SEGURIDAD INFORMATICA

CONCEPTOS BASICOS

FUNDAMENTOS

- La **información** se ha convertido en uno de los activos más importantes dentro de cualquier organización y dicho activo debe ser debidamente protegido.
- Existen amenazas externas e internas, las cuales ocasionan que la organización corra el riesgo de que la información sea utilizada de manera maliciosa para obtener ventajas o que sea manipulada ocasionando la perdida y la duda sobre su veracidad.

FUNDAMENTOS

- Se hace necesario garantizar la continuidad comercial, minimizar posibles daños y maximizar el retorno sobre las inversiones y las oportunidades de negocio.
- Mediante el uso de internet cada vez más compañías comparten sus recursos en la red de manera que empleados y proveedores puedan estar en línea con sus sistemas de información, esto ocasiona que se incrementen las posibilidades de que la **información** pueda estar comprometida.

FUNDAMENTOS

Datos	➔	materia prima que procesada produce información
Información	➔	recurso de alto valor para una empresa
Seguridad	➔	certeza, falta de riesgo o contingencia
Amenaza	➔	riesgo de intromisión externa e interna
Soporte	➔	la información puede existir en mucha formas

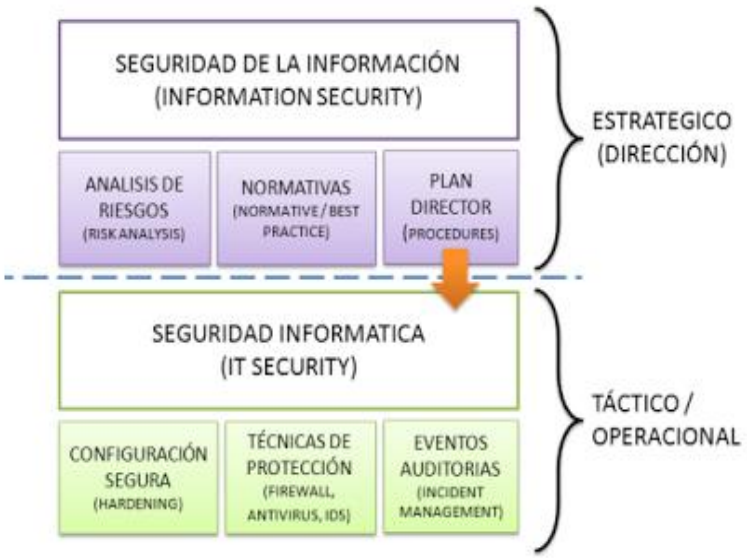
CONCEPTOS GENERALES

- La **Seguridad Informática** (S.I.) es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer **condiciones seguras y confiables** para el procesamiento de datos en sistemas informáticos.

CONCEPTOS GENERALES

- Los 3 elementos principales a proteger en cualquier sistema informático son el **hardware**, el **software** y los **datos**.
- La Seguridad Informática es la parte operativa de la Seguridad, es decir, las medidas técnicas que aseguran la Seguridad de la Información.

CONCEPTOS GENERALES



CARACTERISTICAS

- A ser preservadas
  - » Confidencialidad
  - » Integridad
  - » Disponibilidad
  - » Irrenunciabilidad
  - » Autenticidad

CARACTERISTICAS

- **Confidencialidad** : Garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella, asegurando la privacidad de la información.

  - Las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

  - Es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, ordenadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

CARACTERISTICAS

- **Integridad**: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento, brindando la validez y consistencia necesarias a la información

  - Las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

  - Es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, ordenadores y procesos comparten la misma información.

CARACTERISTICAS

- **Disponibilidad**: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, en referencia a la continuidad requerida.

  - Las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

  - Es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

CARACTERISTICAS

- **Irrenunciabilidad** : Garantizar que exista el establecimiento claro sobre la ejecución de un determinado acto, que permita determinar que cada acción pueda ser inequívocamente ligada a su autor.

  - Las herramientas de Seguridad Informática deben permitir el no repudio o irrenunciabilidad con respecto a la participación de las partes en una comunicación.

  - Existen 2 posibilidades:

    - No repudio en origen: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo el receptor recibe una prueba infalsificable del envío.

