Solución E5 Seguridad Office 365

Inteligencia Artificial

Identity & Access Management

Threat Protection

Information Protection

Security Management

GOBIERNO DE LA REPÚBLICA DOMINICANA

INVI

INSTITUTO NACIONAL DE LA VIVIENDA

Microsoft

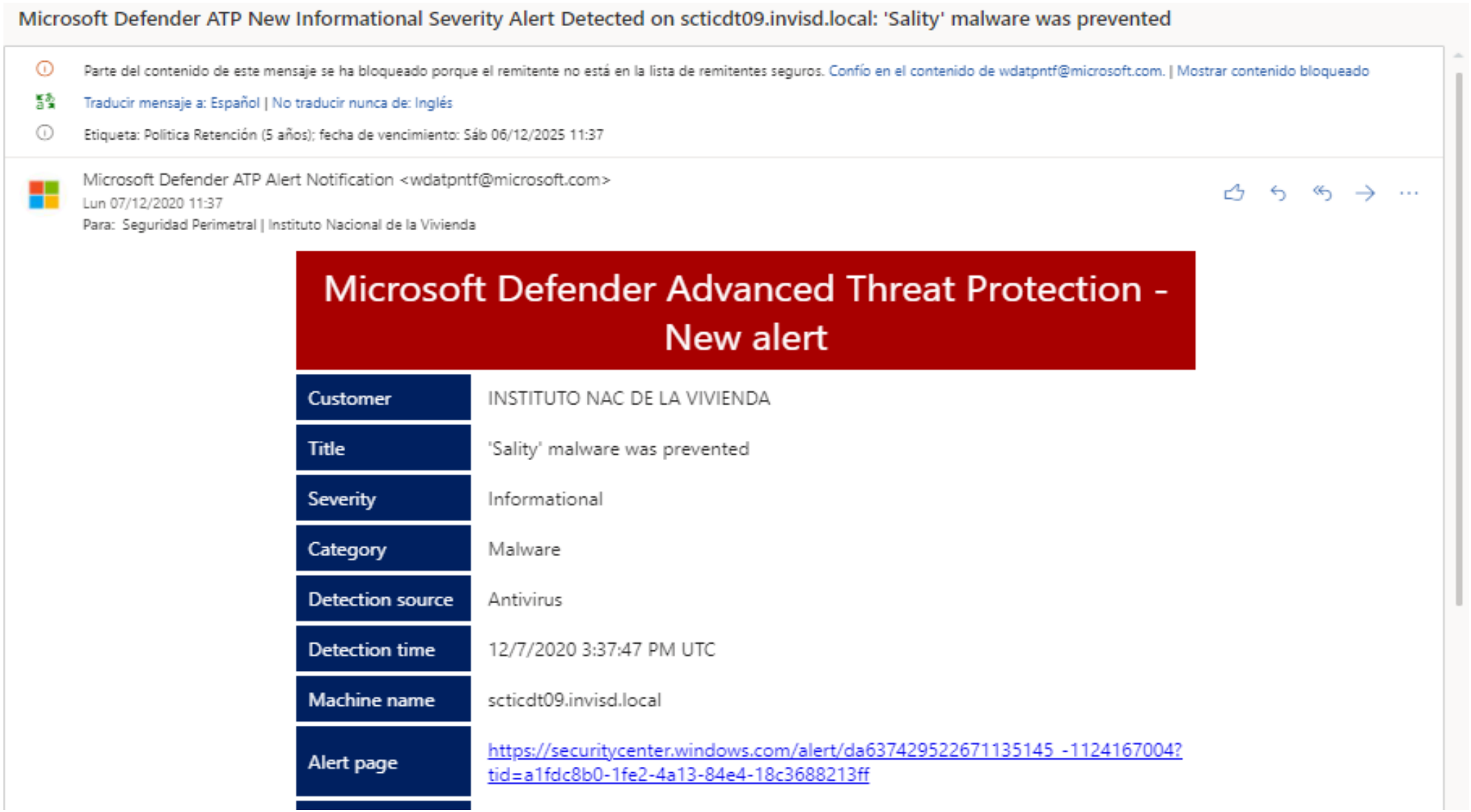
GOBIERNO DE LA
REPÚBLICA DOMINICANA

INVI

INSTITUTO NACIONAL
DE LA VIVIENDA

Alertas por actividad

Alerta de riesgo en equipo local



Microsoft Defender ATP New Informational Severity Alert Detected on scticdt09.invisd.local: 'Sality' malware was prevented

Parte del contenido de este mensaje se ha bloqueado porque el remitente no está en la lista de remitentes seguros. Confío en el contenido de wdatpntf@microsoft.com. | Mostrar contenido bloqueado

Traducir mensaje a: Español | No traducir nunca de: Inglés

Etiqueta: Política Retención (5 años); fecha de vencimiento: Sáb 06/12/2025 11:37

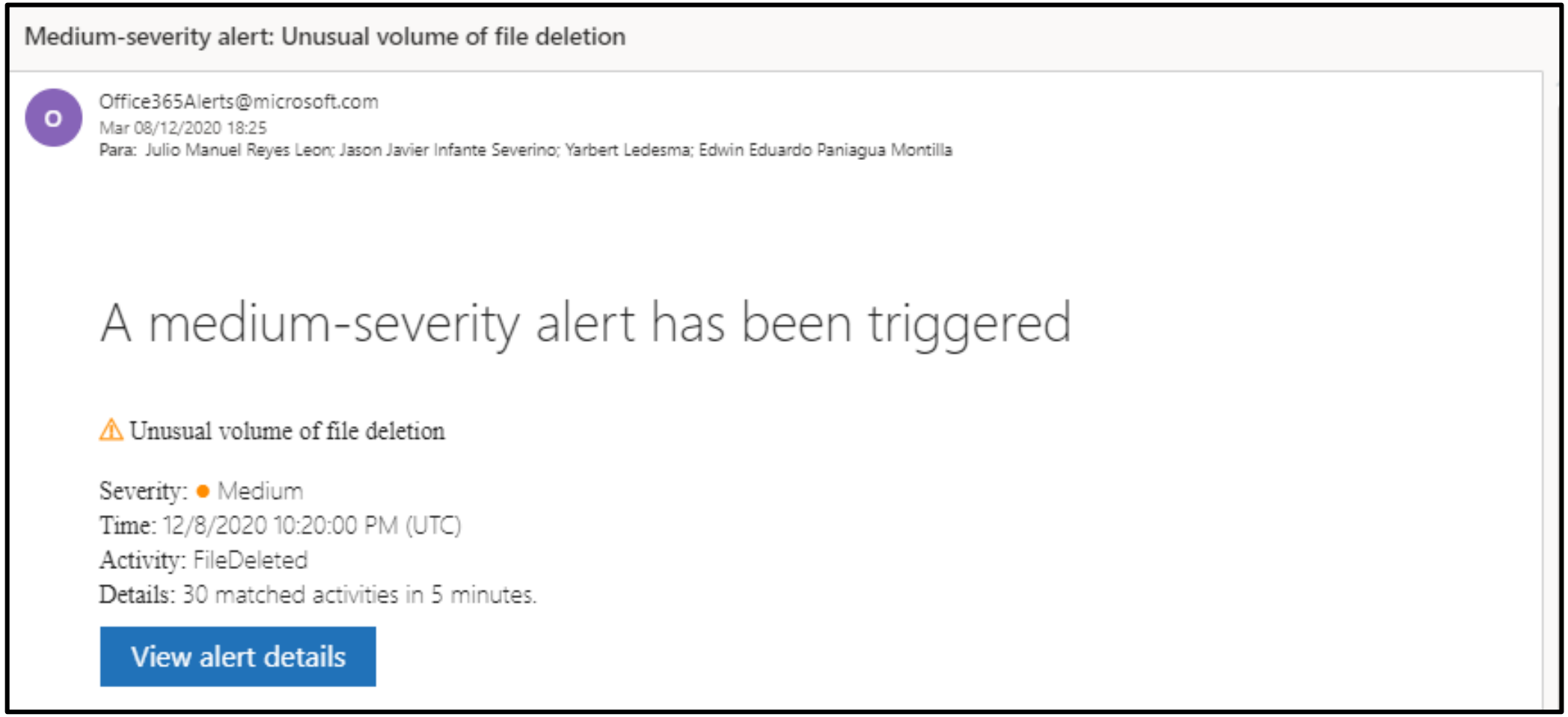
Microsoft Defender ATP Alert Notification <wdatpntf@microsoft.com>
Lun 07/12/2020 11:37
Para: Seguridad Perimetral | Instituto Nacional de la Vivienda

