**UNIDAD NACIONAL DE PROTECCIÓN - UNP**

**INFORME**

**GRUPO DE GESTIÓN DE LAS TECNOLOGÍAS**

**-GGT-**



Informe de Gestión aplicación FortiEDR

Bogotá, 21 diciembre 2024

1. **OBJETIVO**

Realizar el informe mensual de gestión y control de la aplicación **FortiEDR antivirus** del mes de diciembre 2024 en la entidad UNP.

1. **ALCANCE**
2. Verificar el funcionamiento de la aplicación FortiERD del mes de diciembre 2024
3. **DEFINICIONES**
4. **FortiERD**: es una herramienta de diagnóstico y recuperación de incidentes de seguridad desarrollada por **Fortinet**. Fortinet es una compañía conocida por ofrecer soluciones de seguridad, y **FortiERD** es un componente específico dentro de su suite de herramientas para ayudar a resolver problemas relacionados con la seguridad informática, especialmente en sistemas comprometidos. FortiERD generalmente se utiliza para identificar vulnerabilidades, ataques o problemas en redes o dispositivos que utilizan las soluciones de Fortinet, y para realizar análisis forenses o recuperación de incidentes.
5. **Antivirus:** El término **Antivirus** hace referencia a un tipo de software diseñado para detectar, prevenir y eliminar programas maliciosos (malware), como virus, troyanos, gusanos y otros tipos de amenazas. Los antivirus analizan los archivos y programas de un sistema en busca de patrones sospechosos o firmas conocidas de malware. Además de la protección en tiempo real, los antivirus suelen ofrecer funciones como análisis programados, protección en la web, y actualizaciones automáticas de su base de datos para mantenerse al día con las nuevas amenazas. Aunque su nombre proviene de los "virus", hoy en día, estos programas protegen contra una variedad de amenazas cibernéticas
6. **ASPECTOS RELEVANTES**
7. Durante el mes de diciembre de 2024, **FortiEDR** en la Unidad Nacional de Protección cumplió una función esencial en el bloqueo de aplicaciones sospechosas, proporcionando una capa de seguridad continua y adaptativa, **FortiEDR** detectó y bloqueó actividades potencialmente maliciosas, como aplicaciones no confiables que podrían comprometer la seguridad del entorno. Su capacidad para monitorear en tiempo real permitió que amenazas emergentes fueran contenidas rápidamente, minimizando el impacto en la infraestructura de la organización.
8. **CONTENIDO.**
9. **Gestión de antivirus**
10. Situación analizada y gestión realizada:

Este software se mantuvo actualizado en su versión 5.2.2.577 contando con 1341 licencias para workstations y 499 para servidores con el fin de realizar la inspección y los bloqueos necesarios de programas que pudieran atentar contra la seguridad de la entidad.



Este software detecto y bloqueo aplicaciones que pueden vulnerar la seguridad de la información de la entidad como se muestra en las imágenes relacionadas a continuación.



1. **ANEXOS.**

**System\_events\_report03-Oct-2024**

**Cordialmente,**

 **Julian Camilo Bejarano Rojas**

Contratista

 GGT-OAPI

 Unidad Nacional de Protección

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

***Archívese en:***

| **VERSIÓN INICIAL** | **DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO** | **FECHA** | **VERSIÓN****FINAL** |
| --- | --- | --- | --- |
| 00 | Se creó el presente documento para orientar el diligenciamiento del Informe de Estado y Gestión de GGTST. Grupo de Gestión Tecnológica y Soporte Técnico | 29/07/2016 | 01 |
| 01 | Se realizan modificaciones al formato  | 29/08/2018 | 02 |
| 02 | Se realiza actualización del formato se hace redefinición de los ítems de contenido para hacerlo de fácil utilización en los diferentes temas tratados por el proceso. incluyendo cambio de logos, actualización del instructivo y actualización en el nombre del grupo interno de trabajo a Grupo de Gestión de las Tecnologías GGT | 12/11/2024 | 03 |

**NO IMPRIMIR**

| **INSTRUCTIVO** |
| --- |
| **CAMPO** | **DESCRIPCION DEL CAMPO** |
| Portada | Escribir el nombre del tema a desarrollar y fecha de elaboración del documento  |
| Tabla de Contenido | Realizar la identificación de los temas a tratar dentro del documento |
| Objetivo | Describir de forma clara y detallada del propósito del documento, el cual responde a las preguntas ¿para qué fue creado? o ¿con qué finalidad se creó? El objetivo inicia con un verbo en infinitivo, por ejemplo: definir, establecer, entre otros |
| Alcance | Describe la trascendencia o delimitación que se le quiere dar al documento desde donde inicia hasta donde finaliza.  |
| Definiciones | Explicar los términos usados en el texto que se consideran necesarios para un mejor entendimiento del documento |
| Aspectos relevantes | Relacionar los aspectos significativos que impactan el Estado y la Gestión Tecnológica |
| Contenido | El contenido del Informe debe describir cada uno de los temas y/o actividades desarrolladas, de manera concreta, incluyendo especificaciones técnicas de ser necesario.     Para cada uno de los eventos y/o actividades incluidas en el Informe, es necesario que se detalle:  1. Situación analizada y gestión realizada [X]
2. Riesgos asociados [Opcional]
3. Alternativas de solución planteadas [Opcional]
 |
| ANEXOS | En caso de ser requerido para claridad de los temas tratados en el informe detallar los anexos soporte del informe |
| Archívese en | Diligencie la ruta de disposición final (almacenamiento) del documento ya sea físico o Digital cumpliendo los lineamientos y directrices establecidos por Gestión Documental |