




Universidad Estatal a Distancia
Rectoría
Dirección de Tecnología de Información y Comunicaciones



Instructivo para la atención de alertas e incidentes


UNIDAD DE SEGURIDAD DIGITAL



	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	1 de 19

Contenido

1	Propósito.....	3
2	Alcance.....	3
3	Responsabilidades.....	3
4	Definiciones.....	3
5	Documentos Relacionados.....	4
6	Abreviaturas.....	4
7	Normativa relacionada.....	4
8	Descripción del proceso.....	5
8.1	Actividades para la atención de las alertas e incidentes.....	5
8.2	Atención de la alerta e incidente provenientes del SOC.....	5
8.3	Atención de la alerta o incidente del Proceso Consolas de Seguridad de Punto Final y EDR 15	
8.4	Gestión de alertas e incidentes de Boletines y Alertas Técnicas.....	18
9	Anexos.....	19
10	Control de cambios.....	19

	Instructivo para la atención de alertas e incidentes	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	2 de 19

Participantes

Elaboración

Nombre	Puesto	Dependencia
Johnny Saborío Álvarez	Coordinador de la USD	Dirección de Tecnología de Información y Comunicaciones
Michael González Flores	Especialista en Seguridad Informática	Dirección de Tecnología de Información y Comunicaciones
Alejandro Sánchez Rivera	Especialista en Seguridad Informática	Dirección de Tecnología de Información y Comunicaciones

Validación

Nombre	Rol	Dependencia	Fecha
Francisco Durán Montoya	Director	Dirección de Tecnología de Información y Comunicaciones	25 de setiembre de 2023


Aprobación

Aprobado mediante acuerdo tomado por el Consejo de Rectoría, sesión extraordinaria No. 2318-2024, Artículo VI, inciso 2) celebrada el 27 de mayo del 2024 (REF. CR-2024-935).

_____.

Asesoría Técnica

Lic. Carlos Salazar Castañeda, Centro de Planificación y Programación Institucional.
 Lic. Paula Martínez Sánchez, Centro de Planificación y Programación Institucional.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	3 de 19

1 Propósito

Describir las tareas que deben realizar las personas funcionarias de la USD, en la atención de alertas e incidentes a la Infraestructura Tecnológica, de la Universidad Estatal a Distancia.

2 Alcance


Este documento debe ser aplicado por las personas funcionarias de la Unidad de Seguridad Digital.

3 Responsabilidades

- Las personas funcionarias en la Unidad de Seguridad Digital tienen la responsabilidad técnica de identificar, analizar y mitigar las alertas e incidentes de seguridad, que se generan del monitoreo de eventos; así como, de ejecutar las solicitudes que indique la persona coordinadora.
- La persona coordinadora de la USD es la encargada de la coordinación, planificación, control y seguimiento de las actividades que se realizan en dicha unidad.

4 Definiciones

- **Alerta:** es un aviso reactivo ante una posible amenaza de ciberseguridad, que puede representar un alto riesgo para la infraestructura tecnológica y la información de la UNED.
- **Consola de Seguridad de Punto Final:** es un antivirus institucional, programa o herramienta encargada de eliminar el malware a nivel institucional
- **Dashboard:** es una forma de presentar de manera visual, mediante un portal web, los datos más importantes a nivel de ciberseguridad de las Apps, servicios, servidores y dispositivos finales, entre otros, de la infraestructura tecnológica que se está monitoreando, mostrando valores estadísticos, tendencias, elementos más críticos o de mayor importancia y relevancia.
- **Detecciones:** son posibles amenazas (tipo malware) que pueden afectar a los dispositivos que son protegidos mediante la seguridad del punto final.
- **Directorio Activo:** es una base de datos y un conjunto de servicios, que conectan a los usuarios con los recursos de red, que necesitan para realizar su trabajo.
- **Equipo de Respuesta a Incidentes de la UNED:** personal seleccionado de las unidades de la DTIC, el cual tendrá la responsabilidad, según el escenario que se presente de la atención de incidentes de ciberseguridad de la Universidad, convirtiéndose en la primera línea de ciberdefensa de la UNED. La UNED cuenta de forma adicional, con un equipo de respuesta a incidentes externo, que brinda esta función, producto del contrato de servicios de SOC (Centro de Operaciones de Seguridad).
- **Incidente:** un incidente de seguridad es un evento adverso en un sistema de Información, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	4 de 19

alguna vulnerabilidad o un intento o amenaza, de romper los mecanismos de seguridad existentes.

- **Malware:** es un programa informático, cuya principal característica es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema. Tomado de INCIBE.
- **Ransomware:** es un tipo de malware que toma por completo el control del equipo, bloqueando o cifrando la información del usuario para pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. Tomado de INCIBE.

