

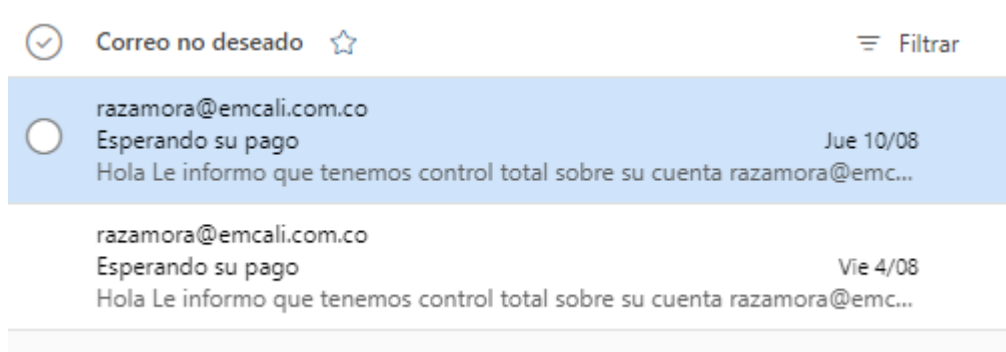
## Manual para reportar Correo malicioso en ambientes Web

- Objetivo

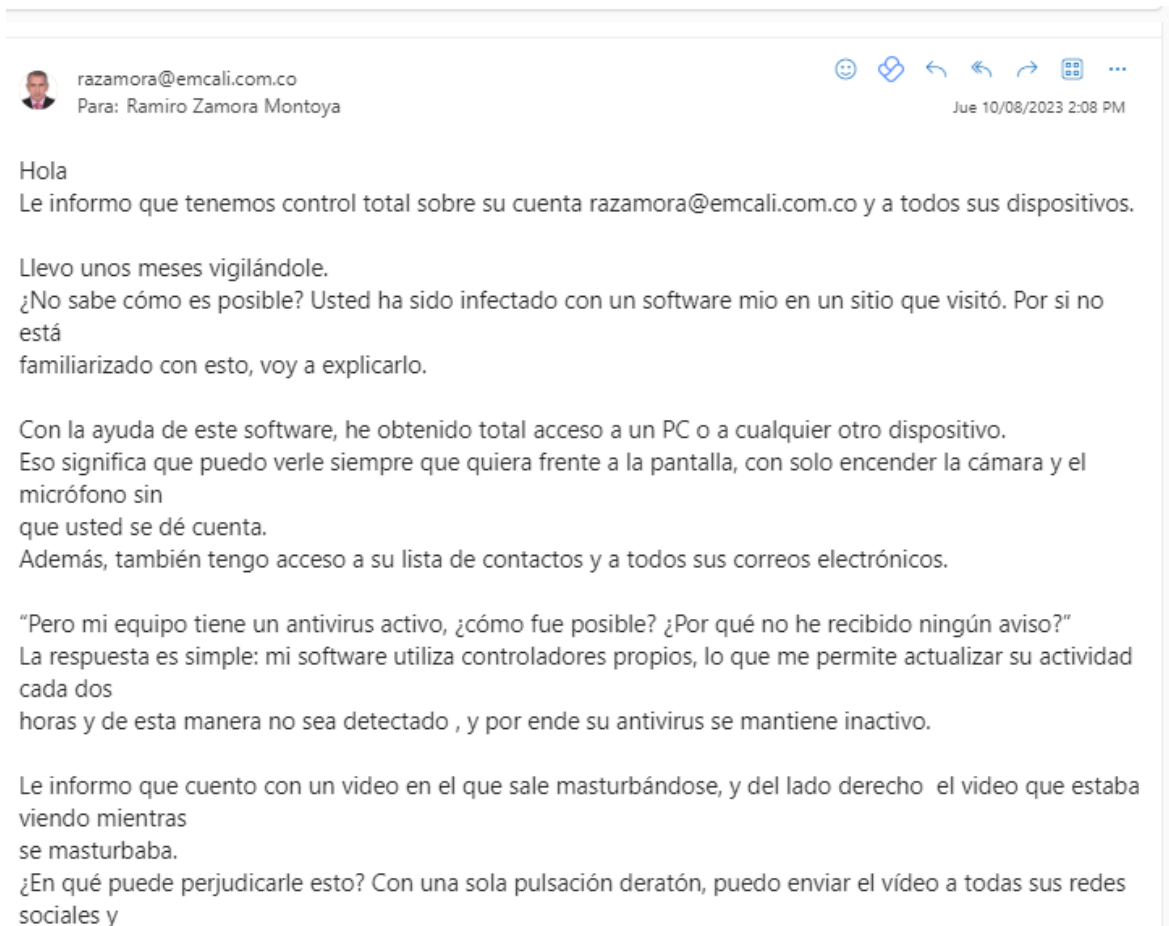
Suministrar el paso a paso necesario para la recepción y reporte de incidentes vinculados con correos maliciosos en ambientes Web.

