

Guía de la mejor práctica para el Anti-Spam, el contra virus, Graymail y los filtros del brote

Contenido

[Overview](#)

[Anti-Spam](#)

[Verifique las teclas de función](#)

[Habilite la Multi-exploración inteligente \(IMS\) global](#)

[Habilite la cuarentena centralizada del Spam](#)

[Configure el Anti-Spam en las directivas](#)

[Contra virus](#)

[Verifique las teclas de función](#)

[Habilite la exploración del contra virus](#)

[Configure el contra virus en las directivas del correo](#)

[Graymail](#)

[Verifique las teclas de función](#)

[Habilite Graymail y la caja fuerte desinscribe los servicios](#)

[La configuración Graymail y la caja fuerte desinscriben en las directivas](#)

[Filtros del brote](#)

[Verifique las teclas de función](#)

[Habilite el servicio de los filtros del brote](#)

[Configure los filtros del brote en las directivas](#)

[Conclusión](#)

Información general

El amplia mayoría de las amenazas, los ataques, y las molestias hechas frente por una organización a través del correo electrónico vienen bajo la forma de Spam, malware, y ataques mezclados. El dispositivo de seguridad del email de Cisco (ESA) incluye varias diversas Tecnologías y características para cortar estas amenazas en el gateway antes de que ingresen la organización. Este documento describirá los acercamientos de la mejor práctica para configurar el Anti-Spam, el contra virus, Graymail y los filtros del brote, en el flujo entrante y saliente del correo electrónico.

Anti-Spam

La protección del Anti-Spam dirige una gama completa de amenazas sabidas incluyendo los ataques del Spam, del phishing y del zombi, así como duro-a-detecta el volumen bajo, las amenazas efímeras del correo electrónico tales como ["419" los timos](#). Además, la protección del Anti-Spam identifica las nuevas y de desarrollos amenazas mezcladas tales como ataques del Spam que distribuyen el contenido malévolo con una descarga URL o un ejecutable.

La Seguridad del correo electrónico de Cisco ofrece las soluciones siguientes del anti-Spam:

- Filtración del Anti-Spam de IronPort (IPA)
- Filtración inteligente de la Multi-exploración de Cisco (IMS)

Usted puede autorizar y habilitar ambas soluciones en su ESA pero puede utilizar solamente uno en una directiva determinada del correo. Con el fin este documento de la mejor práctica, nosotros vaya a utilizar la característica IMS.

Verifique las teclas de función

- En el ESA, navegue a la **administración del sistema** > a las **teclas de función**
- Busque la licencia inteligente de la Multi-exploración y asegúrese la es activo.

Habilite la Multi-exploración inteligente (IMS) global

- En el ESA, navegue a los **Servicios de seguridad** > al **IMS** y a **Graymail**
- Haga clic el **Enablebutton** en las **configuraciones globales IMS**:

IMS Global Settings	
Ironport Intelligent Multi-Scan:	Enabled
Regional Scanning:	Off
Edit IMS Settings	

- Busque las **configuraciones globales comunes** y el tecleo **edita las configuraciones globales**
- Aquí usted puede configurar las configuraciones múltiples. Las configuraciones recomendadas se muestran en la imagen abajo:

Edit Common Global Settings	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds

- **Cometer de Submitand** del tecleo **sus cambios**.

Si usted no tiene una suscripción de la licencia IMS:

- Navegue a los **Servicios de seguridad** > al **Anti-Spam de IronPort**
- Haga clic el **Enablebutton** en la **descripción del Anti-Spam de IronPort**
- El tecleo **edita las configuraciones globales**
- Aquí usted puede configurar las configuraciones múltiples. Las configuraciones recomendadas se muestran en la imagen abajo:

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> Enable IronPort Anti-Spam Scanning	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="2M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</p> <p>Never scan messages larger than <input type="text" value="3M"/> Maximum Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> Aggressive Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</p> <p><input type="radio"/> Regional (China)</p>