5 Documentos Relacionados


NA

6 Abreviaturas

- **DTIC:** Dirección de Tecnología de Información y Comunicaciones.
- **FW:** Firewall
- **RDP:** Remote Desktop Protocol (Protocolo de Escritorio Remoto).
- **SOC:** Centro de Operaciones de Seguridad.
- **UIT:** Unidad de Infraestructura Tecnológica.
- **USD:** Unidad de Seguridad Digital.
- **VPN:** Red Privada Virtual.
- **R.C.:** Redes Críticas.

7 Normativa relacionada

- Marco de Gobierno y Gestión de TI de la UNED, objetivo de gobierno y objetivo de gestión: seguridad de la información.
- Normas técnicas para el gobierno y gestión de las tecnologías de la información del MICITT, proceso XI Seguridad y Ciberseguridad.
- Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, capítulo II, artículo 5, incisos: a), b), d), e), f), h), i), m), n), q) y el capítulo VI.
- Acuerdo de Políticas para el Uso y Seguridad de internet (Sesión 1604-2002, Art. VIII, inciso 2) celebrada el 24 de octubre del 2002).
- Políticas para el Uso y Desarrollo de Tecnologías de la Información y la Comunicación de la UNED.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	5 de 19

- Acuerdo de creación de la Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC)-UNED y sus funciones, sesión: 2406-2015, Artículo II, inciso 1-a).

8 Descripción del proceso

8.1 Actividades para la atención de las alertas e incidentes

En los siguientes apartados se detallan las diferentes actividades asociadas a alertas e incidentes, que puede realizar la persona funcionaria de la USD.

8.2 Atención de la alerta e incidente provenientes del SOC


8.2.1 La persona funcionaria de la USD, identifica y da inicio al seguimiento de la siguiente forma:

8.2.2 Se analiza el correo y clasifica las alertas o incidentes, principalmente en:

- | | |
|---------------------------------------|--------------------|
| a. Autenticaciones Excesivas Windows. | Ver punto 8.2.2.1 |
| b. Autenticaciones Excesivas VPN. | Ver punto 8.2.2.2 |
| c. Evento sospechoso RDP. | Ver punto 8.2.2.3 |
| d. Posible Ransomware Detectado. | Ver punto 8.2.2.4 |
| e. Contacto IP CONTI. | Ver punto 8.2.2.5 |
| f. Malware Detectado. | Ver punto 8.2.2.6 |
| g. Conexiones Maliciosas R.C. | Ver punto 8.2.2.7 |
| h. Cambio políticas FW. | Ver punto 8.2.2.8 |
| i. Bloqueo de cuentas privilegiadas. | Ver punto 8.2.2.9 |
| j. Alertas consola DARKTRACE | Ver punto 8.2.2.10 |

8.2.2.1 Autenticaciones Excesivas Windows


- Se recibe el correo con el encabezado AUTENTICACIONES EXCESIVAS WIN, criticidad y número de tiquete.
- Se corroboran lo siguientes datos:
 - Cantidad de intentos.
 - Fecha y hora del evento.
 - Usuario.
 - Ip origen.
 - Ip destino.
 - Dispositivo.
- Se revisa el detalle en la “Descripción de la alerta”.
- Se analizan las **recomendaciones**.
- En caso de ser el usuario de un funcionario, se realiza la consulta mediante correo electrónico, TEAMS, llamada telefónica o cualquier otro medio, para corroborar que efectivamente él fue quien cometió los errores de autenticación.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	6 de 19

- f. En caso de ser un usuario de sistema, se localiza al desarrollador encargado de la aplicación y que da uso a ese usuario en los sistemas, para corroborar el porqué de los fallos de autenticación.
- g. Si se logra determinar en cualquiera de los dos casos anteriores, con el funcionario o el encargado del usuario de sistema, que ellos no han realizado o provocado ese evento y no se tiene conocimiento sobre estos intentos **fallidos de autenticación Windows**, se procede a realizar la investigación, de ser requerido, se solicita la colaboración del SOC y del Equipo de Respuesta a Incidentes de la UNED.
- h. Una vez realizada la investigación, se procede a tomar las medidas de seguridad necesarias para contener cualquier amenaza, de ser necesario erradicar algún malware y mitigar cualquier riesgo asociado a la alerta y posible incidente.
- i. Luego de haber realizado la investigación con el funcionario o el encargado del usuario de sistema; así como, de la atención de la alerta e incidente, se procede a redactar el correo de respuesta al **SOC**, para que sea cerrado el ticket o correo correspondiente.
- j. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente (ticket, intentos de autenticación, fecha y hora, usuario, ip origen, ip destino, host, causa).

