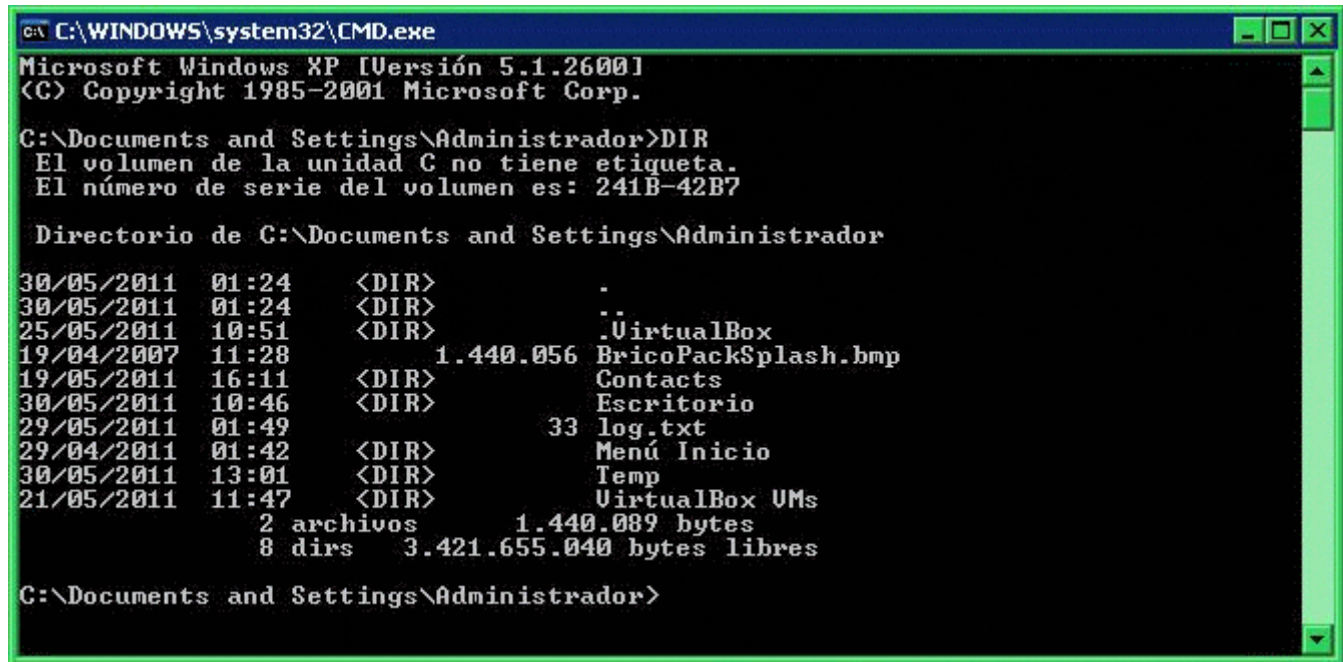


# Capítulo 1: Tríada CIA y Gestión de Activos

Este capítulo es **fundamental** para establecer los fundamentos de la ciberseguridad. Aquí, exploraremos los conceptos esenciales de la **Tríada CIA** y cómo se relacionan con la **Gestión de Activos**, dos pilares sobre los que se construye la protección de cualquier sistema de información.



```
C:\WINDOWS\system32\CMD.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrador>DIR
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 241B-42B7

Directorio de C:\Documents and Settings\Administrador

30/05/2011  01:24    <DIR>          .
30/05/2011  01:24    <DIR>          ..
25/05/2011  10:51    <DIR>          .VirtualBox
19/04/2007  11:28    1.440.056 BricoPackSplash.bmp
19/05/2011  16:11    <DIR>          Contacts
30/05/2011  10:46    <DIR>          Escritorio
29/05/2011  01:49    33 log.txt
29/04/2011  01:42    <DIR>          Menú Inicio
30/05/2011  13:01    <DIR>          Temp
21/05/2011  11:47    <DIR>          VirtualBox VMs
                2 archivos      1.440.089 bytes
                8 dirs    3.421.655.040 bytes libres

C:\Documents and Settings\Administrador>
```

## 1.1 Tríada CIA: Pilares de Seguridad

La **Tríada CIA** es el **corazón** de la seguridad de la información. Representa los tres **objetivos principales** que toda organización debe perseguir para proteger sus activos de información. Imagínala como un triángulo equilátero, donde cada lado es igualmente importante y esencial para la estabilidad del conjunto.