    - No repudio de destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

CARACTERISTICAS

- **Autenticidad**: La información debe ser reflejo de los hechos reales, debe corresponder a la verdad en cuanto a su elaboración o pertenencia.

  - Las herramientas de Seguridad Informática deben permitir verificar que un documento ha sido elaborado o pertenece a quien el documento dice.

  - Se debe identificar el generador de la información, usualmente se aplica el uso de cuentas de usuario y contraseñas de acceso.

OBJETIVO

- La **seguridad** siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma.
- La **seguridad** podría ser catalogada como la ausencia de riesgo (contratiempo o desgracia que ocasione perjuicio o daño), involucra cuatro acciones
  - Prevención del riesgo
  - Transferir el riesgo
  - Mitigar el riesgo
  - Aceptar el riesgo

OBJETIVO

- La principal tarea de la **seguridad informática** es la de **minimizar** los **riesgos**.
- El riesgo proviene de muchas partes, puede ser en la entrada de datos, en el medio que transporta la información, el hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando.

OBJETIVO

- os riesgos provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

OBJETIVO

- La Seguridad Informática se debe aplicar sobre:
  - Los usuarios
  - La información, y
  - La infraestructura
- Los **usuarios** son considerados como el eslabón más débil de la cadena, su control es muy difícil, un usuario puede cometer errores, olvidos, accidentes y este suceso puede significar la pérdida de información, en muchos casos el sistema y la información deben ser protegidos del mismo usuario.

OBJETIVO

- La **información** se considera el principal activo de la seguridad informática, ya que es lo que se desea proteger y lo que tiene que estar a salvo.
- La **infraestructura** es la más controlada, pero eso no implica que sea laque corre menos riesgos. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, robo del equipo, desastres naturales y otros.

MECANISMOS PREVENTIVOS

- Consiste en una serie de revisiones periódicas, algunos cambios o mejoras de diferentes aspectos que pueden ser de hardware, software o de cualquier elemento involucrado en los sistemas y procesos.
- Los mecanismos preventivos en realidad son a largo plazo y por esta razón son considerados por la mayoría como una pérdida de tiempo y dinero.
- El obstáculo más fuerte a la que se enfrenta una empresa al querer aplicar los mecanismos preventivos, es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

MECANISMOS PREVENTIVOS

- Elementos:
  - **El respaldo de información**: Es uno de los procesos más comunes que se pueden realizar en las compañías y que gozan de cierta aceptación general. Entre los factores a considerar se tiene los formatos de archivos se tienen, por ejemplo, MP3, archivos de texto, bases de datos, imágenes y vídeos, etc.
  - **Horario de respaldo**: Otro reto es a qué hora se puede hacer el respaldo, es común seleccionar las horas de menos tráfico.

MECANISMOS PREVENTIVOS

- **Control de los medios**: El tener acceso a respaldos es algo de alto riesgo, se puede robar la información, manipular, perder, así que, el respaldo es una solución, pero también es otro problema que se debe resolver.
- **La compresión de la información**: No toda la información se puede comprimir, pero existe alguna que, sí lo necesita, así que se deben hacer las valoraciones respectivas.

MECANISMOS PREVENTIVOS

- Otros ejemplos de proceso que se tienen en el mecanismo preventivo son:
  - Actualización de sistemas
  - Antivirus
  - Firewall
  - Navegación por internet
  - Contraseñas
  - Accesos remotos.

MECANISMOS CORRECTIVOS

- Se aplican después de que algo sucedió y la función principal es corregir las consecuencias.
- Entre las características que tienen los mecanismos correctivos normalmente son muy caros, esto se debe a que el problema ya se lo tiene encima y no se puede tenerlo durante mucho tiempo.
- El tiempo es limitado y se vuelve algo muy apremiante en estos casos.

MECANISMOS CORRECTIVOS

- Pasos:
  - **Catalogación y asignación de problemas**: Se hace un catálogo de los problemas a los que se pueden enfrentar, detectar y clasificar para poder abordar las situaciones y buscar solución.
  - **Análisis del problema**: Analizar el problema que se ha presentado, en muchos casos esta parte se realiza por los expertos, ya no, por las personas involucradas en el problema.