a. **Toma de evidencia:**

1. Tomar captura de los correos maliciosos.



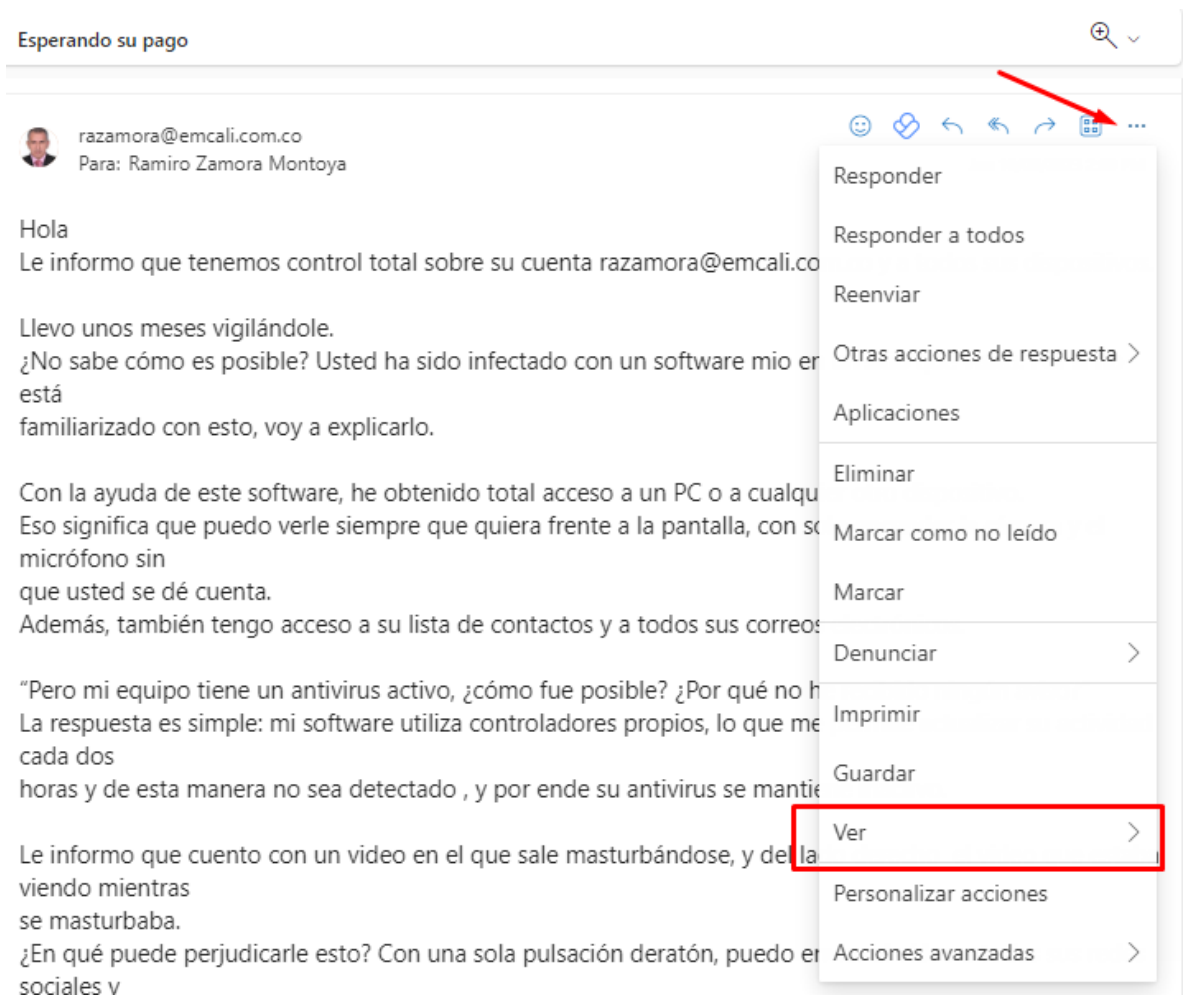
## 2. Tomar captura del cuerpo del mensaje del correo maliciosos