- Cisco recomienda el seleccionar del perfil **agresivo de la** exploración para un cliente que desee un énfasis fuerte en el bloqueo del Spam.
- Cometer de Submitand del tecleo sus cambios

Cuarentena centralizada permiso del Spam

Puesto que el Anti-Spam tiene la opción que se enviará para quarantine, es importante asegurarse de que la cuarentena del Spam está configurada:

- Navegue a los **Servicios de seguridad** > a la **cuarentena del Spam**
- Hacer clic el **Configure** button le llevará a la página siguiente.
- Aquí usted puede habilitar la cuarentena marcando el **enable** box y señalar la cuarentena que se centralizará en un dispositivo de SecurityManagement (S A) byfilling en el **IP address** SMANAMEAND. Las configuraciones recomendadas se muestran abajo:

External Spam Quarantine Settings	
<input checked="" type="checkbox"/> Enable External Spam Quarantine	
Name:	<input type="text" value="centralized_spam"/> (e.g. spam_quarantine)
IP Address:	<input type="text" value="sma_ip_address"/>
Port:	<input type="text" value="6025"/>
Safelist/Blocklist:	<input checked="" type="checkbox"/> Enable End User Safelist/Blocklist Feature Blocklist Action: <input type="text" value="Quarantine"/>

- Cometer de Submitand del tecleo sus cambios

Para más información sobre configurar y las cuarentenas centralizadas, refiera por favor al documento de las mejores prácticas:

[Mejores prácticas para la directiva, configuración de las cuarentenas del virus y del brote, y migración centralizadas del ESA al S A](#)

Anti-Spam de la configuración en las directivas

Una vez que la Multi-exploración inteligente se ha configurado global, usted puede ahora aplicar la Multi-exploración inteligente para enviar las directivas:

- Navegue **para enviar las directivas** > las **directivas del correo entrante**
- Las directivas del correo entrante utilizan las configuraciones del Anti-Spam de IronPort por abandono.

- Hacer clic el link azul bajo el Anti-**Spam** permitirá para que esa directiva determinada utilice las configuraciones personalizadas del Anti-Spam.
- Debajo de usted verá un ejemplo que muestre la política predeterminada usando las configuraciones personalizadas del Anti-Spam:

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	IronPort Intelligent Multi-Scan Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	

Personalice las configuraciones del Anti-Spam para una directiva del correo entrante haciendo clic el link azul bajo el Anti-**Spam** para la directiva que usted desea personalizar.

Aquí usted puede seleccionar la opción de la exploración del Anti-Spam que usted desea habilitar para esta directiva.

- Con el propósito de este documento de la mejor práctica, haga clic el botón de radio al lado de la **Multi-exploración inteligente de IronPort** del uso:

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input type="radio"/> Use IronPort Anti-Spam service <input checked="" type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled

Las dos secciones siguientes incluyen las **configuraciones Positivo-identificadas del Spam** y las **configuraciones sospechosas del Spam**:

- La mejor práctica recomendada es configurar la acción de la **cuarentena** en la configuración del **Spam Positivo-Identificar** con el **[SPAM]** prepended del texto agregado al tema y;
- Aplíquese **para entregar** como la acción para las **configuraciones del Spam Suspected** con el **[SUSPECTED SPAM]** prepended del texto agregó al tema:

Positively-Identified Spam Settings	
Apply This Action to Message:	Spam Quarantine ↓ <i>Note: If local and external quarantines are defined, mail will be sent to local quarantine.</i>
Add Text to Subject:	Prepend ↓ [SPAM]
▶ Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver ↓ Send to Alternate Host (optional):
Add Text to Subject:	Prepend ↓ [SUSPECTED SPAM]
▶ Advanced	Optional settings for custom header and message delivery.

