Informe de Registros de Incidentes de Seguridad

## Introducción

El presente informe detalla los incidentes de seguridad registrados en la red de datos durante el período de evaluación. El propósito es analizar los tipos de incidentes ocurridos, sus causas, las medidas de mitigación adoptadas y las recomendaciones para prevenir futuros incidentes.

[**Introducción**](#_pr1x21sxj9qi) **1**

[**1. Resumen de Incidentes Registrados**](#_ngmrvpsbu47a) **1**

[**2. Detalle de Incidentes**](#_klkuj8a74ebj) **2**

[2.1. Incidente 1: Intento de Acceso No Autorizado](#_vx24pqx7q584) 2

[2.2. Incidente 2: Malware Detectado](#_k17rp8oyhqu4) 2

[2.3. Incidente 3: Ataque de Denegación de Servicio (DoS)](#_91dtl37s18vo) 2

[2.4. Incidente 4: Phishing](#_wgm1h1ycs75x) 2

[2.5. Incidente 5: Vulnerabilidad de Software](#_dnjeoprrvzyr) 3

[**3. Análisis de Incidentes**](#_ev8t5w9va73f) **3**

[3.1. Causas Comunes](#_svy3kp41t315) 3

[3.2. Impacto](#_s1w21ufj12dj) 3

[**4. Medidas Correctivas y Preventivas**](#_diijdtwngc48) **3**

[4.1. Fortalecimiento del Firewall](#_lmm5x0nn1frm) 3

[4.2. Capacitación de Usuarios](#_cbzocsjuud34) 4

[4.3. Mejora de Mitigación de Ataques DoS](#_o30krjav4kdm) 4

[4.4. Gestión de Vulnerabilidades](#_l8i4gvvi5cso) 4

[**5. Conclusiones y Recomendaciones**](#_4pa4amqczsn9) **4**

[Conclusiones:](#_n7odp9lfnf3i) 4

[Recomendaciones:](#_yuy0ghdpr6cy) 4

## 1. Resumen de Incidentes Registrados

Durante el período de evaluación, se registraron un total de **10 incidentes** de seguridad. A continuación, se detallan los incidentes más relevantes, clasificados por su tipo y severidad.

## 2. Detalle de Incidentes

### 2.1. Incidente 1: Intento de Acceso No Autorizado

**Fecha y Hora:** 12 de abril de 2024, 14:35  
**Descripción:** Se detectó un intento de acceso no autorizado a la red desde una IP externa.  
**Medida de Mitigación:** El firewall bloqueó automáticamente la IP sospechosa.  
**Estado:** Resuelto  
**Recomendación:** Revisar y fortalecer las reglas de acceso del firewall.

### 2.2. Incidente 2: Malware Detectado

**Fecha y Hora:** 20 de abril de 2024, 09:20  
**Descripción:** El sistema de detección de intrusiones (IDS) identificó un malware en un correo electrónico recibido por un usuario.  
**Medida de Mitigación:** El correo fue puesto en cuarentena y se ejecutó un escaneo completo en el dispositivo afectado.  
**Estado:** Resuelto  
**Recomendación:** Continuar con la capacitación de usuarios sobre la identificación de correos sospechosos y reforzar las políticas de filtrado de correo.

### 2.3. Incidente 3: Ataque de Denegación de Servicio (DoS)

**Fecha y Hora:** 25 de abril de 2024, 15:45  
**Descripción:** Se detectó un ataque DoS dirigido a uno de los servidores web.  
**Medida de Mitigación:** Se configuró una regla en el firewall para bloquear el tráfico anómalo y se aplicaron medidas de tasa de limitación.  
**Estado:** Resuelto  
**Recomendación:** Implementar sistemas adicionales de mitigación de DoS, como el uso de servicios de protección en la nube.

### 2.4. Incidente 4: Phishing

**Fecha y Hora:** 1 de mayo de 2024, 11:30  
**Descripción:** Un usuario reportó un correo de phishing intentando obtener credenciales de acceso.  
**Medida de Mitigación:** Se alertó a todos los usuarios sobre el correo de phishing y se agregó la dirección de correo del remitente a la lista negra.  
**Estado:** Resuelto  
**Recomendación:** Incrementar la frecuencia de simulaciones de phishing y la capacitación sobre ciberseguridad.

### 2.5. Incidente 5: Vulnerabilidad de Software

**Fecha y Hora:** 8 de mayo de 2024, 13:10  
**Descripción:** Se descubrió una vulnerabilidad en el software de uno de los servidores críticos.  
**Medida de Mitigación:** Se aplicó un parche de seguridad proporcionado por el proveedor del software.  
**Estado:** Resuelto  
**Recomendación:** Implementar una política de actualizaciones regulares y realizar auditorías de seguridad periódicas.

## 3. Análisis de Incidentes

### 3.1. Causas Comunes

* **Acceso No Autorizado:** Fallas en la configuración del firewall y falta de segmentación adecuada.
* **Malware y Phishing:** Usuarios no suficientemente capacitados para reconocer amenazas comunes.
* **Ataques DoS:** Falta de medidas preventivas robustas para mitigar ataques volumétricos.
* **Vulnerabilidades de Software:** Parches de seguridad desactualizados y falta de un programa de gestión de vulnerabilidades efectivo.

### 3.2. Impacto

* **Disponibilidad:** Los ataques DoS afectaron temporalmente la disponibilidad de algunos servicios.
* **Integridad:** No se detectaron incidentes que comprometieran la integridad de los datos.
* **Confidencialidad:** No se registraron filtraciones de datos sensibles durante el período de evaluación.

## 4. Medidas Correctivas y Preventivas

### 4.1. Fortalecimiento del Firewall

* Revisar y actualizar las reglas de acceso.
* Implementar segmentación de red para limitar el alcance de posibles intrusiones.

### 4.2. Capacitación de Usuarios

* Realizar programas de capacitación continua sobre ciberseguridad.
* Ejecutar simulaciones de phishing para mejorar la capacidad de respuesta de los usuarios.

### 4.3. Mejora de Mitigación de Ataques DoS

* Implementar servicios de mitigación en la nube.
* Configurar reglas de tasa de limitación más estrictas en los firewalls.

### 4.4. Gestión de Vulnerabilidades

* Establecer un programa de actualización regular de software y parches de seguridad.
* Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.

## 5. Conclusiones y Recomendaciones

### Conclusiones:

* La mayoría de los incidentes fueron mitigados con éxito gracias a las medidas de seguridad implementadas.
* Es esencial continuar mejorando la capacitación de los usuarios y la gestión de vulnerabilidades para prevenir futuros incidentes.

### Recomendaciones:

* Fortalecer las políticas y procedimientos de seguridad existentes.
* Implementar una estrategia de monitoreo continuo para detectar y responder rápidamente a incidentes.
* Realizar revisiones periódicas de las medidas de seguridad para asegurar su efectividad continua.