Microsoft Defender Advanced Threat Protection - New alert

Customer	INSTITUTO NAC DE LA VIVIENDA
Title	'Sality' malware was prevented
Severity	Informational
Category	Malware
Detection source	Antivirus
Detection time	12/7/2020 3:37:47 PM UTC
Machine name	scticdt09.invisd.local
Alert page	https://securitycenter.windows.com/alert/da637429522671135145 -1124167004?tid=a1fdc8b0-1fe2-4a13-84e4-18c3688213ff

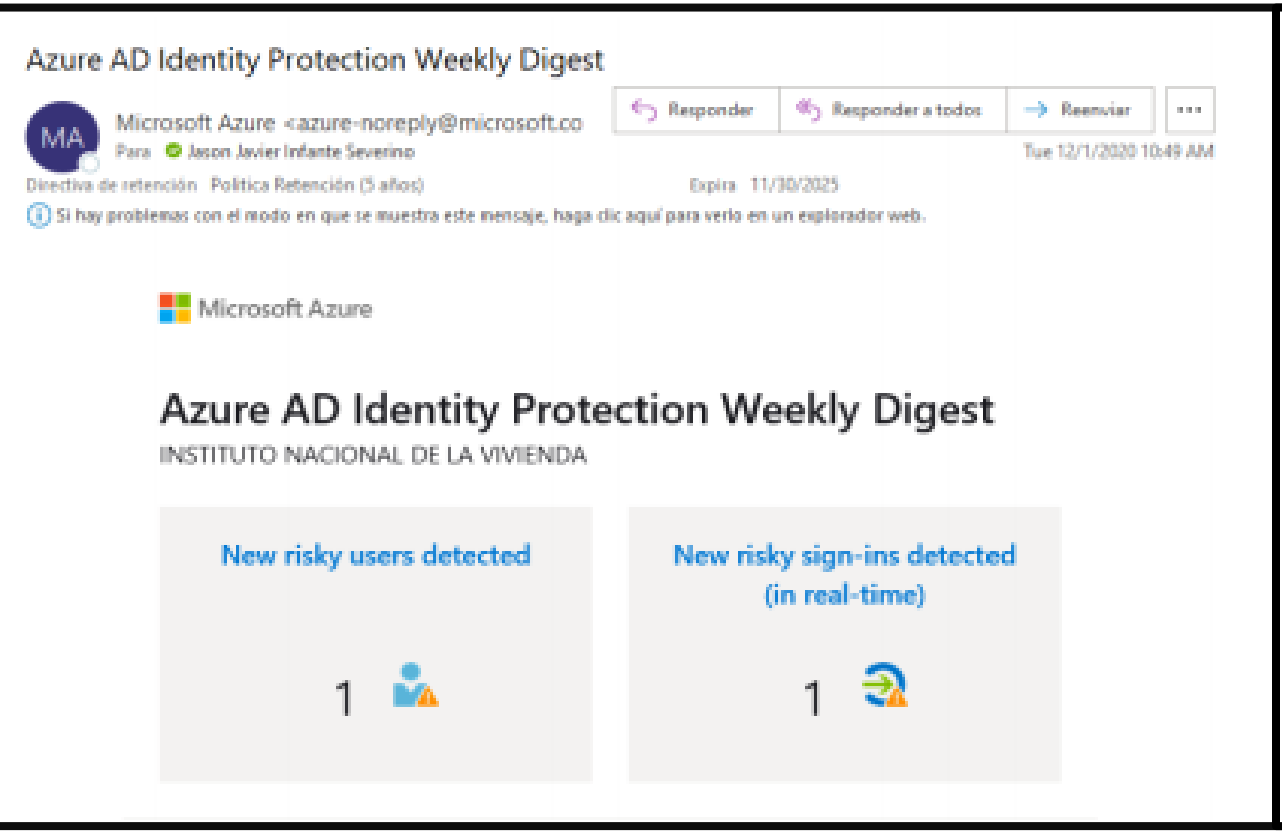
Evento-1

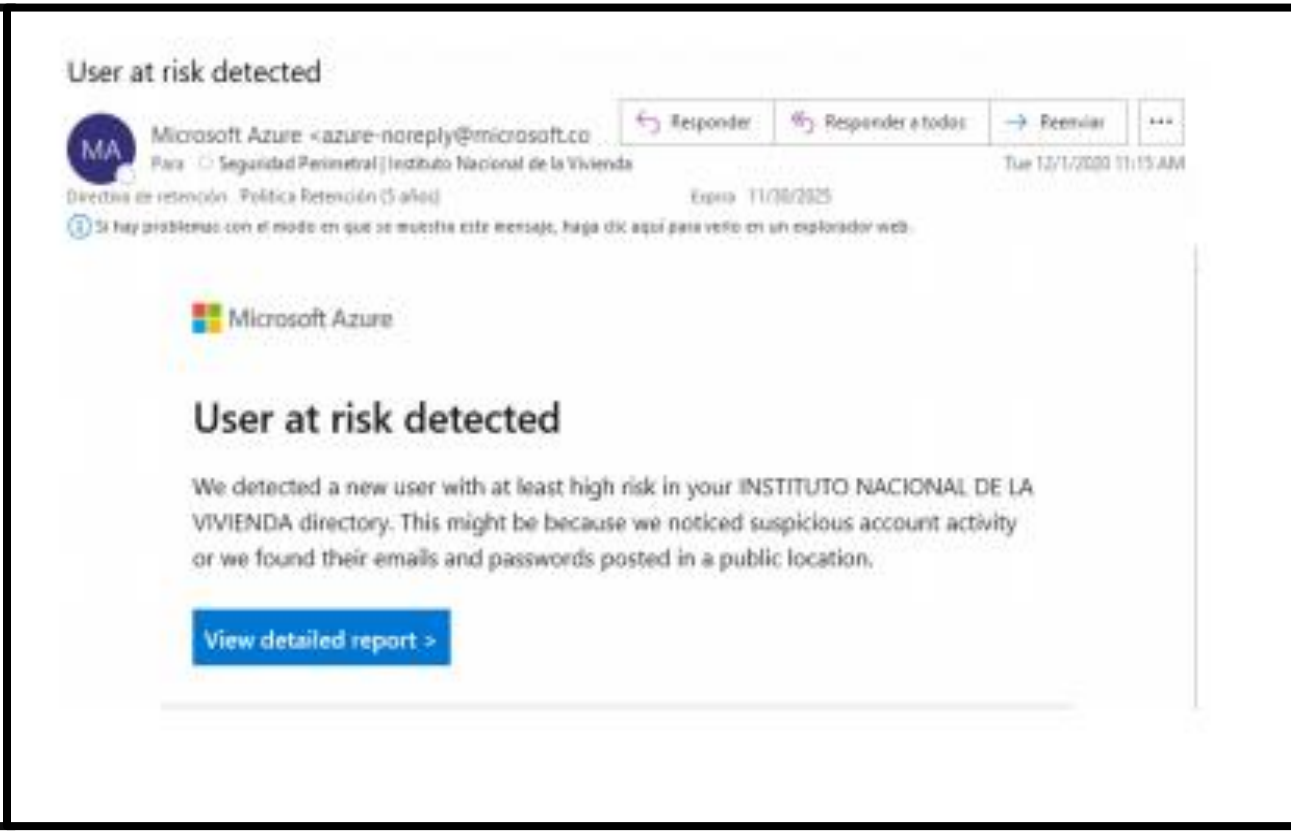
Alerta de riesgo almacenamiento en la nube