8.2.2.2 Autenticaciones Excesivas VPN


- a. Se recibe el correo con el encabezado **AUTENTICACIONES EXCESIVAS VPN**, criticidad y número de ticket.
- b. Se corroboran lo siguientes datos:
 1. Cantidad de intentos.
 2. Fecha y hora del evento.
 3. Usuario.
 4. Ip de Origen.
 5. Usuario destino.
 6. Ip destino.
 7. Dispositivo.
- c. Se revisa el detalle en la **“Descripción de la alerta”**.
- d. Se analizan las **recomendaciones**.
- e. Se debe de localizar al funcionario y realizar la consulta, mediante correo electrónico, TEAMS, llamada telefónica o cualquier otro medio, para corroborar que efectivamente él fue el que cometió los errores de autenticación VPN.
- k. Si se logra determinar con el funcionario que no ha realizado o no se tiene conocimiento sobre esos errores de autenticación, se procede a realizar la investigación, de ser requerido se solicita la colaboración del SOC y del Equipo de Respuesta a Incidentes de la UNED.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	7 de 19

- l. Una vez realizada la investigación, se procede a tomar las medidas de seguridad necesarias para contener cualquier amenaza, de ser necesario erradicar algún malware y mitigar cualquier riesgo asociado a la alerta y posible incidente.
- f. Luego de haber realizado la investigación; así como, de la atención de la alerta e incidente, se procede a redactar el correo de respuesta al **SOC**, para que sea cerrado el ticket o correo correspondiente.
- g. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresan lo siguientes datos (ticket, intentos de autenticación, fecha y hora, usuario, ip origen, ip destino, host, causa).

8.2.2.3 Evento sospechoso RDP


- a. Se recibe el correo con el encabezado **EVENTO SOSPECHOSO RDP**, criticidad y número de ticket.
- b. Se corroboran lo siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. URL.
 3. Ip de Origen.
 4. Dispositivo que recibió la alerta (**Receiver**).
 5. Nombre de la Regla que activo la alerta.
 6. Host involucrado.
 7. Proceso.
- c. Se revisa el apartado de "**Referencias Adicionales**".
- d. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisa los detalles del mismo. Se actualiza los productos de seguridad en caso de ser necesario y se atienden las posibles amenazas reportadas en el equipo.
- e. Se da clic izquierdo sobre el evento de RDP y luego se selecciona Investigar, esto nos dirigirá a la Consola EDR, donde se visualizarán más detalles de la alerta y posible incidente, como la dirección IP que intentó conectarse mediante RDP.
- f. Se analiza si la dirección IP que intentó conectarse por medio de RDP, cuenta con reputación maliciosa. Si la IP es maliciosa, debe ser agregada en los sistemas de ciberdefensa de la UNED, de lo contrario pasa al punto K.
- g. Se consulta la existencia de la dirección Ip, que causó la alerta RDP en el archivo de Excel utilizado por la USD, para el control de IPs maliciosas, ubicado en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\ip´s.xls](#)), una vez ingresada la ip en el Excel, se procede a realizar una búsqueda, aplicando un formato condicional, de valores duplicados sobre todos los datos del archivo, corroborando si esta Ip ya se encuentra en nuestra lista de bloqueos de los equipos de seguridad perimetral.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	8 de 19

- h. Si la Ip no se encuentra en esta lista anterior, se agrega al Excel utilizado por la USD para el control de IPs maliciosas, luego se debe de agregar al archivo utilizado por el personal de la **Unidad de Infraestructura Tecnológica** para realizar los bloqueos respectivos, el cual se encuentra en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\BloqueosFortinet\Ips.txt](#)).
- i. Si se ingresó la Ip como se indica en el punto H, se debe de crear un ticket de Solicitudes de atención y requerimientos, en la siguiente dirección: <https://solicitudesdtic.uned.ac.cr/>, donde se debe de indicar que se actualicen los archivos de indicadores de compromiso para los Equipos de Seguridad Perimetral que contienen las **direcciones IPs, archivos hash, direcciones Url y dominios a bloquear**.
- j. Luego de haber realizado alguna de las tareas anteriores, se debe dar respuesta al SOC, donde se indique todo lo realizado y que se proceda con el cierre del ticket.
- k. Por último, se ingresa el contenido del detalle del ticket de Solicitudes de atención y requerimientos en el control del Sprint actual, en el apartado de incidentes de seguridad.

8.2.2.4 Posible Ransomware Detectado

- a. Se recibe el correo con el encabezado **POSIBLE RANSOMWARE DETECTADO**, criticidad y número de ticket.
- b. Se corroboran lo siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Usuario origen.
 3. Ip de Origen.
 4. Ip de Destino.
 5. Host involucrado.
- c. Se revisa el apartado **"External Resources"**.
- d. Se revisa el apartado **"Summary"**.
- e. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisan los detalles del mismo.
- f. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si existen, eliminarlas.
- g. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
- h. Se identifica la amenaza reportada en el equipo.
- i. Se da clic izquierdo sobre el evento de POSIBLE RANSOMWARE, luego se selecciona **Investigar**, esto nos dirigirá a la **Consola EDR**, donde se visualizará más detalle de la alerta y posible incidente, como el nombre del archivo que generó dicha alerta de POSIBLE RANSOMWARE.
- j. Estando en la consola EDR se analiza el apartado **"Command line"**, para determinar la línea de comando que generó la alerta. **El SHA-1** se verifica en Virus Total o cualquier otro sitio de


	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	9 de 19

análisis de archivos Hash, si se determina que está comprometido, se ingresa el Sha-1 en la lista de **Bloqueo de Hashes**.

