**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:**  19/02/24 | **Entrada:**  1 |
| Descripción | Ataque Ramsonware a clínica médica atención primaria EEUU. 9:00. Computadoras inutilizadas. Servicio detenido. Grupo hacker conocido 🡪 Nota rescate ($) 🡪 Archivos cifrados . Acceso: Correo phishing |
| Herramienta(s) utilizada(s) | Enumera las herramientas de ciberseguridad que se utilizaron. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: Grupo Hacker poco ético * **What**: Ataque ramsonware 🡪 Secuestro datos/sistemas 🡪 $ * **When:** martes a las 09:00 aprox * **Where:** Clinica médica atención primaria EE.UU * **Why:** Acceso mediante ataque correo phishing |
| Notas complementarias | Que dia acceden y localizar correo malicioso. Analizar sistema en busca de malware. Respaldo de datos para reiniciar sistemas? Servicio de cloud de respaldo? Como evitar que vuelva a sucederles? Han realizado algún pago? |

|  |  |
| --- | --- |
| **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. |

|  |  |
| --- | --- |
| **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. |