Evento-2

Alerta de riesgo de identidad





Evento-3

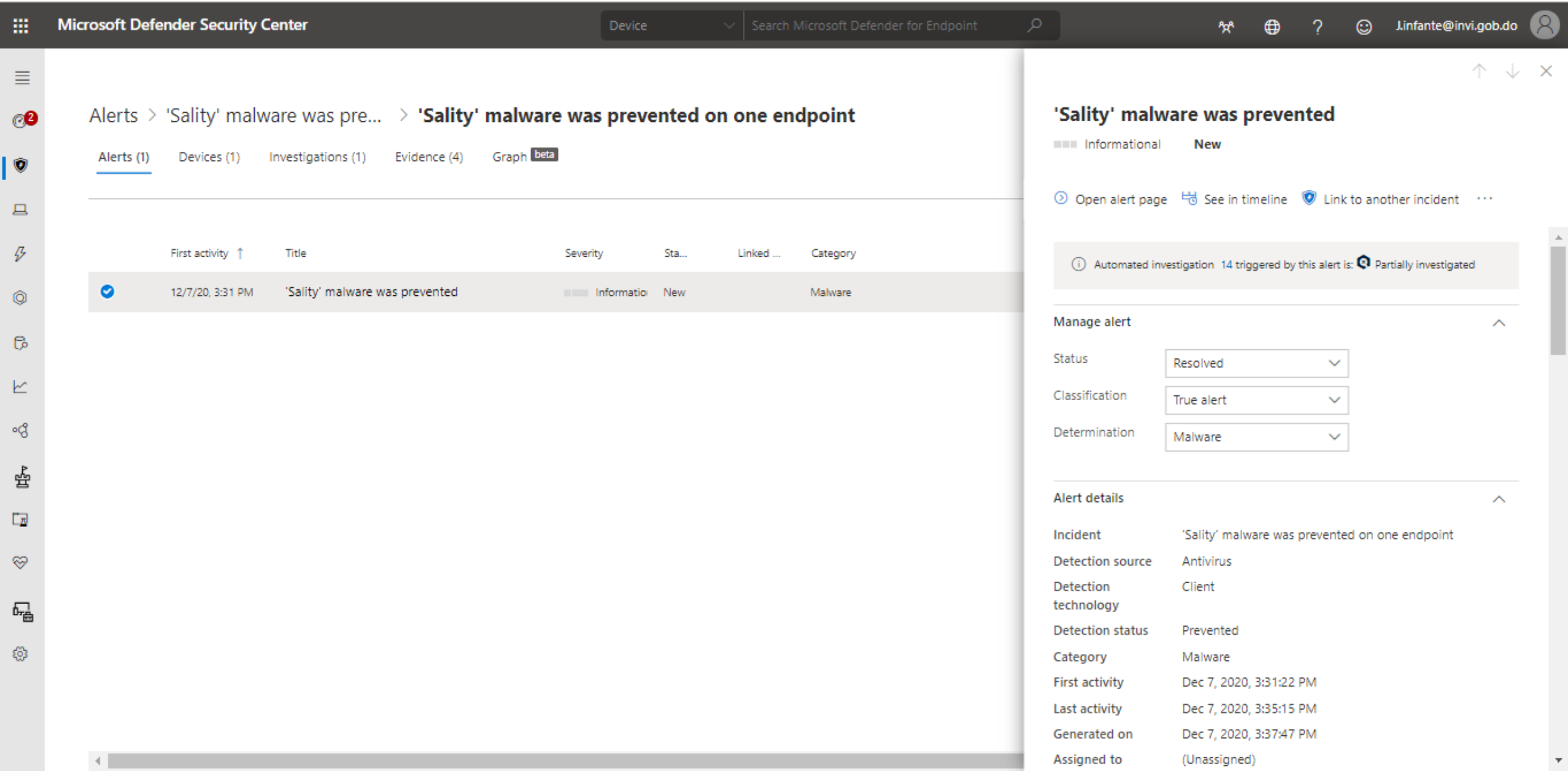
GOBIERNO DE LA
REPÚBLICA DOMINICANA

INVI

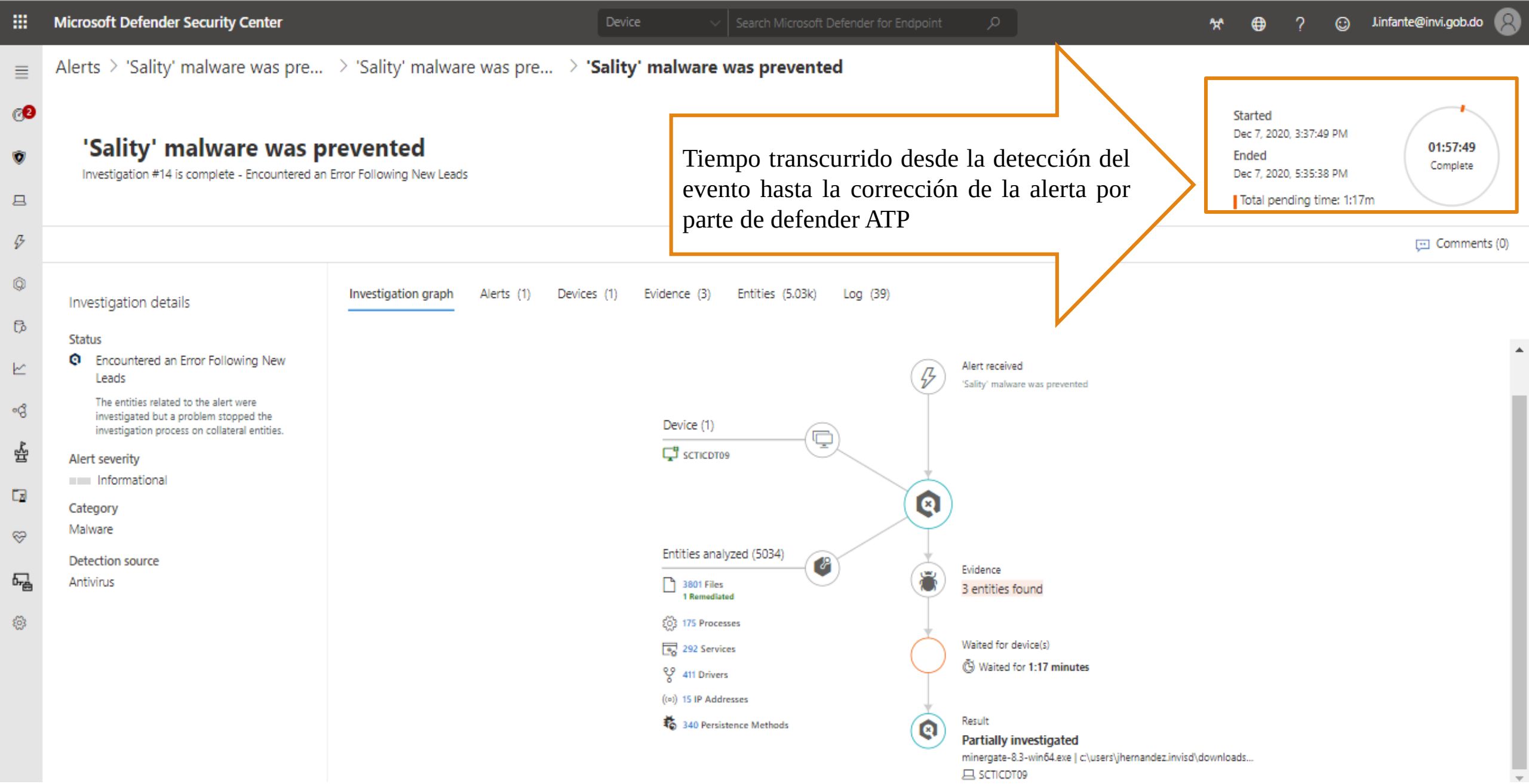
INSTITUTO NACIONAL
DE LA VIVIENDA

Auto investigación y corrección de los eventos de seguridad

EVENTO - 1



Descripción del evento



Registros de investigación y corrección del evento

'Sality' malware was prevented

Investigation #14 is complete - Encountered an Error Following New Leads

Started
Dec 7, 2020, 3:37:49 PM
Ended
Dec 7, 2020, 5:35:38 PM
Total pending time: 1:17m

01:57:49
Complete

Comments (0)

Investigation details

Status
Encountered an Error Following New Leads

The entities related to the alert were investigated but a problem stopped the investigation process on collateral entities.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Devices (1) | **Evidence (3)** | Entities (5.03k) | Log (39)

The following suspicious entities were investigated. The verdict for each is listed in the table below.

Type	Status	Device	Path	Impacted entity	Action	Detection type	Detection source
File	Unknown	SCTICDT09.INVISD.LOCAL	g:system volume information.exe	system volume information.exe		Alert	'Sality' malware was prevented
