# Diario del gestor de incidentes

## Instrucciones

A medida que avances en tu carrera, puedes utilizar esta plantilla para registrar tus hallazgos después de completar una actividad o tomar notas sobre lo que has aprendido sobre una herramienta o concepto específico. También puedes usar este diario como una forma de registrar los puntos clave sobre las diferentes herramientas o conceptos de ciberseguridad que encuentres en tu trayectoria profesional.

|  |  |
| --- | --- |
| Fecha: | 3 de diciembre de 2024 |
| Entrada: | 01 |
| Descripción: | Documentación de un incidente de seguridad en una clínica sanitaria de EE. UU. |
| Herramientas utilizadas: | No se usaron herramientas en esta etapa. |
| ¿Quién causó el incidente? | Un grupo organizado de piratas informáticos cifraron los archivos de la empresa. |
| ¿Qué ocurrió? | Los atacantes accedieron a la red de la clínica a través de correos electrónicos de phishing con archivos adjuntos maliciosos. Esto instaló un ransomware que cifró los archivos de la empresa como los registros médicos. |
| ¿Cuándo ocurrió el incidente? | El martes por la mañana aproximadamente a las 9:00 a.m. |
| ¿Dónde ocurrió el incidente? | En una clínica sanitaria en EEUU. |
| ¿Por qué ocurrió el incidente? | Los atacantes aprovecharon e hicieron un ataque de phishing para introducir ransomware en los sistemas de la clínica. |
| Reflexiones/Notas | Es importante tomar las medidas de ciberseguridad como la capacitación a los empleados para que no vuelva a ocurrir. También aplicar mecanismos preventivos como filtros de correo electrónico y herramientas de detección de malware. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |

|  |  |
| --- | --- |
| Fecha: | Registra la fecha de la entrada en el diario. |
| Entrada: | Registra el número de la entrada en el diario. |
| Descripción: | Proporciona una breve descripción de la entrada en el diario. |
| Herramientas utilizadas: | Enumera las herramientas de ciberseguridad que se utilizaron. |
| ¿Quién causó el incidente? |  |
| ¿Qué ocurrió? |  |
| ¿Cuándo ocurrió el incidente? |  |
| ¿Dónde ocurrió el incidente? |  |
| ¿Por qué ocurrió el incidente? |  |
| Reflexiones/Notas | Registra notas adicionales. |