- El **establecimiento del umbral del Spam** puede ser cambiado, y las configuraciones recomendadas son personalizar la **calificación de spam Positivo-identificada a 90** y la **calificación de spam sospechosa a 43**:

Spam Thresholds	
Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input type="radio"/> Use the Default Thresholds <input checked="" type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="43"/> (minimum 25, cannot exceed positive spam score)

- Cometer de Submitand del tecleo sus cambios

Contra virus

La protección del contra virus se proporciona a través de dos motores del otro vendedor – Sophos y McAfee. Estos motores filtrarán todas las amenazas malévolas sabidas, cayéndolas, limpiando o quarantining según lo configurado.

Verifique las teclas de función

Para marcar que ambas teclas de función están habilitadas y active:

- Vaya a la **administración del sistema** > a las **teclas de función**
- Asegurese el **contra virus de Sophos** y las licencias del **McAfee** son activas.

Exploración del contra virus del permiso

- Navegue a los **Servicios de seguridad** > al **contra virus - Sophos**
- Haga clic el **Enablebutton**.
- Asegurese la **actualización automática se habilita** y la actualización de los archivos del contra virus de Sophos está trabajando muy bien. En caso necesario, **actualización del tecleo ahora** para iniciar la actualización del archivo inmediatamente:

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: (?)	Enabled
Edit Global Settings...	

Current Sophos Anti-Virus files			
File Type	Last Update	Current Version	New Update
Sophos Anti-Virus Engine	Wed Nov 6 10:04:30 2019	3.2.07.377.1_5.68	Not Available
Sophos IDE Rules	Wed Nov 6 12:03:56 2019	2019110602	Not Available
No updates in progress.			Update Now

- Cometer de Submitand del tecleo sus cambios.

Si la licencia del McAfee es activa también, navegue a los **Servicios de seguridad** > al **contra virus - McAfee**

- Haga clic el **Enablebutton**.

- Asegurese la **actualización automática se habilita** y la actualización de los archivos del contra virus del McAfee está trabajando muy bien. En caso necesario, la **actualización del teclado ahora** para iniciar el archivo se pone al día inmediatamente.
- **Cometer de Submitand del teclado sus cambios**

Contra virus de la configuración en las directivas del correo

En una directiva del correo entrante, se recomienda lo que sigue:

- Navegue **para enviar las directivas > las directivas del correo entrante**
- Personalice las configuraciones del **contra virus** para una directiva del correo entrante haciendo clic el link azul bajo el contra virus para la directiva que usted desea personalizar.
- Aquí usted puede seleccionar la opción de la exploración del contra virus que usted desea habilitar para esta directiva.
- Con el propósito de este documento de la mejor práctica, seleccione el **McAfee** y el **contra virus de Sophos**:

Anti-Virus Settings	
Policy:	DEFAULT
Enable Anti-Virus Scanning for This Policy:	<input checked="" type="radio"/> Yes <input checked="" type="checkbox"/> Use McAfee Anti-Virus <input checked="" type="checkbox"/> Use Sophos Anti-Virus <input type="radio"/> No

- No intentamos reparar un archivo, así que los restos de la exploración del mensaje **analizan para los virus solamente**:

Message Scanning	
	Scan for Viruses only <input type="button" value="v"/> <input type="checkbox"/> Drop infected attachments if a virus is found <input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	<input type="text" value="Deliver As Is"/>
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	<input type="text" value="[WARNING: VIRUS REMOVED]"/>
Advanced	Optional settings for custom header and message delivery.

- La acción recomendada para los **mensajes cifrado** y de **Unscannable** es **entregar como está** con un asunto modificado para su atención.
- La política recomendada para el antivirus es **descenso** todos los **mensajes Virus-infectados** tal y como se muestra en de la imagen abajo:

Encrypted Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[A/V UNSCANNABLE]
▶ Advanced	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING : VIRUS DETECTED]
▶ Advanced	Optional settings for custom header and message delivery.

- **Cometer de Submitand del tecleo sus cambios**

Una directiva similar se recomienda para las directivas salientes del correo, sin embargo, no recomendamos el modificar del asunto en el correo electrónico saliente.