File	Not found	SCTICDT09.INVISD.LOCAL	g:\system volume information.exe	system volume information.exe		Alert	'Sality' malware was prevented
File	Remediated	SCTICDT09.INVISD.LOCAL	c:\users\jhernandez.invisd\downloads\minerga	minergate-8.3-win64.exe	The file was quarantined	Investigation	Get downloaded executable files

Evidencias encontradas

'Sality' malware was prevented

Investigation #14 is complete - Encountered an Error Following New Leads

Started
Dec 7, 2020, 3:37:49 PM
Ended
Dec 7, 2020, 5:35:38 PM
Total pending time: 1:17m

01:57:49
Complete

Comments (0)

Investigation details

Status
Encountered an Error Following New Leads

The entities related to the alert were investigated but a problem stopped the investigation process on collateral entities.

Alert severity
Informational

Category
Malware

Detection source
Antivirus

Investigation graph | Alerts (1) | Devices (1) | Evidence (3) | Entities (5.03k) | Log (39)

Evidence summary (5,034)

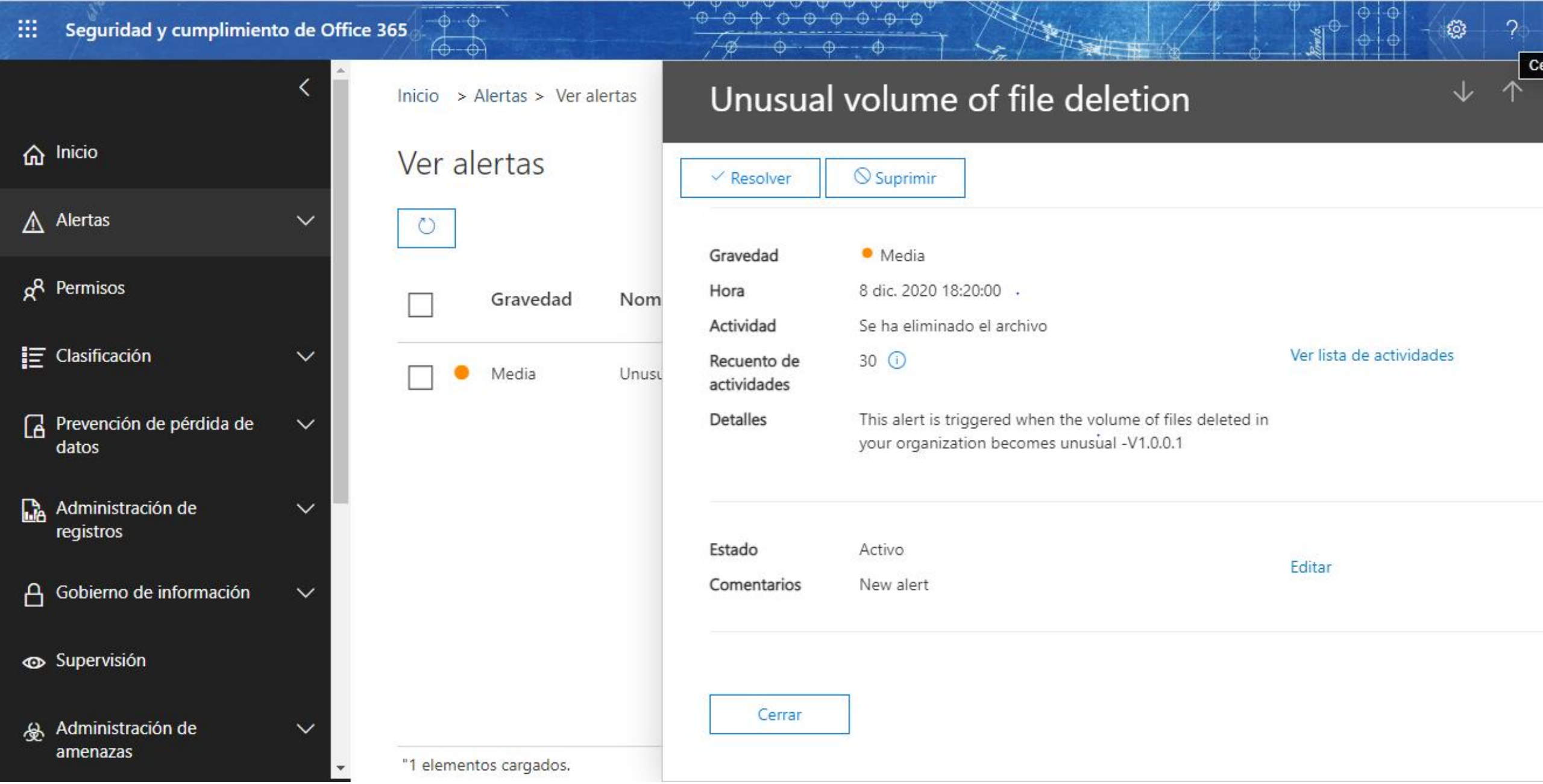
- Files (3,801)
- Processes (175)
- Services (292)
- Drivers (411)
- IP Addresses (15)
- Persistence Methods (340)