- k. Luego de haber analizado dicha alerta, si es necesario se contacta con el funcionario dueño del activo para solicitar conexión y poder revisar el equipo vía TeamViewer.
- l. Si se determina que el equipo efectivamente está infectado, se procede con el aislamiento **del equipo en la red Institucional**, y el seguimiento a partir de este momento se realiza, de ser necesario, en conjunto con la unidad de Soporte Técnico, la colaboración del SOC y de ser necesario con el equipo de respuesta de incidentes.
- m. Luego de haber revisado y descartado la amenaza, se debe enviar un correo de respuesta al SOC, informando lo realizado y así se podrá dar cierre al ticket.
- n. Luego se procede a ingresar el contenido del detalle del ticket de Solicitudes de atención y requerimientos, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (usuario, ip origen, ip destino y dispositivo).

8.2.2.5 Contacto con IP CONTI


- a. Se recibe el correo con el encabezado **CONTACTO IP CONTI**, criticidad y número de ticket.
- b. Se corroboran los siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Ip de Origen.
 3. Puerto Origen.
 4. Ip de Destino.
 5. Puerto Destino.
 6. Protocolo.
 7. Subtype.
 8. Host involucrado.
- c. Se revisa el apartado **“External Resources”**.
- d. Se revisa el apartado **“Summary”**.
- e. Se validan las **“Recomendaciones”**.
- f. Se analiza si la dirección IP que generó dicha alerta cuenta con reputación maliciosa, tanto en Virus Total como Abuse IP y cualquier otro sitio de consulta de IPs maliciosas. Si se determina que la IP es maliciosa debe ser agregada en los sistemas de ciberdefensa de la UNED, de lo contrario pasa al punto O.
- g. Se consulta la existencia de dicha dirección en el archivo de Excel utilizado por la USD para el control de IPs maliciosas, ubicado en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios – Hash\Ip´s.xls](#)), una vez ingresada la ip en el Excel, se procede a realizar una búsqueda, aplicando un formato condicional de valores duplicados sobre todos los datos del archivo, corroborando si esta Ip ya se encuentra en nuestra lista de bloqueos de los equipos de seguridad perimetral.

	Instructivo para la atención de alertas e incidentes	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	10 de 19

- h. Si la Ip no se encuentra en esta lista anterior, se agrega al Excel utilizado por la USD para el control de IPs maliciosas, luego se debe de agregar al archivo utilizado por el personal de la **Unidad de Infraestructura Tecnológica** para realizar los bloqueos respectivos, el cual se encuentra en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\BloqueosFortinet\IPS_Maliciosas.txt](#)).
- i. Si se ingresó la **Ip** como se indica en el punto H, se debe de crear un ticket de Solicitudes de atención y requerimientos, en la siguiente dirección: <https://solicitudesdtic.uned.ac.cr/>, donde se debe de indicar que se actualicen los archivos de indicadores de compromiso para los Equipos de Seguridad Perimetral, que contienen las **direcciones IPs, archivos hash, direcciones Url y dominios a bloquear**.
- j. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisa los detalles del mismo.
- k. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
- l. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
- m. Si luego del análisis enviado se determina que el equipo efectivamente está infectado, se procede con **el aislamiento del equipo en la red Institucional**, y el seguimiento a partir de este momento, se realiza de ser necesario en conjunto con la unidad de Soporte Técnico, la colaboración del SOC y de ser necesario con el equipo de respuesta de incidentes.
- n. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (ip origen, puerto origen, ip destino, puerto destino, protocolo, host).
- o. Luego de haber realizado alguna de las tareas anteriores, se debe dar respuesta al SOC, donde se indique todo lo realizado y que se proceda con el cierre del ticket.

8.2.2.6 Malware detectado


- a. Se recibe el correo con el encabezado **MALWARE DETECTADO**, criticidad y número de ticket.
- b. Se corroboran lo siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Usuario origen.
 3. Ip origen.
 4. Ip destino.
 5. Host.
- c. Se revisa el apartado **"External Resources"**.
- d. Se revisa el apartado **"Summary"**.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	11 de 19


