Fecha del Reporte: Seleccione una fecha.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Incidente** | | | | |
| **Fecha y Hora de Detección:**  Seleccione la fecha y la hora de descubrimiento del incidente | | **Nombre y dependencia de la Persona que Detectó el Incidente:** | | |
| **Descripción Detallada:**  Realice una descripción detallada de lo sucedido, teniendo en cuenta los siguientes interrogantes**: Quién, Cómo, Cuándo, Dónde, Por qué y Para qué** | | | | |
| **Método de Detección:**  Describa cómo fue detectado el incidente. Ej.; reportado por usuario, alerta de herramientas de monitoreo | | | | |
| **Contención:**  Describa las actividades realizadas para contener el incidente | | | | |
| **Clasificación del Incidente: Seleccione la clase y tipo de incidente.**  **Malware:** Elija un elemento.  **Disponibilidad:** Elija un elemento.  **Obtención de Información:** Elija un elemento.  **Intrusiones:** Elija un elemento.  **Compromiso de Información:** Elija un elemento.  **Fraude:** Elija un elemento.  **Contenido Abusivo:** Elija un elemento.  **Política de Seguridad:** Elija un elemento.  **Otros:**  Escriba la clasificación del incidente, si no se encuentra en las listas desplegables | | | | |
| **Servicios Afectados** | | | | |
|  | | | | |
| **Descripción Detallada del Activo o Servicio Afectado:**  Realice una descripción detallada del activo como: tipo de hardware, sistema operativo, tipo de licenciamiento, motor de base de datos, buzón de correo electrónico, servidor web, dirección ip, proveedor de servicio de internet. etc | | | | |
| **Debido al Incidente:** | Alguien no autorizado tuvo acceso a la información: | | |
| Se ha impedido algún usuario el acceso a la información: | | |
| Se ha borrado, modificado y eliminado alguna información: | | |
| **Impacto del incidente:** | | | |
| **Causa Raíz:**  Escriba cual fue la causa raíz, por la cual se presentó el incidente. | | | |
| **Realizo Plan de Mejoramiento:** | | | |
| **Actividades Mitigación/Contención y radicación de Causa Raíz:**  Escriba las actividades de manera secuencial, que permitirán eliminar y/o controlar la causa raíz. | | | |
| **Después de realizar la contención el incidente se encuentra:** | | | **El incidente ya se había presentado:** |
| **Duración del Incidente: Días**   **Horas Minutos** | | | |
| **Observaciones:**  Escriba cualquier otra información relacionada con el incidente, que no se encuentre contenida en el formato. Por ejemplo, el número de caso generado en la herramienta de mesa de ayuda u otras plataformas de notificación a terceros. | | | |

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Nombre del administrador del Activo de Información** | **Firma** |