All evidence (5,034)

Entity type	Total	Remediated	Malicious	Suspicious	Verified	No threats found	Unknown	Not found	Unremediated
Files	3801	1	-	-	-	3,688	102	10	-
Processes	175	-	-	-	-	165	10	-	-
Services	292	-	-	-	-	292	-	-	-
Drivers	411	-	-	-	-	408	3	-	-
IP Addresses	15	-	-	-	-	3	12	-	-
Persistence Methods	340	-	-	-	-	204	136	-	-

Entidades investigadas y corregidas por parte de Defender ATP

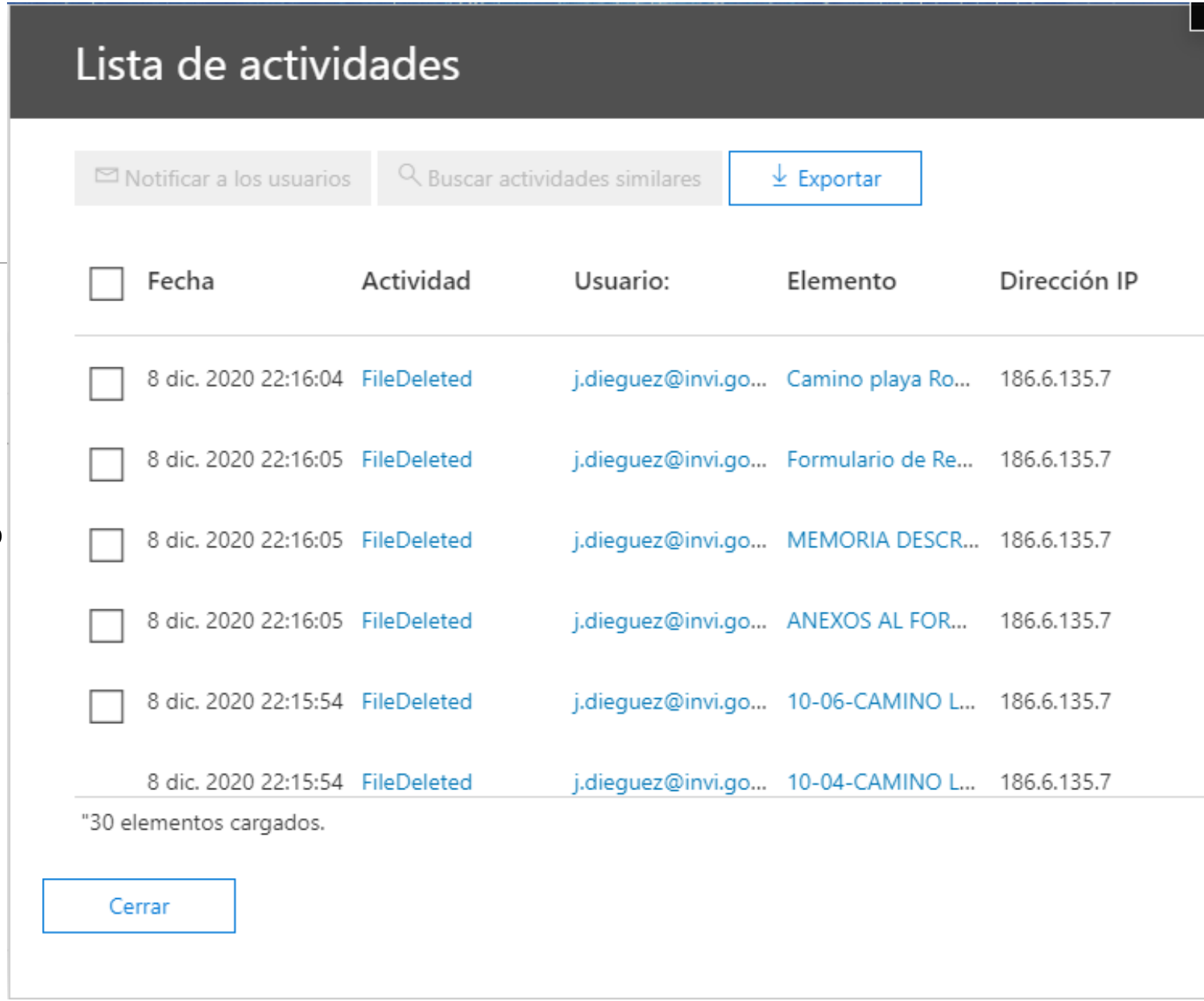
EVENTO - 2



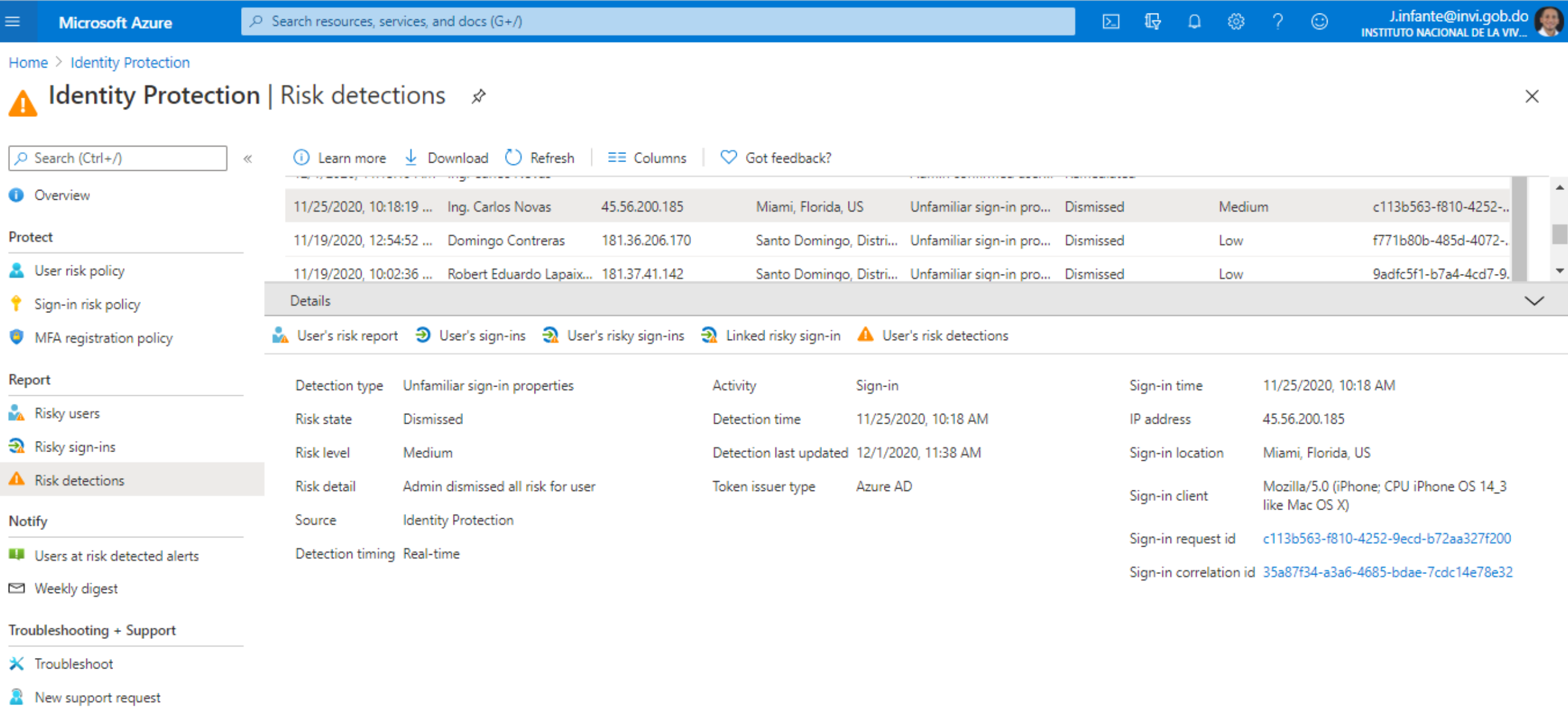
Evento inusual de eliminación de archivos

Listado de actividad, describe:

el usuario, tipo y nombre del archivo eliminado, tiempo exacto de eliminación y la localización en donde office 365 envía los documentos para su almacenamiento provisional, hasta confirmar si el evento fue malicioso o no.



EVENTO - 3



Usuario Bloqueado: Debido al comportamiento inusual en el login del usuario este fue bloqueado.

Descripción del evento

Identificación de la solicitud	Tiempo de detección
