**REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| INFORMACIÓN GENERAL. | | | | | | |
| Nombres y Apellidos: | |  | | | | |
| Vinculación: | |  | | | | |
| Área/Dependencia: | |  | | | | |
| Correo Electrónico: | |  | | | | |
| Teléfono: | |  | | | | |
| Celular: | |  | | | | |
| ID Incidente | |  | | | | |
| INFORMACIÓN SOBRE EL INCIDENTE | | | | | | |
| Fecha en que se observó | |  | | | | |
| Hora en que se observó | |  | | | | |
| Lugar en que se observo | |  | | | | |
| **Marque con una X las opciones que considere aplicables.** | | | | | | |
| 1 | Uso indebido de información critica. | |  | 2 | Ingeniería social, fraude o phishing. |  |
| 3 | Uso prohibido de un recurso informático la red de la Universidad. | |  | 4 | Modificación no autorizada de un sitio o página web de la Universidad. |  |
| 5 | Divulgación no autorizada de información personal. | |  | 6 | Eliminación insegura de información. |  |
| 7 | Intrusión física. | |  | 8 | Modificación o eliminación no autorizada de datos. |  |
| 9 | Eliminación no autorizada de información. | |  | 10 | Anomalía o vulnerabilidad técnica de software. |  |
| 11 | Robo o pérdida de información. | |  | 12 | Amenaza o acoso por medio electrónico. |  |
| 13 | Interrupción prolongada en un sistema o servicio de red. | |  | 14 | Ataque o infección por código malicioso (virus,gusanos, troyanos, etc.) |  |
| 15 | Modificación, instalación o eliminación no autorizada de software. | |  | 16 | Robo o pérdida de un recurso informático (componentes de Hardware y programas) de la Universidad. |  |
| 17 | Acceso o intento de acceso no autorizado a un sistema informático. | |  | 18 | Otro no contemplado.  Describa: |  |
|  |  | |  |  |  |  |
| **Describa el incidente (aporte detalles completos y concretos a las opciones seleccionadas).** | | | | | | |
|  | | | | | | |
| **Cómo detectó el incidente:** | | | | | | |
|  | | | | | | |
| **El incidente aún está en progreso:**  SI[ ] NO[ ] | | | | | | |
| **Tiempo estimado de duración del incidente:** | | | | | | |
| **Detalle las personas que han accedido al sistema afectado desde que se detectó el incidente:** | | | | | | |
| Relacione soportes, si los tiene (archivos, rutas, documento impreso, copia de mensajes, otros). | | | | | | |
| INFORMACIÓN SOBRE EL INCIDENTE | | | | | | |
| **Sistema/computador afectado:** | | | | | | |
|  | | | | | | |
| **Ubicación (física, lugar web):** | | | | | | |
|  | | | | | | |
| **Describa brevemente la información contenida en el sistema / computador/ medio físico:** | | | | | | |
|  | | | | | | |
| **¿Existe copia de respaldo de los datos o software afectado?**  SI[ ] NO[ ] | | | | | | |
| **¿El recurso afectado tiene conexión con la red de la Universidad?**  SI[ ] NO[ ] | | | | | | |
| **¿El recurso afectado tiene conexión a Internet?**  SI[ ] NO[ ] | | | | | | |
| **Sistema operativo:** | | | | | | |
| OTROS CONTACTOS | | | | | | |
| **Nombres e información de contacto de otras personas que pueden tener información para asistir en la investigación del incidente:** | | | | | | |
| Apellido y nombres:  Datos de contacto: | | | | | | |
| Apellido y nombres:  Datos de contacto: | | | | | | |
| Apellido y nombres:  Datos de contacto: | | | | | | |