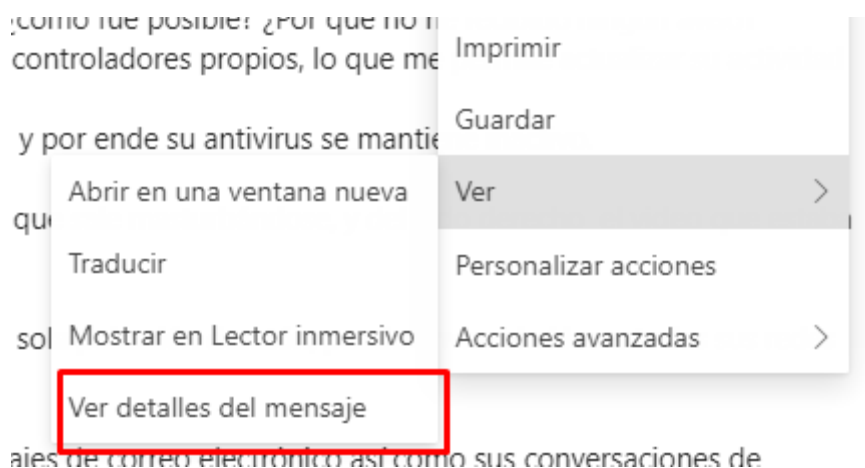
### b. Detalles de mensaje

Extraer la trazabilidad del correo de la siguiente manera:

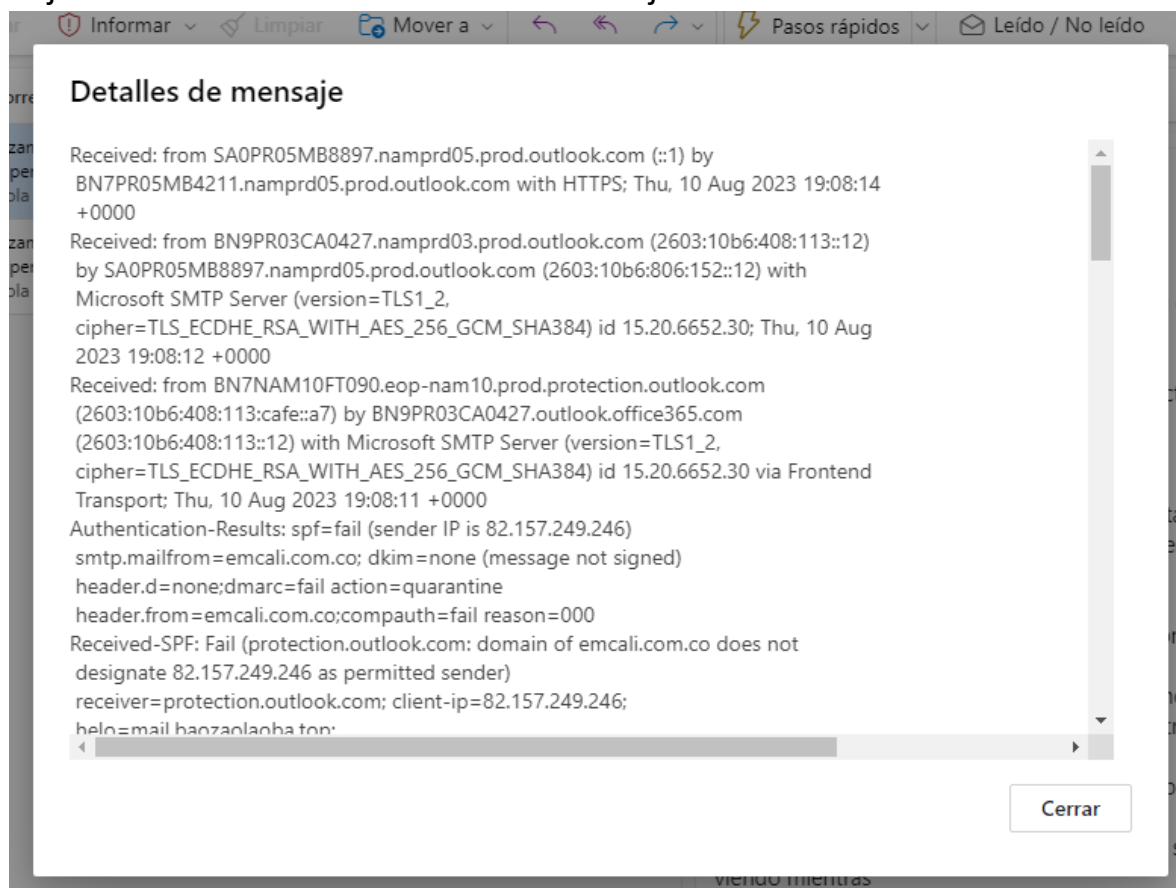
1. Clic en opciones del mensaje y seleccionar la opción ver.



## 2. Clic en VER DETALLES DEL MENSAJE.



3. Posteriormente, desplegará una lista, copiar todo el contenido y adjuntar en un archivo Word donde se alojará la evidencia.



Received: from SA0PR05MB8897.namprd05.prod.outlook.com (::1) by BN7PR05MB4211.namprd05.prod.outlook.com with HTTPS; Thu, 10 Aug 2023 19:08:14 +0000

Received: from BN9PR03CA0427.namprd03.prod.outlook.com (2603:10b6:408:113::12) by SA0PR05MB8897.namprd05.prod.outlook.com (2603:10b6:806:152::12) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6652.30; Thu, 10 Aug 2023 19:08:12 +0000

Received: from BN7NAM10FT090.eop-nam10.prod.protection.outlook.com (2603:10b6:408:113:cafe::a7) by BN9PR03CA0427.outlook.office365.com (2603:10b6:408:113::12) with Microsoft SMTP Server (version=TLS1\_2, cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6652.30 via Frontend Transport; Thu, 10 Aug 2023 19:08:11 +0000

Authentication-Results: spf=fail (sender IP is 82.157.249.246) smtp.mailfrom=emcali.com.co; dkim=none (message not signed) header.d=none;dmarc=fail action=quarantine header.from=emcali.com.co;compauth=fail reason=000

Received-SPF: Fail (protection.outlook.com: domain of emcali.com.co does not designate 82.157.249.246 as permitted sender)