fdbed23201d5d55e466f976ec109098d7	Tiempo real
Identificador de correlación	**Actividad**
35a87f34-a3a6-4685-bdae-7cdc14e78e32	Inicio de sesión
Tipo de detección	**Activity time**
Propiedades de inicio de sesión desconocidos	2020-11-25T14:18:19.5945919Z
Estado de riesgo	**Detection time**
Confirmado comprometido	2020-11-25T14:18:19.5945919Z
Nivel de riesgo	**Detection last updated**
Medio	2020-12-01T15:18:07.6390818Z
Detalle de riesgo	**User object ID**
El administrador confirmó el inicio de sesión comprometido	2b0b5a32-a296-4247-9e4f-33c10e49a65e
Fuente	**Usuario**
Protección de la identidad	Ing. Carlos Novas
UPN	**IP address**
Cnovas@invi.gob.do	45.56.200.185
Location	Miami - Florida - US

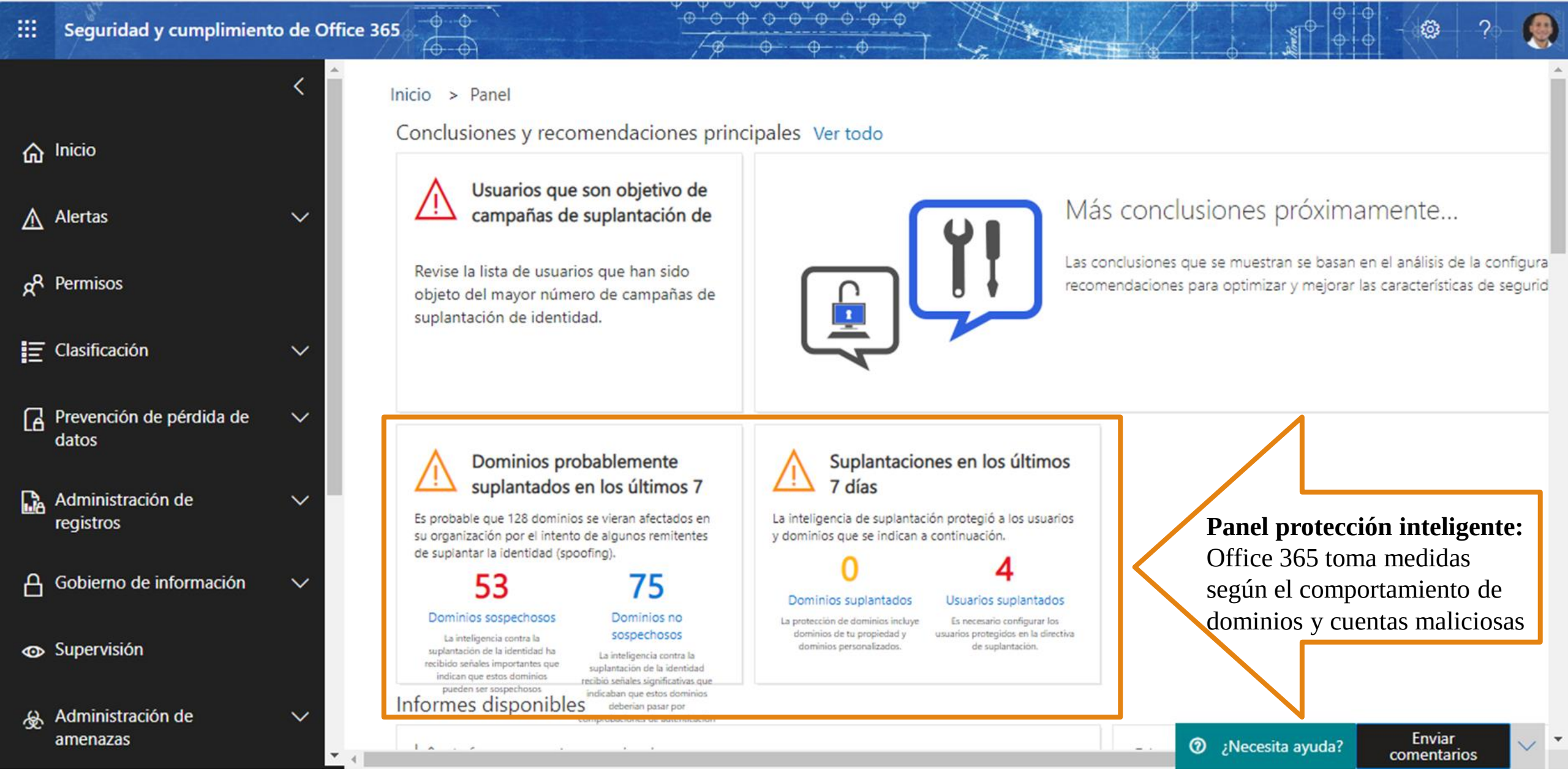
Nota: El caso fue evaluado. Según verificamos con el Sr. Carlos Nova, el mismo nos comunico que estaba utilizando un cliente VPN en su equipo móvil, en donde tiene registrada la cuenta de la institución. Le comunicamos que este tipo de acción hace que la cuenta se bloquee.