- **Confidencialidad**

Asegurar que la **información sensible** solo sea accesible para **entidades autorizadas**, ya sean personas, procesos o sistemas. Piensa en la **confidencialidad** como el arte de mantener secretos en el mundo digital. No se trata solo de ocultar información a "extraños", sino de controlar rigurosamente quién tiene acceso a qué, incluso dentro de la propia organización.

- **Cifrado Simétrico (AES-256)**

Este es el **caballo de batalla** del cifrado para datos en reposo. **AES-256** (Estándar de cifrado avanzado con clave de 256 bits) es un algoritmo de **clave secreta**. Esto significa que la

misma clave se utiliza tanto para **cifrar** (convertir la información legible en ilegible) como para **descifrar** (revertir el proceso).

**Analogía:** Imagina que tienes una **caja fuerte** (el cifrado) y una **única llave** (la clave **AES-256**). Solo con esa llave puedes abrir la caja fuerte y acceder a los documentos valiosos que guardas. Quien tenga la llave, tiene acceso a los secretos.

**Uso Práctico:** Es ideal para proteger datos almacenados en **discos duros cifrados**, bases de datos o archivos sensibles en general. Si alguien no autorizado accede al disco duro cifrado, solo verá datos ininteligibles sin la clave correcta.

**Robusto:** **AES-256** se considera **extremadamente seguro** y es un estándar ampliamente adoptado a nivel mundial, incluso por gobiernos y organizaciones militares.

#### ◦ **Cifrado Asimétrico (RSA)** -

A diferencia del simétrico, **RSA** (Rivest-Shamir-Adleman) utiliza un par de claves: una **clave pública** y una **clave privada**.

**Analogía:** Piensa en tener un **buzón de correo público** (clave pública) donde cualquiera puede depositar cartas cifradas para ti. Sin embargo, solo tú, con tu llave privada secreta, puedes abrir ese buzón y leer las cartas.

#### **Funcionamiento:**

- Con la **clave pública**, cualquiera puede **cifrar** mensajes o verificar firmas digitales.
- La **clave privada**, que debes mantener **absolutamente secreta**, es necesaria para **descifrar** mensajes cifrados con la clave pública correspondiente o para **crear firmas digitales**.

**Uso Práctico:** Fundamental para **comunicaciones seguras** a través de internet, como en **SSL/TLS** (HTTPS). Permite establecer canales de comunicación cifrados sin necesidad de

intercambiar claves secretas previamente. También se utiliza para **firmas digitales**, garantizando la autenticidad y no repudio de documentos electrónicos.

**Ejemplo SSL/TLS:** Cuando visitas una página web con `https://` en la barra de direcciones, tu navegador y el servidor web intercambian claves públicas **RSA** para establecer un canal de comunicación cifrado. Esto asegura que la información que viaja entre tu ordenador y el servidor web (contraseñas, datos personales, etc.) se mantenga confidencial y no pueda ser interceptada por terceros.

- **Caso: Equifax (Filtración de Datos 2017)**

Este caso ilustra dramáticamente las consecuencias de no proteger la **confidencialidad** de los datos. Equifax, una de las mayores agencias de informes crediticios, sufrió una brecha de seguridad que expuso **datos personales de 147 millones de personas**.

**Fallo Clave:** La **falta de cifrado** de datos sensibles en reposo fue un factor crítico. Si los datos de los clientes hubieran estado debidamente cifrados, el impacto de la filtración habría sido mucho menor. Aunque los atacantes hubieran accedido a la base de datos, habrían encontrado datos ilegibles sin la clave correcta.

**Lecciones Aprendidas:** Este incidente subrayó la **imperiosa necesidad de implementar el cifrado como una medida de seguridad fundamental** para proteger la **confidencialidad** de la información, especialmente en organizaciones que manejan grandes volúmenes de datos personales y sensibles. No basta con proteger el acceso perimetral a los sistemas; los datos en sí mismos deben estar protegidos mediante cifrado.

---

- **Integridad**

Garantizar la **exactitud y completitud** de la información a lo largo de su ciclo de vida, previniendo la **alteración no autorizada**. La **integridad** se centra en la **fiabilidad** de los datos. No solo importa que la información sea confidencial, sino que también sea **veraz y auténtica**.

- **Funciones Hash (SHA-256)**

Las **funciones hash** son algoritmos matemáticos que toman una entrada de datos (de cualquier tamaño) y producen una salida de tamaño fijo, llamada **hash** o **resumen**.