receiver=protection.outlook.com; client-ip=82.157.249.246;  
helo=mail.baozaolaoba.top;  
Received: from mail.baozaolaoba.top (82.157.249.246) by  
BN7NAM10FT090.mail.protection.outlook.com (10.13.156.162) with Microsoft SMTP  
Server id 15.20.6678.19 via Frontend Transport; Thu, 10 Aug 2023 19:08:11  
+0000  
Received: from [192.141.244.133] (unknown [192.141.244.133])  
by mail.baozaolaoba.top (Postfix) with ESMTP id A42AE1C9926  
for <razamora@emcali.com.co>; Tue, 1 Aug 2023 19:14:23 +0800 (CST)  
From: razamora@emcali.com.co  
To: razamora@emcali.com.co  
Subject: Esperando su pago  
Date: 1 Aug 2023 05:14:22 -0600  
Message-ID: <20230801051422.744FD04A4F6DFFEB@emcali.com.co>  
MIME-Version: 1.0  
Content-Type: text/plain;  
charset="utf-8"  
Content-Transfer-Encoding: quoted-printable  
Return-Path: razamora@emcali.com.co  
X-MS-Exchange-Organization-ExpirationStartTime: 10 Aug 2023 19:08:11.5814  
(UTC)  
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit  
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000  
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit  
X-MS-Exchange-Organization-Network-Message-Id:  
078a7bd7-82a0-41dc-d719-08db99d52419  
X-EOPAttributedMessage: 0  
X-EOPTenantAttributedMessage: 76320c82-2ebf-4b6e-8e5c-df0e21d196c8:0  
X-MS-Exchange-Organization-MessageDirectionality: Incoming  
X-MS-PublicTrafficType: Email  
X-MS-TrafficTypeDiagnostic:  
BN7NAM10FT090:EE\_|SA0PR05MB8897:EE\_|BN7PR05MB4211:EE\_  
X-MS-Exchange-Organization-AuthSource:  
BN7NAM10FT090.eop-nam10.prod.protection.outlook.com  
X-MS-Exchange-Organization-AuthAs: Anonymous  
X-MS-Office365-Filtering-Correlation-Id: 078a7bd7-82a0-41dc-d719-08db99d52419  
X-MS-Exchange-AuthSource: SA|SL  
X-MS-Exchange-Organization-SCL: 9  
X-Forefront-Antispam-Report:  
  
CIP:82.157.249.246;CTRY:CN;LANG:es;SCL:9;SRV:;IPV:NLI;SFV:SPM;H:mail.baozaolaoba.top;PTR:In  
foDomainNonexistent;CAT:HSPM;SFS;DIR:INB;  
X-Microsoft-Antispam: BCL:0;  
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 10 Aug 2023 19:08:11.0189  
(UTC)  
X-MS-Exchange-CrossTenant-Network-Message-Id: 078a7bd7-82a0-41dc-d719-08db99d52419