- e. Se validan las **“Recomendaciones”**.
- f. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisan los detalles del mismo.
- g. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
- h. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
- i. Se da clic izquierdo sobre el evento de **MALWARE DETECTADO**, luego se selecciona **Investigar**, esto nos dirigirá a la **Consola EDR**, donde se visualizará más detalle de la alerta y posible incidente, como el nombre del archivo que generó dicha alerta.
- j. Estando en la consola EDR se analiza el apartado **“Command line”**, para determinar la línea de comando que generó la alerta. **El SHA-1** se verifica en Virus Total o cualquier otro sitio de análisis de archivos Hash, si se determina que está comprometido, se ingresa el **SHA-1** en la lista de **Bloqueo de Hashes**.
- k. Luego de haber analizado dicha alerta, si es necesario se contacta con el funcionario dueño del activo, para solicitar conexión y poder revisar el equipo vía TeamViewer.
- l. Si se determina que el equipo efectivamente está infectado se procede con el aislamiento **del equipo en la red Institucional**, y el seguimiento a partir de este momento, en caso de ser necesario, se realiza en conjunto con la Unidad de Soporte Técnico, la colaboración del SOC y el equipo de respuesta de incidentes.
- m. Luego de haber revisado y descartado la amenaza, se debe enviar un correo de respuesta al SOC, informado lo realizado y así se podrá dar cierre al tiquete.
- n. Luego se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (usuario, ip origen, ip destino y dispositivo)

8.2.2.7 Conexiones Maliciosas & Conexiones Maliciosas R.C.

- a. Se recibe el correo con el encabezado **CONEXIONES MALICIOSAS o CONEXIONES MALICIOSASA R.C.** criticidad y número de tiquete.
- b. Se corroboran lo siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Ip origen.
 3. Puerto origen.
 4. Ip destino.
 5. Puerto destino.
 6. Protocolo.
 7. Subtype.

	Instructivo para la atención de alertas e incidentes	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	12 de 19

8. Host.
- c. Se revisa el apartado **“External Resources”**.
 - d. Se revisa el apartado **“Summary”**.
 - e. Se validan las **“Recomendaciones”**.
 - f. Se analiza si la dirección IP que generó dicha alerta, cuenta con reputación maliciosa, tanto en Virus Total como Abuse IP y cualquier otro sitio de consulta de IPs maliciosas. Si se determina que es maliciosa, debe ser agregada en los sistemas de ciberdefensa de la UNED, de lo contrario pasa al punto **O**.
 - g. Se consulta la existencia de dicha dirección en el archivo de Excel, utilizado por la USD para el control de IPs maliciosas, ubicado en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios – Hash\Ip´s.xls](#)), una vez ingresada la ip en el Excel, se procede a realizar una búsqueda, aplicando un formato condicional de valores duplicados, sobre todos los datos del archivo, corroborando si esta Ip ya se encuentra en nuestra lista de bloqueos, de los equipos de seguridad perimetral.
 - h. Si la Ip no se encuentra en esta lista anterior, se agrega al Excel utilizado por la USD, para el control de IPs maliciosas, luego se debe agregar al archivo utilizado por el personal de la **Unidad de Infraestructura Tecnológica**, para realizar los bloqueos respectivos, el cual se encuentra en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\BloqueosFortinet\IPS_Maliciosas.txt](#)).
 - i. Si se ingresó la **Ip** como se indica en el punto **H**, se debe crear un ticket de Solicitudes de atención y requerimientos, en la siguiente dirección: <https://solicitudesdtic.uned.ac.cr/>, donde se debe solicitar que se actualicen, los archivos de indicadores de compromiso para los Equipos de Seguridad Perimetral, que contienen las **direcciones IPs, archivos hash, direcciones Url y dominios a bloquear**.
 - j. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisa los detalles del mismo.
 - k. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
 - l. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
 - m. Si luego del análisis enviado se determina que el equipo efectivamente está infectado, se procede con **el aislamiento del equipo en la red Institucional**, y el seguimiento a partir de este momento, en caso de ser necesario, se realiza en conjunto con la Unidad de Soporte Técnico, la colaboración del SOC y el equipo de respuesta de incidentes.
 - n. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (ip origen, puerto origen, ip destino, puerto destino, protocolo, host).
 - o. Por último, se ingresa el detalle del ticket de Solicitudes de atención y requerimientos, en el control de seguimiento (Sprint actual), en el apartado de incidentes de seguridad y otros.

	Instructivo para la atención de alertas e incidentes	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	13 de 19


- p. Luego de haber realizado alguna de las tareas anteriores, se debe dar respuesta al SOC, donde se indique todo lo realizado y que se proceda con el cierre del ticket.