#### Propiedades Clave de las Funciones Hash Seguras:

- **Unidireccionalidad:** Es computacionalmente inviable revertir el proceso, es decir, obtener la entrada original a partir del hash.
- **Determinismo:** La misma entrada siempre producirá el mismo hash.
- **Efecto Avalancha:** Un pequeño cambio en la entrada (incluso un solo bit) resulta en un hash completamente diferente.
- **Resistencia a Colisiones:** Es extremadamente difícil (computacionalmente inviable) encontrar dos entradas diferentes que produzcan el mismo hash.

**SHA-256** (Secure Hash Algorithm 256-bit): Una de las **funciones hash más utilizadas y robustas**. Produce un hash de 256 bits (64 caracteres hexadecimales).

**Analogía:** Imagina una **picadora de carne** (función hash). Introduces cualquier tipo de carne (datos de entrada) y siempre obtienes un "resumen" de carne picada (hash) de tamaño fijo. Es imposible reconstruir el tipo original de carne solo viendo la carne picada. Y si cambias mínimamente la carne original, la carne picada resultante será totalmente diferente.

**Uso Práctico:** Ideal para **verificar la integridad de archivos**. Al descargar un archivo, puedes calcular su hash **SHA-256** y compararlo con el hash oficial publicado por el proveedor. Si los hashes coinciden, tienes una alta confianza de que el archivo no ha sido alterado ni corrompido durante la descarga. También se utilizan en **firmas digitales** y **blockchain**.

#### ◦ Firmas Digitales

Las **firmas digitales** combinan el **cifrado asimétrico** y las **funciones hash** para proporcionar **autenticidad, integridad y no repudio** a documentos electrónicos.

#### Proceso:

1. Se calcula el **hash** del documento usando una función hash como **SHA-256**.
2. El hash se **cifra** utilizando la **clave privada** del firmante. El resultado cifrado es la **firma digital**.
3. La firma digital se adjunta al documento.

**Verificación:** Para verificar una firma digital:

1. Se calcula nuevamente el **hash** del documento recibido.
2. Se **descifra** la firma digital utilizando la **clave pública** del firmante.
3. Se **compara** el hash calculado con el hash descifrado de la firma. Si coinciden, la firma es válida.

**Beneficios Clave:**

- **Autenticidad:** Verifica que el documento proviene realmente del firmante declarado (ya que solo él posee la clave privada para crear la firma).
- **Integridad:** Asegura que el documento no ha sido alterado después de ser firmado (cualquier modificación cambiaría el hash y, por lo tanto, la firma no sería válida).
- **No Repudio:** El firmante no puede negar haber firmado el documento (ya que la firma está vinculada a su clave privada única).

**Uso Práctico:** Ampliamente utilizadas en **documentos legales en blockchain**, transacciones electrónicas, distribución de software (para verificar la autenticidad e integridad de las actualizaciones), y en general, en cualquier escenario donde se requiera garantizar la autenticidad y no alteración de la información digital.

## ◦ Ejercicio Práctico

Verificar la integridad de un archivo descargado es una práctica esencial en ciberseguridad. Este ejercicio te guiará a través de este proceso.

**Objetivo:** Aprender a **verificar la integridad** de un archivo utilizando funciones hash, asegurando que el archivo descargado sea auténtico y no haya sido modificado maliciosamente.

## Pasos:

1. **Descargar un archivo ISO:** Busca en internet una distribución de Linux (como Ubuntu, Debian, Fedora, etc.) y descarga su imagen ISO. Asegúrate de descargarla del **sitio web oficial** de la distribución.
2. **Ubicar el Hash Oficial:** En el sitio web oficial de la distribución Linux, busca la sección de descargas y localiza el **hash SHA-256** (o SHA-512) correspondiente a la imagen ISO que descargaste. Normalmente, se proporciona junto al enlace de descarga.
3. **Calcular el Hash SHA-256 localmente:** Abre una terminal en tu sistema operativo (Linux, macOS o Windows). Utiliza la herramienta `sha256sum` (en Linux y macOS) o una herramienta equivalente en Windows (como `CertUtil` en PowerShell) para calcular el hash **SHA-256** del archivo ISO que descargaste. El comando en la terminal sería:

```
sha256sum archivo.iso
```

(Reemplaza `archivo.iso` con el nombre real del archivo ISO que descargaste).