MECANISMOS CORRECTIVOS

- Pasos:
  - **Análisis de la solución**: Analizar la propuesta de la solución, se ha cometido un error y se tiene un impacto, así que la solución tiene que estar bien planteada y ejecutada. Antes de empezar a realizar los cambios, actualizaciones y movimientos se debe tratar de analizar y de predecir qué es lo que va a suceder.
  - **La documentación**: Este componente es vital, ya que los cambios que se hacen probablemente son algo rápido y que involucraron muchos recursos, así que la documentación es muy importante. En caso de encontrar algún problema se puede consultar la documentación para detectar si la solución era correcta.

MECANISMOS DETECTIVOS

- Los mecanismos de detección son los más complejos y son en los que se necesita tener alto grado de conocimientos técnicos.
- Los mecanismos de detección parten de que se tiene la idea de que un atacante es capaz de violar la seguridad y puede haber realizado una intrusión total o parcial a un determinado recurso.
- Siempre que se trabaja en los mecanismos de detección se tiene la premisa en mente, se debe trabajar como si lo que se fuera a encontrar es lo peor y se debe estar preparados para la peor de las situaciones posibles.

MECANISMOS DETECTIVOS

- Objetivos:
  - Poder detectar el punto exacto del ataque para poder llegar a una solución y recuperarse del mismo, pero no siempre es posible esto, depende de los problemas que se afrontan.
  - Detectar la actividad que se considera sospechosa y conocer lo sucedido, ya que si no se encuentra donde fue el ataque, lo mínimo que se necesita es saber qué fue lo que sucedió y partir de esa parte.

MECANISMOS DETECTIVOS

- Mecanismos:
  - **Revisión de patrones de acceso**: Analizar los accesos y tratar de encontrar si se está manejando un patrón, por ejemplo, acceso a determinadas horas o el mismo usuario haciendo accesos a la misma sección o módulo.
  - **Revisión de transacción**: La revisión de transacciones es un método muy rápido para detectar subidas o bajadas de información. si se logra encontrar una transacción es como encontrar el objetivo del atacante lo cual es muy valioso.

MECANISMOS DETECTIVOS

- Mecanismos:
  - **Bloqueo automático**: Si se encuentra el problema y no se cuenta con un mecanismo de bloqueo de emergencia, el atacante podrá seguir haciendo daño. Algunos de los mecanismos de bloqueo comunes son los de paro absoluto, el bloqueo del sistema completo, es algo drástico, pero en muchas ocasiones se considera la mejor opción.

FUNDAMENTOS DE SEGURIDAD

- Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener la información, de su importancia, integridad y disponibilidad de la información para sacarle el máximo rendimiento con el mínimo riesgo.
- La seguridad está fundamentada por 3 pilares, pero puede haber más que puedan fundamentar a la seguridad, en este caso, si alguno de los lados es débil se perderá seguridad o usabilidad, si falta alguno de los lados la organización queda expuesta a ataques.

FUNDAMENTOS DE SEGURIDAD

- **Confidencialidad**: La confidencialidad consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas, para garantizar la confidencialidad se recurre principalmente a tres recursos:

FUNDAMENTOS DE SEGURIDAD

- **Autenticación de usuarios**: Sirve para identificar qué quién accede a la información es quien dice ser.
- **Gestión de privilegios**: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizado y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.
- **Cifrado de información**: El cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma legible a una no legible y es aplicable tanto a la información que está siendo transmitida como a la almacenada

FUNDAMENTOS DE SEGURIDAD

- **Integridad**: Consiste en asegurarse de que la información no se pierde ni se ve comprometida voluntaria e involuntariamente, el hecho de trabajar con información errónea puede ser tan nocivo como perder la información, ocasionando toma de decisiones equivocadas.
- Para garantizar la integridad de la información se debe considerar lo siguiente:

FUNDAMENTOS DE SEGURIDAD

- **Monitorear el tráfico de red** para descubrir posibles intrusiones.
- **Auditar los sistemas** para implementar políticas de auditorías que registre quien hace que, cuando y con qué información.
- **Implementar sistemas de control de cambios**, algo tan sencillo como por ejemplo comprobar los resúmenes de los archivos de información almacenados en sistema para comprobar si cambian o no.
- **Copias de seguridad**, que en caso de no conseguir impedir que se manipule o pierda la información permitan recuperarla en su estado anterior.