8.2.2.8 Cambio de políticas FW.

- a. Se recibe el correo con el encabezado **CAMBIO DE POLITICAS FW** criticidad y número de ticket.
- b. Se corroboran los siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Dispositivo.
 3. Usuario origen.
 4. Ip origen.
 5. Comportamiento observado.
- c. Se revisa el apartado **“Recursos externos”**.
- d. Se revisa el apartado **“Análisis”**.
- e. Se validan las **“Recomendaciones”**.
- o. Luego de haber realizado las tareas anteriores, se debe contactar con el funcionario de la unidad de infraestructura tecnológica, quien realizó el cambio, con el fin de programar una sesión y certificar dicha modificación.
- q. Si el funcionario de la UIT indica que no ha realizado este tipo de cambios, se inicia una investigación y se solicita la colaboración del SOC. En caso de ser necesario, se elimina la política y se realizan los ajustes necesarios de seguridad, en los equipos de seguridad perimetral.
- r. Luego de haber realizado y finalizado la investigación, se debe enviar un correo de respuesta al SOC, informado lo realizado y así se podrá dar cierre al ticket.
- p. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (dispositivo, usuario origen, ip origen, comportamiento observado)

8.2.2.9 Bloqueo de cuentas privilegiadas.


- a. Se recibe el correo con el encabezado **BLOQUEO DE CUENTAS PRIVILEGIADAS** criticidad y número de ticket.
- b. Se corroboran lo siguientes detalles del evento:
 1. Fecha y hora del evento.
 2. Usuario origen.
 3. Ip origen.
 4. Usuario destino.
 5. Ip destino.
 6. Domino.
 7. Host.
 8. Dispositivo.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	14 de 19

9. Comportamiento observado.
- c. Se revisa el apartado **“Recursos externos”**.
 - d. Se revisa el apartado **“Análisis”**.
 - e. Se validan las **“Recomendaciones”**.
 - q. Luego de haber realizado las tareas anteriores, se debe contactar con el funcionario de la unidad de infraestructura tecnológica, para revisar en conjunto este evento.
 - s. Si el encargado indica que no ha realizado este tipo de cambios, se inicia una investigación y se solicita la colaboración del SOC. En caso de ser necesario, se elimina el bloqueo y se realizan los ajustes necesarios en el Directorio Activo de la Universidad.
 - t. Luego de haber realizado y finalizado la investigación, se debe enviar un correo de respuesta al SOC, informado lo realizado y así se podrá dar cierre al tiquete.
 - r. Se procede a ingresar la información de la alerta, en el archivo del Sprint actual, donde se ingresa lo siguiente: (dispositivo, usuario origen, ip origen, comportamiento observado).

8.2.2.10 Alertas Consola DARKTRACE

- a. Se recibe alerta mediante correo electrónico de parte del SOC de Darktrace.
- b. Se analiza el correo con el fin de revisar el evento, específicamente:
 1. Número de caso.
 2. Clase de incidente.
 3. Nivel de riesgo.
 4. Fecha y hora.
 5. Origen.
 6. Destino.
 7. Credenciales.
 8. Análisis.
- c. Validar las recomendaciones de seguridad si son aplicables, se procede con la implementación de estas.
- d. Se revisa el evento (modelo de brecha) en el Darktrace.
- e. Se revisa el nombre del equipo en la Consola de Seguridad de Punto Final, si se muestra en consola se ejecutan los pasos siguientes **F al H**, sino pasar al punto **I**.
- f. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
- g. Se da clic izquierdo sobre la alerta que se muestre, luego se selecciona **Investigar**, esto nos dirigirá a la **Consola EDR**, donde se visualizará más detalle de la alerta y posible incidente.
- h. Estando en la consola EDR se analiza el apartado **“Command line”**, para determinar la línea de comando que generó la alerta. **El SHA-1** se verifica en Virus Total o cualquier otro sitio de análisis de archivos Hash, si se determina que está comprometido, se ingresa el **Sha-1**, en la

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	15 de 19

lista de **Bloqueo de Hashes** y se envía un análisis con desinfección para prevenir cualquier alerta activa.

- i. Si luego de realizar el análisis se detecta alguna amenaza, se inicia una investigación en conjunto con la Unidad de Soporte Técnico y de ser requerido, se solicita la colaboración del SOC y del Equipo de Respuesta a Incidentes de la UNED.
- j. Luego de haber realizado y finalizado la investigación, así como mitigado la amenaza, se debe enviar un correo de respuesta al SOC, informando lo realizado y así se podrá dar cierre al caso.
- k. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (dispositivo, usuario origen, ip origen, comportamiento observado).
- l. Se agrega un comentario en la alerta emitida por el Darktrace y se procede con el cierre de esta.

8.3 Atención de la alerta o incidente del Proceso Consolas de Seguridad de Punto Final y EDR


8.3.1 La persona funcionaria de la USD, identifica y da inicio al seguimiento de la siguiente forma:

8.3.2 Se ingresa al Dashboard de la Consola de Seguridad de Punto Final, se analiza las alertas o incidentes y se clasifica principalmente en:

1. EFI/CompuTrace.A Ver punto 8.3.2.1.
2. Filecoder behavior. Ver punto 8.3.2.2.
3. Ransomnote behavioral detection / file was written Ver punto 8.3.3.3.
4. Protocol Mismatch - Detected RDP. Ver punto 8.3.3.4.