4. **Comparar los Hashes:** Compara el hash que calculaste en tu terminal con el **hash oficial** que encontraste en el sitio web. **¡Deben ser exactamente iguales!**
  - **Si los hashes coinciden:** Esto te da una **alta confianza** de que el archivo ISO que descargaste es **auténtico** y no ha sido alterado durante la descarga. Puedes proceder a utilizarlo con seguridad.
  - **Si los hashes no coinciden: ¡Precaución!** Esto indica que el archivo **podría haber sido modificado** o corrompido. No utilices este archivo. Vuelve a descargarlo del sitio web oficial y repite el proceso de verificación del hash. Si el problema persiste, podría indicar un problema de seguridad más grave (como un ataque "man-in-the-middle").

---

## • Disponibilidad

Garantizar que los sistemas y la información estén **accesibles y operativos** para los usuarios autorizados **cuando los necesiten**. La **disponibilidad** se centra en asegurar que los servicios

estén **siempre en línea** y listos para ser utilizados. No importa si la información es confidencial e íntegra si no podemos acceder a ella cuando la necesitamos.

- **Redundancia y Balanceo de Carga**

Son técnicas clave para lograr alta disponibilidad y resistencia a fallos.

**Redundancia:** Implica tener **componentes duplicados** en el sistema (servidores, redes, fuentes de alimentación, etc.). Si un componente falla, otro componente redundante puede tomar su lugar, asegurando la continuidad del servicio.

**Ejemplos:** Servidores espejo (mirror servers), arreglos RAID en discos duros, fuentes de alimentación redundantes en servidores.

**Balanceo de Carga (Load Balancing):** Distribuye el **tráfico de red** y las **solicitudes de los usuarios** entre múltiples servidores, en lugar de sobrecargar un único servidor.

**Beneficios:** Mejora el rendimiento, la capacidad de respuesta y la disponibilidad del servicio, especialmente durante picos de tráfico. Si un servidor falla, el balanceador de carga redirige el tráfico a los servidores restantes.

**Ejemplo: Netflix usa AWS Global Accelerator** : Netflix, para asegurar que sus servicios de streaming estén disponibles para millones de usuarios en todo el mundo, utiliza **AWS Global Accelerator**. Este servicio de Amazon Web Services utiliza balanceo de carga global para dirigir el tráfico de los usuarios al centro de datos de Netflix más cercano y con mejor rendimiento, garantizando una experiencia de visualización fluida y sin interrupciones, incluso en momentos de alta demanda (como el lanzamiento de una serie popular).

- **Plan de Recuperación ante Desastres (DRP)**

Un **DRP** es un **conjunto documentado de procedimientos y políticas** que definen cómo una organización se recuperará de un **desastre** (ya sea natural, técnico o causado por el hombre) que interrumpa sus operaciones normales. El **DRP** es el "plan de emergencia" de la ciberseguridad.

**Componentes Clave** : Un **DRP** efectivo debe incluir, al menos, los siguientes elementos:

- **Backups Automáticos:** Copias de seguridad regulares y automatizadas de datos y sistemas críticos. Es fundamental que los backups sean **verificados** y **almacenados en un lugar seguro y separado** de la infraestructura principal (idealmente, **offline** para protegerlos de ransomware, como veremos más adelante).
- **Centros de Datos Alternos (Sitios de Recuperación):** Ubicaciones geográficamente separadas del centro de datos principal, equipadas para albergar una réplica de la infraestructura crítica de la organización. En caso de un desastre mayor en el sitio principal, las operaciones pueden ser **conmutadas al sitio alternativo** (failover) para minimizar el tiempo de inactividad.
- **Equipos de Respuesta a Incidentes (IRT):** Equipos multidisciplinarios formados por personal de TI, seguridad, comunicación, legal, etc., entrenados para ejecutar el **DRP** y gestionar la recuperación ante desastres. Deben tener roles y responsabilidades claramente definidos.
- **Procedimientos de Recuperación Detallados:** Documentación paso a paso de cómo restaurar sistemas, datos, aplicaciones y servicios críticos, incluyendo tiempos de recuperación esperados (RTO - Recovery Time Objective) y puntos de recuperación (RPO - Recovery Point Objective).
- **Pruebas y Simulacros Regulares:** Es crucial **probar y actualizar periódicamente** el **DRP** para asegurar su efectividad y adaptarlo a los cambios en la infraestructura y las amenazas. Los simulacros permiten identificar puntos débiles y mejorar la preparación del equipo de respuesta.