FUNDAMENTOS DE SEGURIDAD

- **Disponibilidad:** La información para resultar útil y valiosa debe estar disponible para quien la necesita, se debe implementar las medidas necesarias para que tanto la información como los servicios estén disponibles. Ej. denegación de servicio o correo electrónico utilizado para lanzar spam y en consecuencia figurar en listas negras impidiendo la recepción de mensajes.
- Para este propósito se implementan políticas de control como:

FUNDAMENTOS DE SEGURIDAD

- El acuerdo de nivel de servicio o (SLA Service Level Agreement).
- Balanceadores de carga de tráfico para minimizar el impacto de DDoS (Distributed Denial of Service).
- Copias de seguridad para restauración de información perdida.
- Disponer de recursos alternativos a los primarios.
- Elaborar varias normas y procedimientos.
- Definición de acciones que deben emprender las personas.
- Definición del perímetro que se va a afectar.

SEGURIDAD INFORMATICA

ATENCION DE INCIDENTES

TERMINOLOGIA

- **Evento de Seguridad informática**: Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad o una situación previamente desconocida que pueda ser relevante para la seguridad [ISO 18044].
- Un Evento de Seguridad Informática no es necesariamente una ocurrencia maliciosa o adversa.

TERMINOLOGIA

- **Incidente de Seguridad informática**: Es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita.
- También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).
- Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [ISO 18044]

DEFINICION

- Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

DEFINICION

- Se entienden por incidentes de seguridad las violaciones de acceso, intento de acceso, uso inadecuado, divulgación, modificación o destrucción no autorizada de información, cambios no controlados en el sistema, errores humanos, incumplimiento de las políticas de seguridad, pérdida o robo de información o recurso tecnológico, mal funcionamiento, manipulación, sabotaje, virus, códigos maliciosos, negación del servicio, violaciones de confidencialidad, entre otros.

DEFINICION

- El Convenio sobre la Ciberdelincuencia del Consejo de Europa, categoriza los incidentes de seguridad física informática en términos de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

- Las categorías establecidas en este Convenio son las siguientes:

DEFINICION

- 1. **Acceso ilícito**: Acceso ilegítimo a la totalidad o a una parte de un sistema informático.
- 2. **Interceptación ilícita**: Interceptación ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.

DEFINICION

- 3. **Interferencia en los datos**: Comisión ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
- 4**. Interferencia en el sistema**: Obstaculización grave e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

DEFINICION

- 5. **Abuso de los dispositivos**: Producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
  - un **dispositivo**, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos en las anteriores categorías 1 a 4;
  - una **contraseña**, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de utilizarlos para la comisión de cualquiera de los delitos contemplados en las anteriores categorías 1 a 4.

EJEMPLOS

- Un acceso no autorizado.
- El robo de contraseñas.
- Prácticas de Ingeniería Social.
- La utilización de fallas en los procesos de autenticación para obtener accesos indebidos.
- El robo de información.
- El borrado de información de terceros.
- La alteración de la información de terceros.

EJEMPLOS

- El abuso y/o mal uso de los servicios informáticos internos o externos de una organización.
- La introducción de código malicioso en la infraestructura tecnológica de una entidad (virus, troyanos, gusanos, malware en general).

..//

EJEMPLOS

- La denegación del servicio o eventos que ocasionen pérdidas, tiempos de respuesta no aceptables o no cumplimiento de Acuerdos de Niveles de Servicio existentes de determinado servicio.
- Situaciones externas que comprometan la seguridad de sistemas, como quiebra de compañías de software, condiciones de salud de los administradores de sistemas, entre otros.

AUMENTO DE INCIDENTES

- Crecimiento de la dependencia tecnológica
- No hay una conciencia sobre la privacidad
- Amplia disponibilidad de herramientas
- Falta de leyes globales y locales
- Falsa sensación de que todo se puede hacer en Internet
- Gran aumento de vulnerabilidades de seguridad

..//

AUMENTO DE INCIDENTES

- Traslado de negocios con dinero real a Internet (servicios financieros, juegos de azar, sitios de subastas, etc.)
- Oferta y demanda de información confidencial más abierta

SEGURIDAD INFORMATICA

ATENCION DE INCIDENTES

GESTION DE INCIDENTES

PREPARACION

- **Gestión de Parches de Seguridad**: las entidades dependiendo de su organización deben contar con un programa de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, otro software instalado), este programa ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches.