X-MS-Exchange-CrossTenant-Id: 76320c82-2ebf-4b6e-8e5c-df0e21d196c8  
X-MS-Exchange-CrossTenant-AuthSource:  
BN7NAM10FT090.eop-nam10.prod.protection.outlook.com  
X-MS-Exchange-CrossTenant-AuthAs: Anonymous  
X-MS-Exchange-CrossTenant-FromEntityHeader: Internet  
X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA0PR05MB8897  
X-MS-Exchange-Transport-EndToEndLatency: 00:00:03.2947612  
X-MS-Exchange-Processed-By-BccFoldering: 15.20.6652.029  
X-Microsoft-Antispam-Mailbox-Delivery:  
ucf:0;jmr:0;auth:0;dest:J;OFR:SpamFilterAuthJ;ENG:(910001)(944506478)(944626604)(920  
097)(930097)(3100021)(140003);RF:JunkEmail;  
X-Microsoft-Antispam-Message-Info:  
=?us-  
ascii?Q?bGFaQetrasVRrPydNpDytMqdQpOFInbbf8b0uZ8hjmojeTZxMxqR5hdJaa9O?=  
=?us-ascii?Q?BIEXyOnl7ybNneDs3ZkPUS2NIGrkRapgPcqHa5JKzZJuny6O0Ck5EYD9/mK?=  
=?us-ascii?Q?1MaAO9U092/ZzXTHgLG4pNiigeviuJFRoiY0uBdFZ36QEwcRiqWLOktCV4xj?=  
=?us-ascii?Q?a4FvvrXWdGiSkj6NbeQnRLggnN6PGI3N4Lqb+0r1iMDSmPcRzVK4J+7/5ui?=  
=?us-ascii?Q?HAWntyDRapLsx+Ec9S85XGrDkX8nQvmZIUio1BqK98HmqSdd9CcH9V0PzYtL?=  
=?us-ascii?Q?vp+xlAMplHU4sBd+1VLc09ifevcLW9DzeXogZ9qXfsTgv1rXbz+c3V3hClrk?=  
=?us-  
ascii?Q?Z4DHEaCgHe7VxXTnBRdWZ8ZsCptPmR8SowewNfreljwTnVb7KWJhmYaQH3P+?=  
=?us-ascii?Q?RBs1JROhHkXpVZ58Y8Yv2hN/03l8XUGnDJlICD+0lN/0wBUw0g1TrjrW2bRA?=  
=?us-ascii?Q?4H0mCnzlcCGhEDCri/4QPRcfkAdFIB2Exysl1wVUXwn1iLgCkjynKZ/HwJ2m?=  
=?us-ascii?Q?HLSJ9XQOUiQcNyksZQMLNybaUNJzvdjXUhZ6o59vRLyG4Mz+zN27UTnVyMi?=  
=?us-ascii?Q?rYq2K110FJFE+j7cObopJuNVqnmaLbks/WxiuoHukdhvA8ZvwjTb1729cvlK?=  
=?us-ascii?Q?b3ipf/R0qEV69rgcxhA77k/ln0FJwy8jnDPD2Bp6QhHfV28slZESJmF6oYk?=  
=?us-ascii?Q?evRQ2agrgQYBHy71zhsD8f6aH1TDfC66eywVxWXjHFjXPYVL/2RyKyWGWWI2?=  
=?us-ascii?Q?5heiHjpn/3pt3yixBk9ver6hGoOi14Hqoz4ltHDxk+hzNbnZ9zDh+iLzRESh?=  
=?us-ascii?Q?LMlBt5Viyj3+913HVbjoSfpB3ETJWPYeEQlyujbOAFx4cDv597jkoWUGdsLA?=  
=?us-ascii?Q?+ORELiQaluKLrKCwm73VUds79AGGi9nUD36cYQSfDRfpUxWdCgYjJlJQfCZL?=  
=?us-ascii?Q?CBoX1ZDwHV5bO6xbSJx9CpNiPzf37cMjdmKjW2gU/NAtHg8hXEJISBBV5Nom?=  
=?us-ascii?Q?IJTS6CogGF/FobPsCDToosPZTVkQzq1Oam9hx9d98fkiy+7quGh+jCWyAjau?=  
=?us-  
ascii?Q?NIOWGEmTBmt6wKD30+e1ucB27QuRhHjd00sFhqZgVQlUn3pYvn2YvqWAYFx+?=  
=?us-ascii?Q?+QCYEV1ARDhPnxH9hOLFJ+CbaRUHufRofwylG5FEBI0/ZtU1IFy75c8CNFYs?=  
=?us-ascii?Q?Az8w0FuP3PXijChzZ2fC7zyip6OxnH3syB8y7q8HJGw8T5k3NNNMV+ZFvxhZ?=  
=?us-ascii?Q?zvfkGokpUmxwdFrYp6irWw9apoulbG3QloAMgIK/e41GeJsMlquCYroVwcmN?=  
=?us-ascii?Q?cwCE000KYF1H/t9bX3jChleus2ai4/krVI2M8PuzahyzXFMTqu3WCqJX21pb?=  
=?us-ascii?Q?9jyKuNW0Usr4WCKNjglvjK//ZmZmuCRDTPKOS6s4jek5mjWXIsAWxLadX60Z?=  
=?us-ascii?Q?q49CPHvhJHTNHT2Xd151rbG+papF2JVj7D/AytMSVKi/NkZ59hoMSzyxBNka?=  
=?us-ascii?Q?YnADU0he/8QYRjndqhQodCKZRys29yqRbxBzVARcmY1XYbBXdxmrUeuryHR0?=  
=?us-ascii?Q?hAvUobfe2+ak4tmrlc+Y+UfBmI54xlCWxJ0t+2ZHTsfB1ModpXKerR3cKZOs?=  
=?us-ascii?Q?7FdDVHBeE+WfV63ZXh9od2O8aw7xgeMj5QkgUzfa15fLZJkhXamZj5LH50Ed?=  
=?us-ascii?Q?wMA/yahvgJwwUH52X7G1lr67fYeyZQyLL17gGCQONS8Y6wGHm/dxP5anpDjA?=  
=?us-ascii?Q?MU/90lx/O5KWpqEHg17HNdizupEaD1HvssVjr7qv0s+yy0a0KIDRFLZTMxd6?=  
=?us-ascii?Q?ib4RNU24hpk7/ILkCslwHWppcDneE4485iPH62aJf6eykxBXvAjNc+ITAZ?=

