5,165,200
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR	PAICBF	899,999,239	2	12	$5,165,200	$0	$0	$5,165,200
SENA (ADMINISTRADORAS: 1)				12	$3,443,600	$0	$0	$3,443,600
SENA	PASENA	899,999,034	1	12	$3,443,600	$0	$0	$3,443,600
TOTAL				97	$139,192,200	$0	$0	$139,192,200

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)*	-	36.774.600 COP	Enviado a la Entidad Estatal	Detalle
Pago 002	FE-3	5 días de tiempo transcurrido *(16/02/2024 10:29:00(UTC-05:00) Bogotá, Lima, Quito)*	-	103.720.380 COP	Enviado a la Entidad Estatal	Detalle

Crear

Documentos de ejecución del contrato

Descripción	Nombre del archivo	Cargado por

No existen resultados que cumplan con los criterios de búsqueda especificados

Borrar Cargar nuevo

Cancelar

< Evaluación de la Entidad Estatal >