GOBIERNO DE LA
REPÚBLICA DOMINICANA

INVI

INSTITUTO NACIONAL
DE LA VIVIENDA

Protección de correos



Panel protección inteligente: Office 365 toma medidas según el comportamiento de dominios y cuentas maliciosas

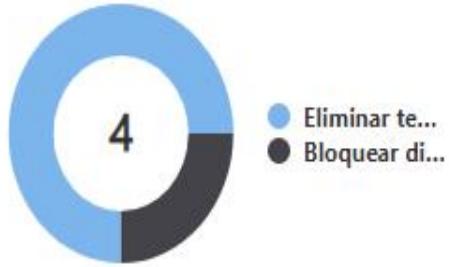
Inicio
Alertas
Permisos
Clasificación
Prevención de pérdida de datos
Administración de registros
Gobierno de información
Supervisión
Administración de amenazas

Resumen de investigaciones

No hay datos disponibles

Ahorro de eficiencia diaria

Acciones pendientes



Principa

Cebo purg

Cómo hemos protegido su organización frente a las amenazas en los últimos 7 días

Configurar archivos adjuntos seguros

Configurar protección para SPO, ODB y Teams

para la protección contra malware de día cero

Protección contra amenazas avanzadas de malware de día cero en mensajes de correo electrónico y archivos de SharePoint, OneDrive y

13

mensajes detectados de phishing avanzada

Protección contra amenazas avanzadas de suplantación de identidad y phishing de objetivo definido

Configurar vínculos seguros

para la protección en el momento del clic

Vínculos maliciosos bloqueados en mensajes entrantes y en el ámbito de su organización mediante la protección en el momento del clic de Vínculos seguros

Esta

Informe de protección de ...

Detecciones de amenazas globales semanales

Ten

¿Necesita ayuda?

Enviar comentarios

Seguridad y cumplimiento de Office 365

Inicio
Alertas
Permisos
Clasificación
Prevención de pérdida de datos
Administración de registros
Gobierno de información
Supervisión
Administración de amenazas
Flujo de correo
Privacidad de los datos
Buscar

Inicio > Explorador

Explorador es una herramienta eficaz y casi en tiempo real para ayudar a los equipos de operaciones de seguridad a investigar y responder a amenazas en el Centro de seguridad y cumplimiento. Obtenga más información sobre Explorador.

Ver Suplantar identidad

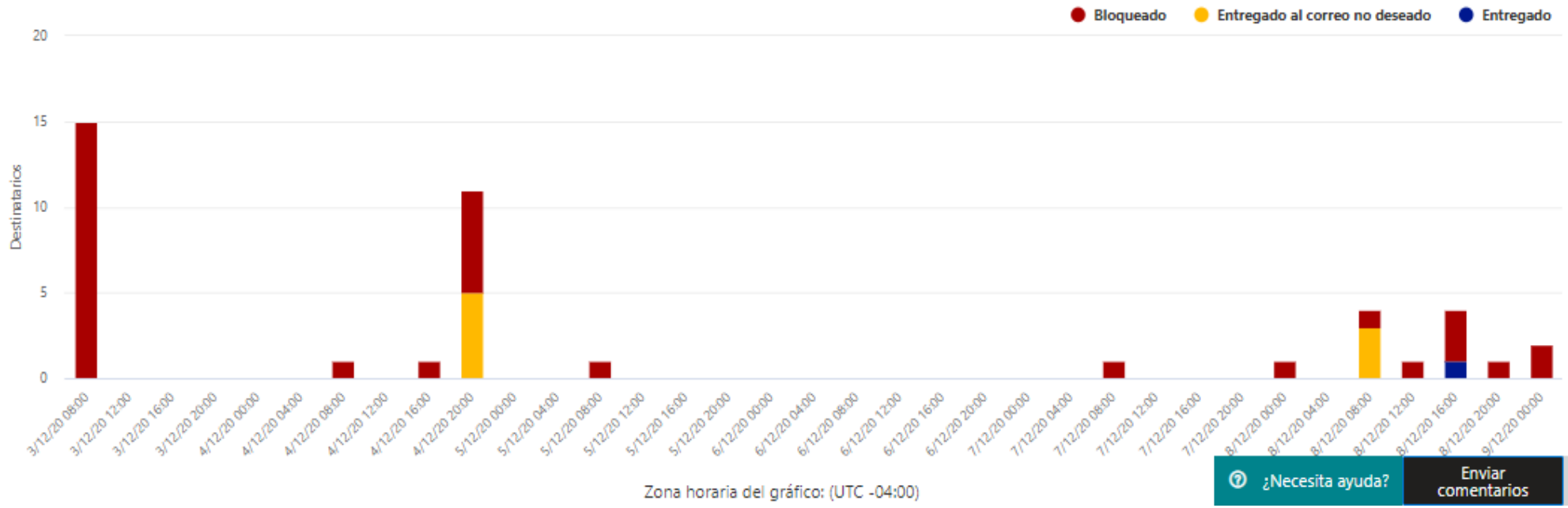
Esta vista muestra información sobre los mensajes de correo electrónico identificados como mensajes con amenazas de phishing. También puede tener una vista de las direcciones URL y los clics en las direcciones URL dentro de los correos electrónicos. Esta vista muestra características, como filtros útiles para la búsqueda de amenazas en mensajes de correo electrónico, así como capacidad para exportar hasta 9.990 registros para su análisis sin conexión. Mostrar más

Guardar consulta | Guardar consulta como | Configuración de la consulta guardada | Exportar

Remitente | Utilice comas (,) para separar varias entradas. Haga clic en Acti | Actualizar | Filtro avanzado