Graymail

La solución de administración del graymail en el dispositivo de seguridad del correo electrónico comprende de dos componentes: un motor e integrados de la exploración del graymail nube-basados desinscriben el servicio. La solución de administración del graymail permite que las organizaciones identifiquen el graymail usando el motor integrado del graymail y aplicar los controles de políticas apropiados y proporcionar un mecanismo fácil para que los usuarios finales desinscriban de los mensajes no deseados usando desinscriba el servicio.

Las categorías de Graymail incluyen el correo electrónico del márketing, el correo electrónico social de la red y el correo electrónico a granel. Las opciones avanzadas incluyen agregar una encabezado de encargo, el envío a un host alterno y archivar el mensaje. Para esta mejor práctica, habilitaremos la caja fuerte de Graymail desinscribimos la característica para la directiva predeterminada del correo.

Verifique las teclas de función

- En el ESA, navegue a la **administración del sistema** > a las **teclas de función**
- Busque **Graymail Unsubscription seguro** y asegúrese lo es activo.

Habilite Graymail y la caja fuerte desinscribe los servicios

- En el ESA, navegue a los **Servicios de seguridad** > al **IMS** y a **Graymail**
- Haga clic el **editar Graymail Settings** button en las **configuraciones globales de Graymail**
- Seleccione todas las opciones - **Habilite la detección de Graymail**, **habilite la caja fuerte desinscriben** y **habilitan las actualizaciones automáticas**:

Graymail Global Settings	
Graymail Detection	Enabled
Safe Unsubscribe	Enabled
Automatic Updates ?	Enabled

[Edit Graymail Settings](#)

- Haga clic el cometer de **Submitand sus cambios**

Configure Graymail y la caja fuerte desinscribe en las directivas

Una vez que Graymail y Unsubscribe seguro se ha configurado global, usted puede ahora aplicar estos servicios para enviar las directivas.

- Navegue **para enviar las directivas > las directivas del correo entrante**
- Hacer clic el link azul bajo **Graymail** permitirá para que esa directiva determinada utilice las configuraciones personalizadas de Graymail.
- Aquí usted puede seleccionar el Graymailoptions que usted desea habilitar para esta directiva.
- Con el propósito de este documento de la mejor práctica, haga clic el botón de radio al lado de **habilitan la detección de Graymail para esta directiva y habilitan a Graymail que desinscribe para esta directiva:**

Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages (Recommended) <input type="radio"/> Unsigned Messages

Las tres secciones siguientes incluyen la **acción en las configuraciones del correo electrónico del márketing**, la **acción en las configuraciones sociales del correo electrónico de la red** y la **acción en las configuraciones a granel del correo electrónico**.

- La mejor práctica recomendada es habilitar todos y seguir siendo la acción como **entrega** con el texto prepended agregado al tema por lo que se refiere a las categorías como se muestra abajo:

✓ Action on Marketing Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[MARKETING]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Social Network Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[SOCIAL NETWORK]"/>
▶ Advanced	Optional settings for custom header and message delivery.
✓ Action on Bulk Email	
Apply this action to Message:	Deliver <input type="button" value="v"/> Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append <input type="text" value="[BULK]"/>
▶ Advanced	Optional settings for custom header and message delivery.

- Cometer de Submitand del tecleo sus cambios

La directiva saliente del correo debe hacer que **Graymail** permanezca en la condición discapacitada.

Filtros del brote

Los filtros del brote combinan los activadores en el motor antispam, exploración URL y las Tecnologías y más de la detección para marcar correctamente los elementos con etiqueta que caen fuera de la categoría verdadera del Spam – por ejemplo, el phishing envía por correo electrónico y los correos electrónicos del timo y los maneja apropiadamente con las notificaciones de usuario o la cuarentena.

