|  |  |
| --- | --- |
| REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | |
| FECHA Y HORA REPORTE DE INCIDENTE |  |
| LUGAR DEL INCIDENTE |  |
| DETALLES DE PERSONA QUE REPORTA/IDENTIFICA INCIDENTE | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| DESCRIPCION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION: | | | |
| ¿Qué Sucedió?: |  | | |
| ¿Cómo Sucedió?: |  | | |
| ¿Por qué Sucedió?: |  | | |
| Consideraciones Iniciales sobre componente(s) / Activo(s) de información afectados?: |  | | |
| ¿Impactos adversos para la Entidad?: | Si: | No: | Cual: |
| ¿Se identifica Vulnerabilidad alguna?: | Si: | No: | Cual: |
| ¿Se identifica responsable del Incidente?: | Si: | No: | Cual: |
| ESTADO DEL INCIDENTE | Sucediendo\_\_\_\_ Sucedió \_\_\_ Sucede nuevamente \_\_\_\_ | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CATEGORIA DEL INCIDENTE SE SEGURIDAD DE INFORMACION:** | | | | | |
| **¿Incidente de Seguridad de la Información Real?** |  | |  | **Incidente de Seg. ¿Información Sospechado?** |  |
| **Desastre natural:** | | | | | |
| **Terremoto** |  | |  | **Inundación** | |  | | --- | |  | |
| **Descarga Electromagnética** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Conflicto social:** | | | | | |
| **Disturbio** |  | |  | **Ataque Terrorista** |  |
| **Guerra** |  | |  | **¿Otro? Especifique:** |  |
| **Daño físico:** | | | | | |
| **Incendio** | |  | | --- | |  | | |  | **Agua** | |  | | --- | |  | |
| **Electrostática** |  | |  | **Ambiente Nefasto (Contaminación, polvo, corrosión)** |  |
| **Destrucción de Equipo** |  | |  | **Destrucción de Medios** |  |
| **Robo de Equipos** |  | |  | **Pérdida de Medios** |  |
| **Alteración de Equipo** |  | |  | **Alteración de Medios** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Falla en la infraestructura:** | | | | | |
| **Fallas en la Alimentación Eléctrica** |  | |  | **Falles en las Redes** |  |
| **Fallas en el Aire Acondicionado** |  | |  | **Fallas en el suministro de Agua** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Falla técnica:** | | | | | |
| **Falla en el Hardware** |  | |  | **Mal Funcionamiento del Software** |  |
| **Sobrecarga (saturación de capacidad de los sistemas)** | |  | | --- | |  | | |  | **Violación de Mantenibilidad** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |  | | --- | |  | | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Malware:** | | | | | |
| **Gusano de Red** |  | |  | **Troyano** |  |
| **Botnet** | |  | | --- | |  | | |  | **Ataques combinados** |  |
| **Página WEB con código malicioso incrustado** |  | |  | **Sitio de alojamiento con código malicioso** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Ataque técnico:** | | | | | |
| **Escaneo de Redes** | |  | | --- | |  | | |  | **Aprovechamiento de Vulnerabilidades** |  |
| **Aprovechamiento de Puertas traseras** | |  | | --- | |  | | |  | **Intentos de acceso** |  |
| **Interferencia** | |  | | --- | |  | | |  | **Denegación de Servicio** |  |
| **¿Otro?**  **Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |  | | --- | |  | | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Violación de reglas:** | | | | | |
| **Uso no autorizado de recursos** | |  | | --- | |  | | |  | **Violación a los Derechos de Autor** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Puesta en peligro de las funciones:** | | | | | |
| **Abuso de Derechos** |  | |  | **Falsificación de Derechos, denegación de acciones** |  |
| **Operaciones Incorrectas** |  | |  | **Violación de la Disponibilidad del Personal** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Puesta en peligro de la información:** | | | | | |
| **Interceptación** | |  | | --- | |  | | |  | **Espionaje** |  |
| **Chuzada de Teléfonos** |  | |  | **Divulgación** |  |
| **Enmascaramiento** |  | |  | **Ingeniería Social** |  |
| **Phishing de Redes** |  | |  | **Robo de Datos** |  |
| **Pérdida de Datos** |  | |  | **Alteración de Datos** |  |
| **Error de Datos** |  | |  | **Análisis de Flujo de Datos** |  |
| **Detección de posición** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **Contenidos peligrosos:** | | | | | |
| **Contenido Ilegal** |  | |  | **Contenido que provoca pánico** |  |
| **Contenido Malicioso** |  | |  | **Contenido Abusivo** |  |
| **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | |  | **¿Otro? Especifique\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| **DETALLE DE LA SOLUCION DEL INCIDENTE DE SEGURIDAD DE LA INFORMACION:** | | | | | |
| **Fecha y Hora de la investigación del incidente:** |  | | | | |
| **Nombre(s) del(los) investigador(es) del incidente:** |  | | | | |
| **Fecha y Hora de la Finalización del incidente** |  | | | | |
| **Fecha y Hora de la Finalización del impacto** |  | | | | |
| **Descripción de las acciones tomadas para resolver el incidente de SI:** | | | | | |
|  | | | | | |
| **Descripción de las acciones planeadas para resolver el incidente de SI:** | | | | | |
|  | | | | | |
| **Acciones pendientes para resolver el incidente de SI:** | | | | | |
|  | | | | | |
| **Conclusiones:** | | | | | |
|  | | | | | |
| **Lecciones aprendidas del incidente de SI:** | | | | | |
|  | | | | | |
|  | | | | | |
| **ELABORO** | | **REVISO** | | | |
| **Nombre:** | | **Nombre:** | | | |
| **Área:** | | **Área:** | | | |
| **Rol:** | | **Rol:** | | | |
| **APROBO** | | | | | |
| **Nombre:** | | **Área:** | | | |
| **Cargo:** | | **Fecha:** | | | |