|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **FORMATO PARA REPORTE DE INCIDENTES DE SEGURIDAD IDEAM** | | | | |
| Fecha de notificación: | | | Hora notificación: | |
| Estado incidente: | | | | |
| **DATOS DE LA PERSONA QUE NOTIFICA[[1]](#footnote-1)** | | | | |
| **Apellidos y Nombres:** | | | | |
| Área: | | | Correo Electrónico: | |
| Teléfono Interno: | | | Teléfono particular: | |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | | |
| **Fecha en que se observó:** | | | **Hora en que se observó:** | |
| **Marque con una X las opciones que considere aplicables:** | | | | |
| Uso indebido de información crítica |  | | Ingeniería social, fraude o phishing. |  |
| Uso prohibido de un recurso informático o de red del IDEAM. |  | | Modificación no autorizada de un sitio o página web del IDEAM. |  |
| Divulgación no autorizada de información personal. |  | | Eliminación insegura de información. |  |
| Intrusión física. |  | | Modificación o eliminación no autorizada de datos. |  |
| Destrucción no autorizada de información. |  | | Anomalía o vulnerabilidad técnica de software. |  |
| Robo o pérdida de información. |  | | Amenaza o acoso por medio electrónico. |  |
| Interrupción prolongada en un sistema o servicio de red. |  | | Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.) |  |
| Modificación, instalación o eliminación no autorizada de software. |  | | Robo o pérdida de un recurso informático del IDEAM. |  |
| Acceso o intento de acceso no autorizado a un sistema informático. |  | | Otro no contemplado. Describa: |  |
| **INFORMACIÓN SOBRE EL INCIDENTE** | | | | |
| **Describa el incidente:** | | | | |
|
|
|
|
|
|
|
| Si el incidente: •Se trata de una infección por código malicioso, detalle en lo posible el nombre del virus detectado por el programa antivirus. •Se trata de una anomalía o vulnerabilidad técnica, describa la naturaleza y efecto de la anomalía en términos generales, las condiciones en las cuales ocurrió la vulnerabilidad, los síntomas del problema y mensajes de error que aparezcan en pantalla. •Se trata de un caso de fraude mediante correo electrónico (phishing), no elimine el mensaje de correo, contáctese en forma telefónica con Mesa de Ayuda o a través de correo electrónico | | | | |
| Describa brevemente del incidente: | | | | |
| El incidente aún está en progreso: SI ( ) No ( ) | | | | |
| Detalle de las personas que han accedido al sistema afectado desde la presentación del incidente: | | | | |
|  | | | | |
|
| Sistema, computadora o red afectada: | | | | |
|  | | | | |
|
| Localización Física: | | | | |
|  | | | | |
|
| Describa brevemente la información contenida en el sistema: | |  |  | |
|  | | | | |
|
| ¿Existe copia de respaldo de los datos o software afectado? | | Si ( ) No ( ) | | |
| ¿El recurso afectado tiene conexión con la red del IDEAM? | | Si ( ) No ( ) | | |
| ¿El recurso afectado tiene conexión a Internet? | | Si ( ) No ( ) | | |
| Sistema operativo: | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **HISTORIAL DE CAMBIOS** | | | | | | | |
|  |  |  |  |  |  |  |  |
| VERSIÓN | | | FECHA | | DESCRIPCIÓN | | |
| 01 | | | 27/03/2017 | | Creación del Documento | | |
| 02 | | | 23/04/2018 | | Actualización del documento | | |
|  |  |  |  |  |  |  |  |
| ELABORÓ: Luis Alejandro Pinilla Peralta Oficial de Seguridad de la Información | | | REVISÓ: Eduardo Ramírez Acosta Oficina Informática | | | APROBÓ: Leonardo Cardenas Chitiva Jefe Oficina Informática | |

1. [↑](#footnote-ref-1)