Verifique las teclas de función

- En el ESA, navegue a la **administración del sistema** > a las **teclas de función**
- Busque los **filtros del brote** y asegurese los es activo.

Habilite el servicio de los filtros del brote

- En el ESA, navegue a los **Servicios de seguridad** > a los **filtros del brote**
- Haga clic el **Enable** button en la **descripción de los filtros del brote**
- Aquí usted puede configurar las configuraciones múltiples. Las configuraciones recomendadas se muestran en la imagen abajo:

Outbreak Filters Global Settings	
<input checked="" type="checkbox"/> Enable Outbreak Filters	
Adaptive Rules:	<input checked="" type="checkbox"/> Enable Adaptive Rules
Maximum Message Size to Scan:	<input type="text" value="3M"/> Maximum <i>Add a trailing K or M to indicate units.</i>
Emailed Alerts: (?)	<input checked="" type="checkbox"/> Receive Emailed Alerts
Web Interaction Tracking: (?)	<input checked="" type="checkbox"/> Enable Web Interaction Tracking

- Cometer de Submitand del tecleo sus cambios.

Filtros del brote de la configuración en las directivas

Una vez que el brote Filtershas configurado global, usted puede ahora aplicar las directivas de este tomail de la característica.

- Navegue **para enviar las directivas > las directivas del correo entrante**
- Hacer clic el link azul bajo los **filtros del brote** permitirá para que esa directiva determinada utilice las configuraciones personalizadas de los filtros del brote.
- Con el propósito de este documento de la mejor práctica, guardamos las configuraciones del filtro del brote con los valores predeterminados:

Outbreak Filter Settings	
Quarantine Threat Level: ?	3
Maximum Quarantine Retention:	Viral Attachments: 1 Days Other Threats: 4 Hours <input type="checkbox"/> Deliver messages without adding them to quarantine
Bypass Attachment Scanning: ▶	None configured

- Los filtros del brote pueden reescribir los URL si se juzgan malévolos, sospechados, o phish. Seleccione la **modificación del mensaje del permiso** para detectar y para reescribir las amenazas basadas URL.
- Asegurese la opción de la **reescritura URL** está **permiso** para todos los mensajes como el siguiente mostrado:

Message Modification	
<input checked="" type="checkbox"/> Enable message modification. Required for non-viral threat detection (excluding attachments)	
Message Modification Threat Level: ?	3
Message Subject:	Prepend [Possible \$threat_category Fraud] Insert Variables Preview Text
Include the X-IronPort-Outbreak-Status headers:	<input type="radio"/> Enable for all messages <input type="radio"/> Enable only for threat-based outbreak <input checked="" type="radio"/> Disable
Include the X-IronPort-Outbreak-Description header:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Alternate Destination Mail Host (Other Threats only):	<input type="text"/>
URL Rewriting:	Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails. <input type="radio"/> Enable only for unsigned messages (recommended) <input checked="" type="radio"/> Enable for all messages <input type="radio"/> Disable
Bypass Domain Scanning ?	<input type="text"/>
Threat Disclaimer:	System Generated Preview Disclaimer <small>Disclaimer text will be applied to the top of the message body for Suspicious and Quarantined messages. To create custom disclaimers go to Mail Policies > Text Resources > Disclaimers</small>

- Haga clic el **cometer de Submitand sus cambios**

La directiva saliente del correo debe hacer que los **filtros del brote** permanezcan en la condición **discapacitada**.

Conclusión

Este documento apuntó describir el valor por defecto, o las configuraciones de la mejor práctica para el Anti-Spam, el contra virus, Graymail y los filtros del brote en el dispositivo de seguridad del correo electrónico (ESA). Todos estos filtros están disponibles en las directivas entrantes y salientes del correo electrónico, y la configuración y la filtración se recomiendan en ambos –

mientras que el bulto de la protección está para entrante, la filtración del flujo saliente proporciona la protección contra los correos electrónicos retransmitidos o los ataques maliciosos internos.