=?us-ascii?Q?1n3mJTTbM+gvu34fUUZgwHmAe81ZDPCb5JPex6KdI0iDvw/hBJmL2G4eP3e+?=

=?us-ascii?Q?jy0uLVt8dgh4PQjulrzuWxkEUeHDb2v+gBUuymHI4I/bVgxHYRXaGAtUtrE?=

=?us-ascii?Q?kP4YAMM+r1KD6QTkqbKZUU2SqBlhkka/ff1wx4GQlkW7DHePFGkNXJBO1za?=

=?us-ascii?Q?+h+LlLgO41Z7ul+hz4XjSd9Jr3gsGjRqeOlgidM0WcOIInFUjZqSHt1QCo+J?=

=?us-ascii?Q?NsnDq1Z1KrxyxqjO5cNmX9Jlp0R2Otv3lN/nAGGchIEus9eV3xN1c01+Y2H0?=

=?us-ascii?Q?B4G/rbhwIAXuPXdJap/FBlzJbiKwK3Ek2j31hQ5Cj4K9/Wo0bpliTSyvTUM7?=

=?us-ascii?Q?KwHvJbl9R9hL0qXlzhJgvilsGteHDqpKcT2CRnxB9GisSh1H9dt/+zYxmawA?=

=?us-ascii?Q?FEj0f0lnKHgqXg66hZylXY1JXCP2uXOb3CMz+0KMtrVxrsbSqKoxikRnptfk?=

=?us-ascii?Q?RZ25UywiPYMbmHG5sIlMv36XUJsLDZ76uqdrEweHFcQeBl/aa50v+DkWyhBs?=

=?us-ascii?Q?uTlnfmy4BlUEG3ncvRMDrHf/3MyHD+8zMVjF/rJoo+YDKYiPJ33dO8YlZbo8?=

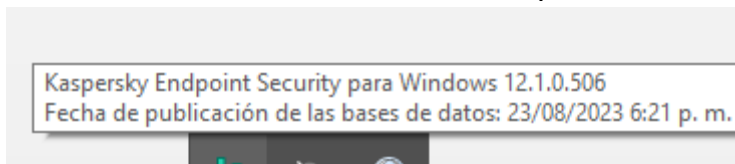
=?us-ascii?Q?LVQQ60ChXcwn/wtftx7okaP/tADIWFa7Vk01TNCr81SgmrP7JN6m0B8FP/RD?=

