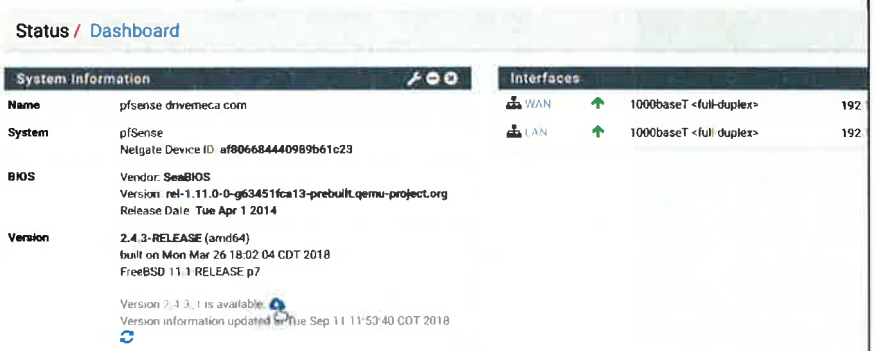
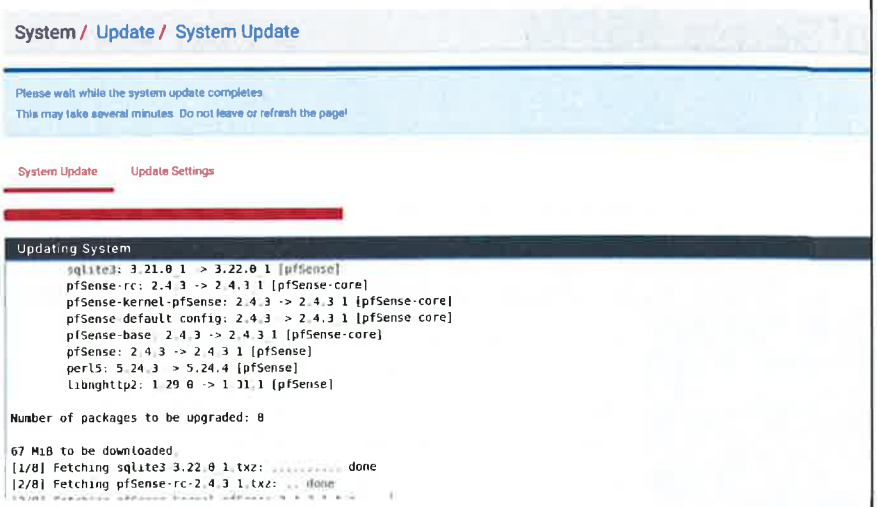
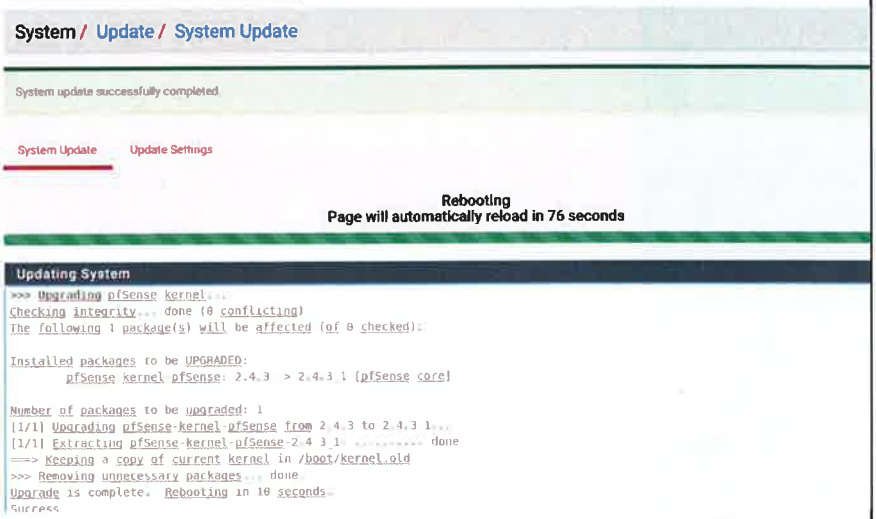
Ficha de mantenimiento técnico
pfSense SSPM

Sophie UNAM

Tarea	Actualización de la unidad de gestión de amenazas centralizada, pfSense
Detalles de la actualización	Versión a instalar: **2.4.5.1-RELEASE** Versión anterior: **2.5.0-RELEASE** Medio de instalación: Descarga vía Internet. Arquitectura o Firmware: amd64 Servicios relacionados: firewall perimetral, sistema de prevención y detección de intrusiones, DNS, sistema de análisis de tráfico de red.
Servicios críticos	• Salida a Internet para la SSPM. • Servicios web públicos de la SSPM. • Sistema de resolución de nombres, DNS, para la LAN SSPM. • Sistema de filtrado de contenidos para la LAN SSPM. • Firewall perimetral. • Sistema de detección y prevención de intrusiones.
Descripción	Dentro del convenio SSPM - UNAM, se actualizó el sistema operativo de la unidad de gestión de amenazas centralizadas, pfSense, de la SSPM a la última versión estable.
Impacto	La actualización resulta en una interrupción de todos los servicios críticos.
Evidencia	1. Menú actualización. 