2020-12-03 00:00 — 2020-12-09 23:30

Acción de entrega



Zona horaria del gráfico: (UTC -04:00)

¿Necesita ayuda? | Enviar comentarios

Medidas automáticas contra Phishing

Inicio
Alertas
Permisos
Clasificación
Prevención de pérdida de datos
Administración de registros
Gobierno de información
Supervisión
Administración de amenazas
Flujo de correo
Privacidad de los datos
Buscar

Zona horaria del gráfico: (UTC -04:00)

Mensaje de correo electrónico | Clics en la dirección URL | Direcciones URL | Principales usuarios de destino | Origen de correo electrónico | Campaña

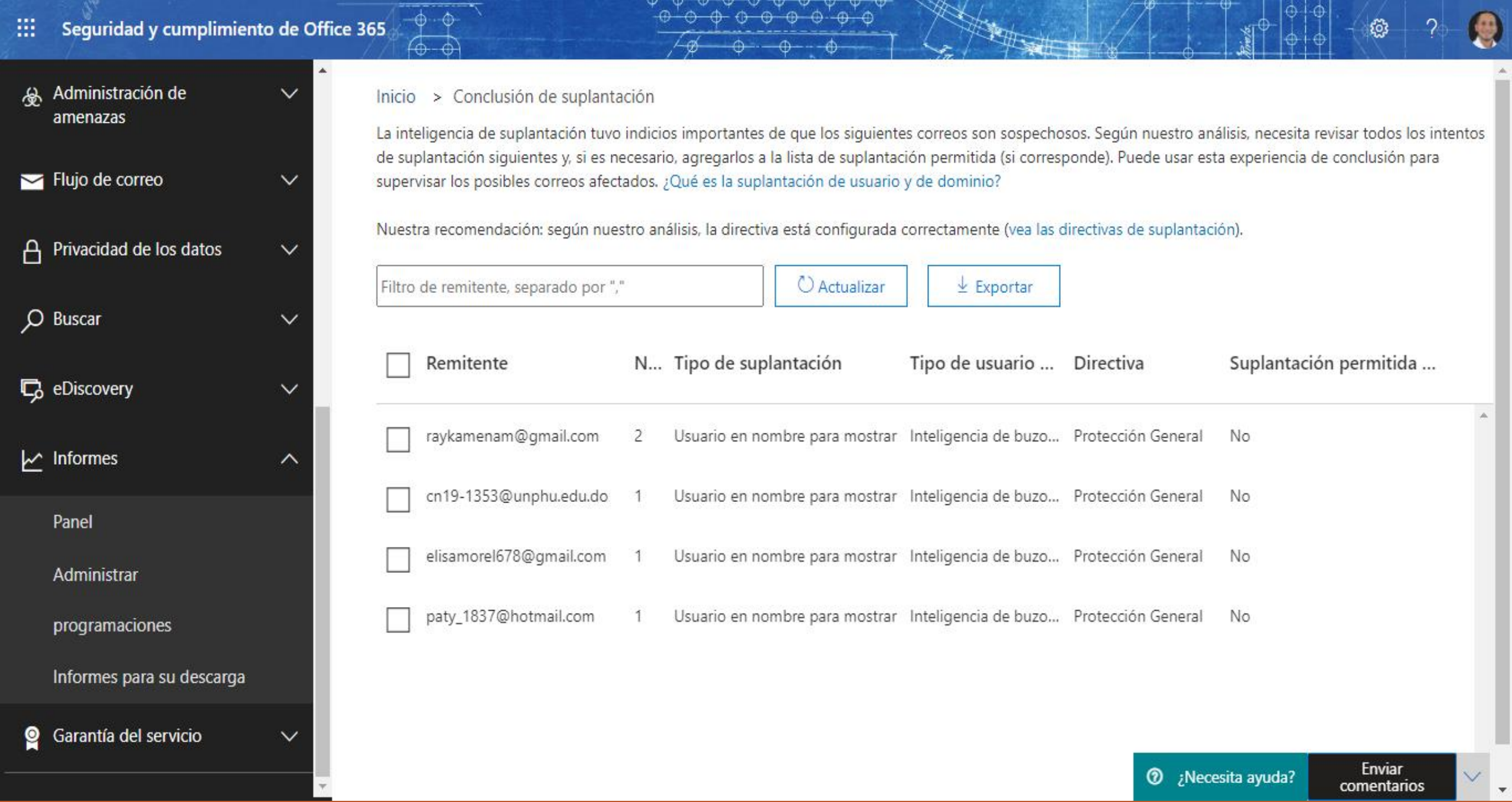
+ Acciones

Opciones de columna

Fecha (UTC -04:00) ...	Asunto	Destinatario	Etiquet...	Remitente	A...	Última ubicación de ...	Ubicación de entrega...
9/12/20 02:12	invi_rd Paid Sponsorship	j.reyes@invi.gob.do	-	influenceenhance@gmail.com	-	Cuarentena	Cuarentena
9/12/20 02:12	invi_rd Paid Sponsorship	j.hernandez@invi.gob.do	-	influenceenhance@gmail.com	-	Depositado	Depositado
8/12/20 20:33	Cuenta APAPenLine@ Restringida	transparencia@invi.gob.do	-	servicioalcliente@apap.com.do	-	Cuarentena	Cuarentena
8/12/20 19:28	1 new voice caller on 08 Decemb...	k.garcia@invi.gob.do	-	frecom@frecom.com	-	Cuarentena	Cuarentena

43 elemento(s) de 43 cargados

¿Necesita ayuda? Enviar comentarios



Medidas contra la suplantación de correos

Inicio
Alertas
Permisos
Clasificación
Prevención de pérdida de datos
Administración de registros
Gobierno de información
Supervisión
Administración de amenazas

La inteligencia contra la suplantación de identidad recibió señales importantes que indican que estos dominios pueden ser sospechosos. Revise cada par de dominios para encontrar falsos positivos y agréguelos a la Lista de permitidos si es necesario. Para obtener una lista completa de los pares de dominios protegidos por la inteligencia contra la suplantación de identidad, use el cmdlet Get-PhishFilterPolicy. Obtenga más información sobre la inteligencia contra la suplantación de identidad.

Filter spoofed domain, separated by ','

Filter infrastructure, separated by ','

Exportar

Filtrar

Dominio con identidad ...	Infraestructura	Número de mens...	Última visualizaci...	Tipo de suplanta...	Suplantación de
hotmail.com	constantcontact.com	16	3/12/2020	Externo	No
minurvi-lac.org	mailjet.com	12	3/12/2020	Externo	No
gmail.com	ymlpsvr.com	10	3/12/2020	Externo	No
eximediard.com	mandrillapp.com	9	3/12/2020	Externo	No
gmail.com	constantcontact.com	9	1/12/2020	Externo	No
wecraft.info	secureserver.net	7	5/12/2020	Externo	No

"53 elementos cargados

¿Necesita ayuda?

Enviar comentarios

GOBIERNO DE LA
REPÚBLICA DOMINICANA

INVI