|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Datos de Contacto de la Entidad** | | | | | | | | | | | |
| **Nombre de la Entidad:** Escriba el nombre de la entidad | | | | | | | | | | | |
| **Dirección:** Escriba la dirección física de la sede | | | | | | | | | | **Sede:** Escriba el nombre de la sede | |
| **Sector:** Escribir el nombre del sector al cual pertenece | | **Ciudad:** Escriba la ciudad donde se encuentra la sede | | | | | | | **Departamento:** Escriba el Departamento al que pertenece la sede | | |
| **Nombre de Quien Reporta:** Escriba el nombre y apellidos de la persona que reporta el incidente | | | | | | | | | | | |
| **Cargo:** Escriba el cargo de la persona que reporta el incidente | | | **Número Contacto:**  **Fijo:** Número Fijo.  **Ext** Número de la extensión **Celular:** Número celular | | | | | | | | |
| **Correo Electrónico:** Escriba su correo de corporativo | | | | | | | | **Skype:** Escriba su usuario de Skype | | | |
| **Incidente** | | | | | | | | | | | |
| **Fecha y Hora del descubrimiento:**  Escriba la fecha y la hora de descubrimiento del incidente | | | | | **Nombre de la Persona que Detectó el Incidente:**  Escriba el nombre y apellidos de la persona que detectó el incidente | | | | | | |
| **Fecha y Hora de Detección:**  Escriba la fecha y la hora de inicio del incidente | | | | | **Nombre del administrador del Activo Informático:**  Escriba el nombre y apellidos de la persona que administra el activo informático – Servidor, DB, Aplicación, Portal, etc. | | | | | | |
| **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:**  Escriba como fue detectado el incidente | | | | | | | | | | | |
| **Acciones Realizadas:**  Escriba qué actividades ha realizado para contener el incidente | | | | | | | | | | | |
| **Acciones Pendientes:**  Escriba qué actividades planeadas para la contención del incidente, están pendiente de ejecutar | | | | | | | | | | | |
| **Clasificación del Incidente: Seleccione la clase y tipo de incidente.**  **Malware:** Elija un elemento.  **Disponibilidad:** Elija un elemento.  **Obtención de Información:** Elija un elemento.  **Instrucciones:** 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 | | | | | | | | | | | |
| **La respuesta al incidente fue efectiva:** | | | | **Duración del Incidente: Días**   **Horas Minutos** | | | | | | | |
| **Se Identificó el Responsable:** | | | | | | **Nombre:** Escriba el nombre y apellidos de la persona responsable | | | | | **Área:** Escriba el nombre del área, al cual pertenece la persona responsable |
| **Hardware y Software Afectado** | | | | | | | | | | | |
| **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 a 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. | | | | | | | | | | | |
| **Realizó Plan de Mejoramiento:** | | | | | | | | | | | |
| **Acciones Planificadas para Solución Causa Raíz:**  Escriba las actividades de manera secuencial, que permitirán eliminar y/o controlar la causa raíz. | | | | | | | | | | | |
| **Lecciones Aprendidas:**  Escriba las lecciones aprendidas generadas en las etapas antes, durante y después del incidente | | | | | | | | | | | |
| **Después de realizar la contención y actividades de mitigación el incidente se encuentra:** | | | | | | | **El incidente ya se había presentado:** | | | | |
| **Otros:**  Escriba cualquier otra información relacionada con el incidente, que no se encuentre contenida en este formato. | | | | | | | | | | | |