=?us-ascii?Q?hCrsgWEI8v8trMZr2YSHr6nwYFihXSEm2RFazBgT2MKTMMyA4xAjZxJv2Wfib?=

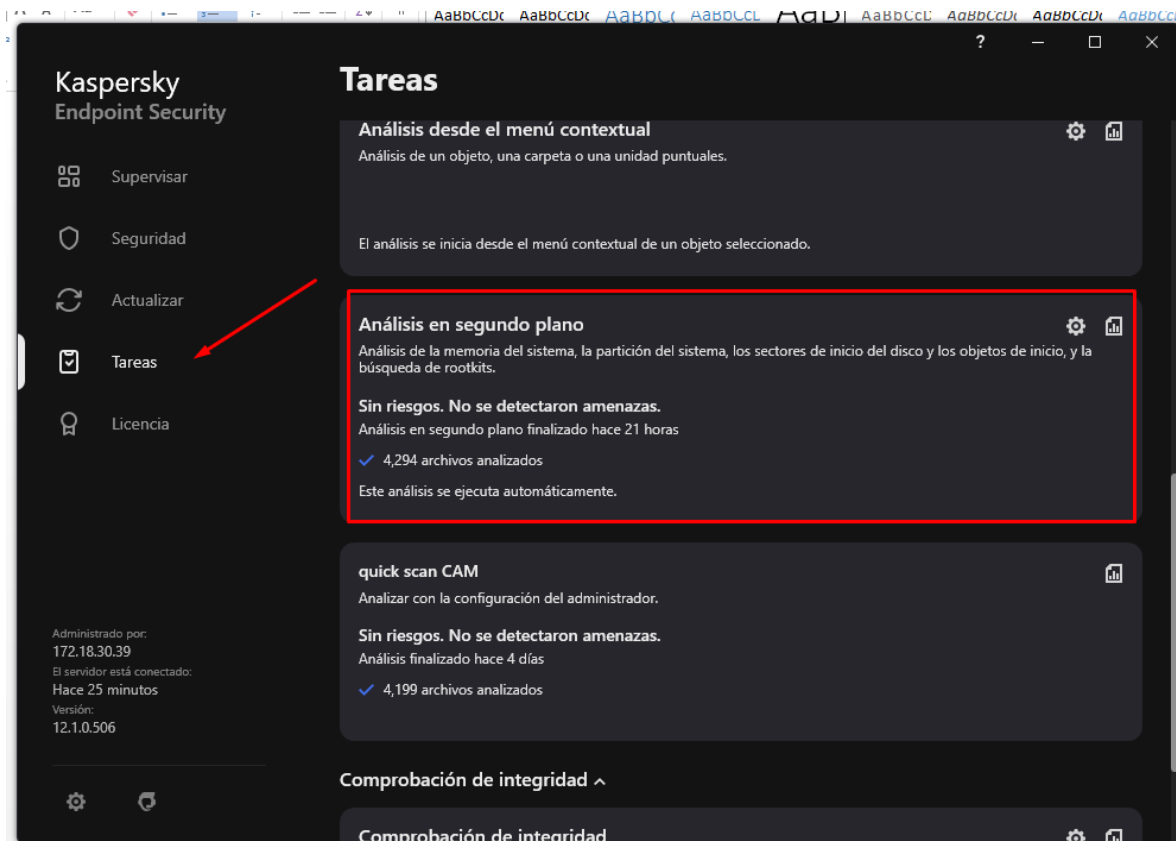
=?us-ascii?Q?RA5GPcmX5ZrkXT8TEpphllIDIN6vEYAz4+yBKFbpzOX?=-

### **C. Análisis del antivirus en el equipo**

1. En el equipo del usuario, validar que la versión de la base de datos este actualizada al día presente.



2. Revisar en el área de tareas del antivirus que se haya realizado el análisis de segundo plano completamente.



3. Tomar los datos del equipo con el siguiente código en CMD.

```
C:\Users\almurillo>ipconfig /all

Configuración IP de Windows

Nombre de host. . . . . : CCGTMS03
Sufijo DNS principal . . . . : emcali.com.co
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: emcali.com.co
```



4. Tomar captura unificada con los datos del análisis y los datos del equipo.

## Tareas

El análisis se ejecuta desde el menú contextual de un objeto seleccionado.

### Análisis en segundo plano


Análisis de la memoria del sistema, la partición del sistema, los sectores de arranque del disco y los objetos de inicio, además de la búsqueda de rootkit.

**Seguro: no se han detectado amenazas.**

Análisis en segundo plano completado hace 16 minutos

✓ 2.497 archivos analizados.

El análisis se ejecuta automáticamente.



Administrador: C:\Windows\system32\cmd.exe

```
Configuración IP de Windows

Nombre de host. . . . . : BOU01GENRAZAMOR
Sufijo DNS principal . . . . : emcali.com.co
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: emcali.com.co

Adaptador de Ethernet Conexión de área local:

Sufijo DNS específico para la conexión. . : emcali.com.co
```

5. Enviar el archivo de evidencia en Word con toda la información al área de **servidores** para que bloqueen el dominio remitente del mensaje malicioso.