**Diario de gestión de incidentes**

**Instrucciones**

A medida que avances en el curso, puedes utilizar esta plantilla para registrar tus observaciones después de finalizar una actividad o para tomar notas sobre lo que aprendiste acerca de una herramienta o un concepto en particular. También puedes emplear este diario para documentar las conclusiones clave sobre las distintas herramientas o conceptos de ciberseguridad que encuentres en este curso.

| **Fecha:** 23 de julio de 2024 | **Entrada:** #1 | | |
| --- | --- | --- | --- |
| Descripción | Documentación del incidente de ciberseguridad | | |
| Herramienta(s) utilizada(s) | Ninguna. | | |
| Las 5 W | * **Who (quién)**: un grupo organizado de hackers éticamente cuestionables * **What (qué)**: un incidente de seguridad de ransomware * **Where (dónde)**: en un centro de salud * **When (cuándo)**: martes a las 9:00 a. m. * **Why (por qué)**: el incidente ocurrió porque hackers éticamente cuestionables lograron acceder a los sistemas de la empresa mediante un ataque de phishing. Después de obtener acceso, los atacantes lanzaron su ransomware contra los sistemas de la compañía, cifrando archivos críticos. La motivación de los atacantes parece ser económica, ya que la nota de rescate que dejaron exigía una gran suma de dinero a cambio de la clave de descifrado. | | |
| Notas complementarias | 1. ¿Cómo podría el centro de salud evitar que se repitiera un incidente de este tipo? 2. ¿Debería pagar el rescate para recuperar la clave de descifrado? | | |

| **Fecha:**  Anota la fecha del asiento. | **Entrada:**  Anota el número de entrada. | | |
| --- | --- | --- | --- |
| Descripción | Describe brevemente la entrada. | | |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. | | |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? | | |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. | | |

| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. | | |
| --- | --- | --- | --- |
| Descripción | Describe brevemente la entrada. | | |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. | | |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? | | |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. | | |

| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. | | |
| --- | --- | --- | --- |
| Descripción | Describe brevemente la entrada. | | |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. | | |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? | | |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. | | |

| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. | | |
| --- | --- | --- | --- |
| Descripción | Describe brevemente la entrada. | | |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. | | |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? | | |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. | | |

| **Fecha:**  Anota la fecha. | **Entrada:**  Anota el número de entrada. | | |
| --- | --- | --- | --- |
| Descripción | Describe brevemente la entrada. | | |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. | | |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente? * **What**: ¿Qué sucedió? * **When:** ¿Cuándo ocurrió el incidente? * **Where:** ¿Dónde ocurrió el incidente? * **Why:** ¿Por qué ocurrió el incidente? | | |
| Notas complementarias | Agrega cualquier otra observación, pregunta o conclusión. | | |

¿Necesitas otra plantilla para las entradas?

Si deseas agregar más entradas, copia una de las tablas anteriores y pégala en la plantilla.

| Reflexiones/notas: registra las notas adicionales. |
| --- |