**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:**  Anota la fecha. | **Entrada:**  Martes alrededor de las 09:00 am. |
| Descripción | Entrada #1 Problema de Hacking por Correo. |
| Herramienta(s) utilizada(s) | Ninguna. |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: Un grupo organizado de hackers éticamente cuestionables. * **What**: Un incidente de seguridad “Ramsonware”. * **When:** Martes a las 09:00 am. * **Where:** En el centro de salud. * **Why:** El incidente ocurrió por que Hackers éticamente cuestionables, lograron acceder a los sistemas de la empresa mediante ataque phishing. Después de obtener acceso, los atacantes lanzaron un 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, exige 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. | **Entrada:**  **Miércoles, 20 julio 2022 09:30:14** |
| Descripción | Entrada #2 Problema de Hacking por correo |
| Herramienta(s) utilizada(s) | **Portal web Virus Total** |
| Las 5 W | Determina las 5 W de un incidente.   * **Who**: ¿Quién causó el incidente?: Grupo de hackers Eticamente Cuestionables. * **What**: ¿Qué sucedió?: Un incidente de seguridad “Ransomware”   **When:** ¿Cuándo ocurrió el incidente?: miércoles, 20 de julio de 2022 09:30:14 a.m.   * **Where:** ¿Dónde ocurrió el incidente? : En la plantilla de **ticket Alerta** * **Why:** ¿Por qué ocurrió el incidente?: El incidente ocurrió por que Hackers éticamente cuestionables, lograron acceder a los correos de la empresa mediante ataque phishing. Después de obtener acceso, los atacantes lanzaron un correo electrónico contra el usuario [hr@inergy.com](mailto:hr@inergy.com) ofreciendo interés por el puesto de la plaza “Ingenero de infraestructura”. La motivación de los atacantes se desconoce, ya envían solamente en el adjunto un archivo de nombre filename="bfsvc.exe" aparente Ransomware. |
| Notas complementarias | Eliminar el correo y enviar al remitente a correo no deseado, por parte del equipo de TI se creará regla anti Spam para ese tipo de dominio. |

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