	2. Descarga de actualizaciones.  3. Actualización terminada.  4. Reinicio con la nueva versión del sistema operativo.
Observaciones	• En atención a las recomendaciones de las autoridades sanitarias, este mantenimiento se llevó a cabo en modalidad de conexión remota, con personal de la SSPM en sitio.
Referencias	https://www.netgate.com/blog/pfsense-2-4-5-release-now-available.html
Firma responsable	Ulises M Alvarez. Sophie UNAM.

Ficha de mantenimiento técnico
pfSense SSPM

Sophie UNAM

Tarea	Actualización SecurityOnion a 2.3.40.
Detalles de la tarea	Objetivo: Actualizar el sistema monitoreo de seguridad en red SecurityOnion a la última versión estable. Versión SecurityOnion: 2.3.40. Medio de instalación: Internet. Arquitectura o Firmware: amd64. Servicios relacionados: Monitor de eventos de seguridad de red.
Servicios críticos	• Monitor de eventos de seguridad de red.
Descripción	Dentro del convenio SSPM - UNAM, se programó la actualización del sistema de monitoreo de eventos de seguridad SecurityOnion a la última versión estable, 2.3.40.
Impacto	Durante la descarga de actualizaciones se interrumpió la camptura de paquetes de red.

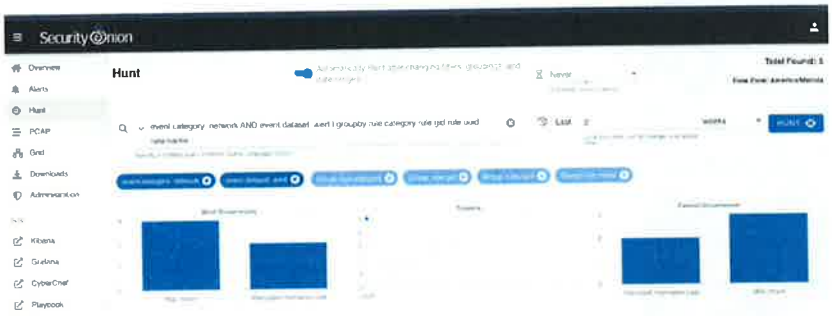
Evidencia	Se siguió el procedimiento estándar para actualizar el sistema:
	1. En la consola, se ejecutó: sudo soup
	`##########################################`
	`##########################################`
	`###                                      ###`
	`###   UNAUTHORIZED ACCESS PROHIBITED   ###`
	`###                                      ###`
	`##########################################`
	`##########################################`
	`uma@132.248.185.246's password:`
	`Last failed login: Mon Mar 29 16:26:54 UTC 2021 from nodo50.geociencias.unam.mx on ssh:not`
	`There was 1 failed login attempt since the last successful login.`
	`Last login: Mon Mar 29 16:16:23 2021 from nodo50.geociencias.unam.mx`
	
	`Access the Security Onion web interface at https://132.248.185.246`
	`(You may need to run so-allow first if you haven't yet)`
	
	`[uma@monitor ~]$ sudo soup`

2. En la consola, se actualizó el sistema operativo: sudo yum update, y se volvió a ejecutar: sudo soup

```
[uma@monitor ~]$ sudo yum update
[sudo] password for uma:
Failed to set locale, defaulting to C
Loaded plugins: fastestmirror, versionlock
Loading mirror speeds from cached hostfile
 * base: mirrors.unifiedlayer.com
 * epel: d2lzk17pfhq30m.cloudfront.net
 * extras: mirror.centos.lax1.serverforge.org
 * updates: repos.forethought.net
Excluding 4 updates due to versionlock (use "yum versionlock status" to show them)
No packages marked for update
[uma@monitor ~]$ sudo soup

SOUP - Security Onion UPdater

Please review the following for more information about the update process and recent updates:
https://docs.securityonion.net/soup
https://blog.securityonion.net

Please note that soup only updates Security Onion components and does NOT update the underlying operating system (OS). When you installed Secur
ity Onion, there was an option to automatically update the OS packages. If you did not enable this option, then you will want to ensure that th
e OS is fully updated before running soup.

Press Enter to continue or Ctrl-C to cancel.
```

3. Se comprobó actualización.

4. Se comprobó funcionalidad.



Una vez finalizadas las pruebas, se declaró la actualización como exitosa.

Observaciones	• Este mantenimiento se llevó a cabo en el sitio. Con personal de la SSPM y de la UNAM.
Referencias	• https://docs.securityonion.net/en/2.3/updating.html

Firma responsable	Ulises M Alvarez. Sophie UNAM.