8.3.2.1 Alertas EFI/CompuTrace.A

1. Se visualiza en la consola una alerta con la indicación **EFI/CompuTrace.A**.
2. Se da clic izquierdo sobre el equipo que generó la alerta.
3. Se verifica el nombre del equipo, fecha y hora del incidente.
4. Se actualizan los productos de seguridad si el equipo lo requiere.
5. Se verifican las detecciones y la cuarentena.
6. Se envía un análisis con desinfección para prevenir cualquier alerta activa.
7. Sobre la alerta **EFI/CompuTrace.A** damos clic izquierdo, luego en **Investigar**.
8. Nos desplazamos sobre la alerta, y revisamos el **SAH-1** en **Virus Total** o cualquier otro sitio de análisis de archivos Hash.
9. Si el Hash da como resultado ser malicioso, se procede a agregarlo en la consola **EDR**, específicamente en **bloqueo de hashes**.
10. Si luego de realizar el análisis, se detecta alguna amenaza, se inicia una investigación en conjunto con la unidad de soporte técnico y de ser requerido se


	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	16 de 19

solicita la colaboración del SOC y del Equipo de Respuesta a Incidentes de la UNED.

11. Una vez finalizada la revisión, si se observa que es un falso positivo, se agrega la causa de la alerta en las **exclusiones** de la consola **EDR**.
12. Lugo de realizar los pasos anteriores, nos devolvemos a la alerta y se marca, en la Consola de Seguridad de Punto Final, como resuelta.
13. Se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (dispositivo, usuario origen, ip origen, comportamiento observado).

8.3.2.2 Filecoder behavior


1. Se visualiza en la consola una alerta con la indicación **Filecoder behavior**.
2. Se da clic sobre el nombre del equipo que presenta la alerta y se revisan los detalles del mismo.
3. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
4. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
5. Se da clic izquierdo sobre el evento de **Filecoder behavior**, luego se selecciona Investigar, esto nos dirigirá a la Consola EDR, donde se visualizarán más detalles de la alerta y posible incidente, como el nombre del archivo que generó dicha alerta.
6. Estando en la consola EDR, se analiza el apartado "Command line", para determinar la línea de comando que genero la alerta. El SHA-1 se verifica en Virus Total o cualquier otro sitio de análisis de archivos Hash, si se determina que está comprometido, se ingresa el Sha-1 en la lista de Bloqueo de Hashes. En caso de ser necesario, el equipo es aislado de la red, mientras se continúa revisando el evento y se mitiga cualquier amenaza.
7. Estando en la consola **EDR**, y luego de haber revisado lo anterior, si se observa que es un falso positivo, se agrega la causa de la alerta en las **exclusiones** y se continua con el punto **10**.
8. Luego de haber analizado dicha alerta, si es necesario se contacta con el funcionario dueño del activo, para solicitar conexión al equipo y poder revisar el equipo vía conexión remota.
9. Si se determina que el equipo efectivamente está infectado, se procede con el aislamiento del equipo en la red Institucional, y el seguimiento a partir de este momento se realiza en conjunto con la unidad de Soporte Técnico, de ser requerido, se solicita la colaboración del SOC y el Equipo de Respuesta a Incidentes de la UNED.

	Instructivo para la atención de alertas e incidentes	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	17 de 19

10. Luego se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (usuario, ip origen, ip destino y dispositivo)
11. Luego de realizar los pasos anteriores, nos devolvemos a la alerta y se marca en la Consola de Seguridad de Punto Final como resuelta.

8.3.2.3 Ransomnote behavioral detection / file was written

1. Se visualiza en la consola una alerta con la indicación **Ransomnote**.
2. Se da clic sobre el nombre del equipo que presenta la alerta y se revisan los detalles del mismo.
3. Se actualizan los productos de seguridad en caso de ser necesario, se verifican las amenazas en cuarentena y si las hay, eliminarlas.
4. Se envía mediante consola un escaneo con desinfección, para prevenir cualquier amenaza activa.
5. Se da clic izquierdo sobre el evento de **Ransomnote behavioral**, luego se selecciona Investigar, esto nos dirigirá a la Consola EDR, donde se visualizarán más detalles de la alerta y posible incidente, como el nombre del archivo que generó dicha alerta.
6. Estando en la consola EDR se analiza el apartado "Command line", para determinar la línea de comando que generó la alerta. El SHA-1 se verifica en Virus Total o cualquier otro sitio de análisis de archivos Hash, si se determina que está comprometido, se ingresa el Sha-1 en la lista de Bloqueo de Hashes.
7. Estando en la consola **EDR**, y luego de haber revisado lo anterior, si se observa que es un falso positivo se agrega la causa de la alerta en las **exclusiones**. y se continua con el punto **10**.
8. Luego de haber analizado dicha alerta, si es necesario se contacta con el funcionario dueño del activo, para solicitar conexión y poder revisar el equipo vía conexión remota.
9. Si se determina que el equipo efectivamente está infectado, se procede con el aislamiento del equipo en la red Institucional, y el seguimiento a partir de este momento se realiza en conjunto con la unidad de soporte técnico, de ser requerido se solicita la colaboración del SOC y del Equipo de Respuesta a Incidentes de la UNED.
10. Luego se procede a ingresar la información de la alerta, en el archivo de seguimiento (Sprint actual), donde se ingresa lo siguiente: (usuario, ip origen, ip destino y dispositivo).
11. Luego de realizar los pasos anteriores, nos devolvemos a la alerta y se marca en la Consola de Seguridad de Punto Final como resuelta.


