Marque con una X donde se presenta el incidente – Oficial de seguridad de la información.

|  |  |  |
| --- | --- | --- |
| **Elementos de comunicación** | | |
| 1 | Información de contactos de los miembros del equipo de atención de incidentes y otras personas dentro y fuera de la entidad (contacto primario y contacto alterno) que pueden servir como apoyo en el manejo del incidente: Técnicos, Abogados, representantes de organismos de seguridad |  |
| 2 | Mecanismo para reporte de incidentes Definición de los mecanismos que se emplearan para el reporte de incidentes, teléfonos, correos electrónicos, formatos online que puedan utilizar los usuarios para reportar los posibles incidentes [deseable contar con un mecanismo para recibir reportes de manera anónima] |  |
| 3 | Teléfonos celulares o radios de comunicaciones Disponer de teléfonos o radios que sean portados por los miembros del equipo de gestión de incidentes en horas de oficina y fuera del horario de trabajo. [deseable contar con un teléfono o radio de servicio que pueda ser rotado por el ingeniero de servicio en horas no hábiles] |  |
| 4 | Área de manejo de crisis Oficina desde la cual se puedan gestionar de manera centralizada las actividades de manejo del incidente. [si no se cuenta con un área permanente se debería definir un mecanismo para reservar una oficina cuando se requiera la atención de incidentes] |  |
| 5 | Área de almacenamiento de evidencias Área física en donde se almacenarán, preservaran y custodiarán las evidencias que se recolecten durante el manejo del incidente |  |
| **Software y Hardware para manejo de Incidentes** | | |
| 1 | Estaciones de trabajo para montaje de un laboratorio para pruebas de herramientas forenses. [si no se cuenta con estaciones suficientes se pueden establecer acuerdos o contratos para tener disponibilidad de laboratorios forenses bajo demanda] |  |
| 2 | Medio de almacenamiento (CD, DVD, BlueRay, discos USB, discos externos) |  |
| 3 | Impresora portátil. Para imprimir evidencias de equipos que no estén conectados a la red |  |
| 4 | Analizadores de protocolos o sniffer |  |
| **Recursos para mitigación de incidentes** | | |
| 1 | Medios de almacenamiento |  |
| 2 | Parches de seguridad |  |
| 3 | Imágenes de respaldo de sistemas operacionales, servidores y sistemas de información. |  |