PREPARACION

- **Fortalecimiento de plataforma**: las entidades dependiendo de su organización deben ser aseguradas correctamente.
  - Se debe configurar la menor cantidad de servicios con el fin de proveer únicamente aquellos servicios necesarios. ..//

PREPARACION

- **Fortalecimiento de plataforma**
  - Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos).
  - Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia.
  - Los servidores deben tener habilitados sus sistemas de auditoría.

PREPARACION

- **Seguridad en redes**: Debe existir una gestión constante sobre los elementos de seguridad.
  - Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente.
  - Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados para su respectivo análisis.

PREPARACION

- **Prevención de código malicioso**: Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.

PREPARACION

- **Sensibilización y entrenamiento de usuarios**: Los usuarios en la entidad incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad. ..//

PREPARACION

- **Sensibilización y entrenamiento de usuarios**:.
- Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

PREPARACION

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad de la información adicionalmente es necesario realizar una evaluación mensual.

SEGURIDAD INFORMATICA

ATENCION DE INCIDENTES

GESTION DE INCIDENTES

PREPARACION

- **RECURSOS DE COMUNICACIÓN**
  - **Información de Contacto**: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

..//

PREPARACION

- **RECURSOS DE COMUNICACIÓN**
  - **Información de Escalamiento**: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad.
    - Información de los administradores de la plataforma tecnológica (Servicios, Servidores)
    - Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
    - Contacto con áreas interesadas o grupos de interés (Policía Nacional, Fiscalía, entre otras)

..//

PREPARACION

- **RECURSOS DE COMUNICACIÓN**
  - **Política de Comunicación**: La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

PREPARACION

- **HARDWARE Y SOFTWARE**

  Para una correcta y eficiente gestión de incidentes la entidad debería tener en cuenta los siguientes elementos:

  - Portátiles Forenses
  - Analizadores de protocolos
  - Software de adquisición

..//

PREPARACION

- **HARDWARE Y SOFTWARE**
  - Software para recolección de evidencia
  - Kit de respuesta a incidentes
  - Software de análisis forense
  - Medios de almacenamiento

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Portátiles Forenses**. Disponer de un portátil que contenga software libre para escanear vulnerabilidades, escanear la red, los puertos, mapeadores de red y de puertos, analizadores de protocolos, detección remota de servicios, detección remota de equipos activos y sistemas operativos, identificación de software y versiones, análisis de banners, búsqueda de aplicaciones web, y análisis de la configuración de las redes wifi.

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Analizadores de Protocolos** También se dispondrá de un software libre analizador de paquetes de código abierto, el cual se utilizará para resolver problemas de red, análisis, desarrollo de protocolos de software y comunicaciones, y principalmente para monitorear el tráfico de red, el cual en todo caso debe garantizar neutralidad tecnológica.

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Software de Adquisición**. Se hará uso del software que permita la gestión de activos, de tal forma que se pueda observar qué activos están asignados, a quién y su ubicación física. Permite revisar el historial completo del activo. Ver qué activos están actualmente desplegados, pendientes (nuevos en espera de instalaciones de software, reparados), listos para implementar o archivados (perdidos, robados o malogrados).

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Software para recolección de evidencia**: La recolección de evidencia está estrechamente ligada al análisis forense, y en ocasiones son usados como sinónimos, por lo tanto, el software forense gratuito seleccionada también debe garantizar la recolección de evidencia.

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Kit de Respuesta a Incidentes**. Todos los elementos mencionados se debe tener a disposición inmediata.
  - **Software de Análisis forense**. Se hará uso del software que permita la detección de huellas de eliminación o alteración de información o de archivos.

PREPARACION

- **HARDWARE Y SOFTWARE**
  - **Medios de almacenamiento**. Se deberá disponer de un lote de dispositivos de almacenamiento externo para recopilar los datos forenses.