	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	18 de 19

8.3.2.4 Protocol Mismatch – Detected RDP

1. Se visualiza en la consola la alerta con la indicación **Detected RDP**.
2. Se ingresa a la Consola de Seguridad de Punto Final, visualizando el equipo que presenta la alerta y se revisan los detalles del mismo. Se actualizan los productos de seguridad en caso de ser necesario y se atienden las posibles amenazas reportadas en el equipo.
3. Se da clic izquierdo sobre el evento de **RDP** y luego se selecciona **Investigar**, esto nos dirigirá a la Consola EDR, donde se visualizan más detalles de la alerta y posible incidente, como la dirección IP que intentó conectarse mediante RDP.
4. Estando en la consola **EDR**, y luego de haber revisado lo anterior, si se observa que es un falso positivo, se agrega en caso de ser necesario, la causa de la alerta en las **exclusiones**.
5. Se analiza si la dirección IP que intentó conectarse por medio de RDP, cuenta con reputación maliciosa. Si la IP es maliciosa, debe ser agregada en los sistemas de ciberdefensa de la UNED, de lo contrario pasa al punto **9**.
6. Se consulta la existencia de la dirección Ip que causo la alerta RDP, en el archivo de Excel utilizado por la USD para el control de IPs maliciosas, ubicado en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\Ip´s.xls](#)), una vez ingresada la ip en el Excel, se procede a realizar una búsqueda, aplicando un formato condicional, de valores duplicados sobre todos los datos del archivo, corroborando si esta Ip ya se encuentra en nuestra lista de bloqueos de los Firewalls.
7. Si la Ip no se encuentra en esta lista anterior, se agrega al Excel utilizado por la USD para el control de IPs maliciosas, luego se debe agregar al archivo utilizado por el personal de la **Unidad de Infraestructura Tecnológica** para realizar los bloqueos respectivos, el cual se encuentra en la siguiente ruta ([OneDrive - Universidad Estatal a Distancia\DTICUSD\2022\Proyectos\Proyecto SIEM\Sitios - Hash\BloqueosFortinet\lps.txt](#)).
8. Si se ingresó la **Ip** como se indica en el punto **7**, se debe crear un ticket de Solicitudes de atención y requerimientos, en la siguiente dirección: <https://solicitudesdtic.uned.ac.cr/>, donde se debe solicitar que se actualicen los archivos de indicadores de compromiso, para los Equipos de Seguridad Perimetral, que contienen las **direcciones IPs, archivos hash, direcciones Url y dominios a bloquear**.
9. Por último, se ingresa el detalle del ticket realizado en el control de seguimiento (Sprint actual), en el apartado de incidentes de seguridad y otros.

8.4 Gestión de alertas e incidentes de Boletines y Alertas Técnicas

- 8.4.1 Se recibe mediante correo electrónico o algún otro tipo de mensajería boletines y alertas técnicas de seguridad.

	<p>Instructivo para la atención de alertas e incidentes</p>	Código	IUNED DTIC-USD 01.01
		Dependencia	Dirección de Tecnología de Información y Comunicaciones-Unidad de Seguridad Digital
		Rige a partir de	1 de julio de 2024
		Versión	1.0
		Página	19 de 19

8.4.2 Se analizan los documentos asociados, con el fin de determinar si las recomendaciones de seguridad son aplicables a la Universidad.

8.4.3 Si las recomendaciones de seguridad son aplicables, se procede con la implementación de las mismas.

8.4.4 En algunos casos, se deben realizar tiquetes para el bloqueo de Indicadores de compromiso, en los equipos perimetrales de la Universidad o la implementación de algún aspecto asociado a buenas prácticas de seguridad.

8.4.5 De forma paralela el personal de la USD, realiza el bloqueo de indicadores de compromiso, en las diferentes soluciones de seguridad que gestiona y, en caso de ser necesario, coordina la implementación de algún aspecto asociado a buenas prácticas de seguridad.

8.4.6 El personal de la USD, coordina el reenvío de boletines e información importante, que tenga relación con Seguridad de la Información y Ciberseguridad a la comunidad universitaria.

9 Anexos

No hay.

10 Control de cambios

Fecha	Versión	Motivo del cambio	Descripción de los cambios