---

## 1.2 Gestión de Activos y Riesgos

Una vez entendidos los pilares de la Tríada CIA, es esencial aplicar estos principios a la **Gestión de Activos y Riesgos**. No todos los activos son iguales, ni todos los riesgos tienen la misma probabilidad e impacto. La gestión de activos y riesgos nos permite **priorizar y concentrar los recursos de seguridad** donde más se necesitan.



- **Asset (Activo)**

En ciberseguridad, un **activo** es **cualquier cosa de valor** para la organización que **debe ser protegida**. Puede ser tangible o intangible, físico o lógico. La clave es identificar qué es valioso para la organización y, por lo tanto, necesita medidas de seguridad.

- **Clasificación (Críticos / No Críticos )**

No todos los activos tienen el mismo valor ni la misma criticidad para la organización. Es fundamental **clasificar los activos** para poder asignarles los niveles de protección adecuados. Una clasificación común es:

**Activos Críticos** : Son aquellos activos cuya **pérdida o compromiso** tendría un **impacto severo o catastrófico** en la organización. Esto podría incluir:

- **Bases de datos de clientes:** Contienen información personal y sensible de los clientes, cuya filtración podría dañar la reputación de la empresa, generar multas regulatorias y pérdida de confianza de los clientes.
- **Sistemas de pago:** Procesan transacciones financieras. Su interrupción o compromiso podría paralizar la actividad comercial y generar pérdidas económicas significativas.
- **Sistemas de producción:** En empresas industriales, los sistemas que controlan la maquinaria y los procesos de producción son críticos. Su fallo podría detener la producción, generar pérdidas y, en algunos casos, incluso poner en riesgo la seguridad física.
- **Propiedad intelectual:** Patentes, secretos comerciales, diseños, etc. Su robo podría dar ventajas competitivas a los rivales y perjudicar la innovación de la empresa.
- **Infraestructura crítica:** Sistemas que gestionan servicios esenciales como energía, agua, transporte, comunicaciones, etc. Su compromiso podría tener consecuencias graves para la sociedad en general.

**Activos No Críticos** : Son activos cuya **pérdida o compromiso** tendría un **impacto menor o manejable** en la organización. Esto podría incluir:

- **Blogs corporativos:** Aunque su contenido es público y su pérdida no paralizaría la operación, sí podrían afectar la imagen de la empresa.

- **Redes sociales:** Similares a los blogs, principalmente relacionados con la imagen y la comunicación, pero menos críticos para la operación principal.
- **Servidores de prueba y desarrollo:** Menos críticos que los sistemas en producción, pero también pueden contener información sensible en desarrollo.
- **Equipos de usuario final (PCs de empleados):** Aunque individuales, la pérdida de un único PC no paralizaría la empresa, pero sí podría afectar la productividad de un empleado y contener información sensible.
- **Documentación pública:** Manuales de usuario, folletos informativos, etc. Su pérdida generalmente no tiene un impacto significativo.

#### ◦ **Ejercicio: Matriz de Criticidad**

Para comprender mejor la clasificación de activos, vamos a crear una **matriz de criticidad** para una empresa de e-commerce con 100 empleados.

**Escenario:** Una empresa de comercio electrónico que vende ropa y accesorios online, con 100 empleados, incluyendo personal de ventas, marketing, logística, desarrollo web, atención al cliente, administración y dirección.

**Tarea:** Clasifica los siguientes activos de la empresa en una **matriz de criticidad**, utilizando las categorías: **Alta, Media, Baja**. Justifica brevemente tu elección para cada activo, considerando el impacto potencial de su pérdida o compromiso en la operación del negocio.

Activo	Criticidad (Alta/Media/Baja)	Justificación
Base de datos de clientes		
Sistema de procesamiento de pagos		
Servidor web de la tienda online		
Servidor de correo electrónico		
Blog corporativo de la empresa		
Cuenta de redes sociales de la empresa		
PCs de empleados de atención al cliente		

Activo	Criticidad (Alta/Media/Baja)	Justificación
PCs de empleados del departamento de marketing		
Servidor de archivos compartidos interno		
Sistema CRM (Customer Relationship Management)		

## • Risk (Riesgo)

Un **riesgo** en ciberseguridad es la **probabilidad** de que una **amenaza** explote una **vulnerabilidad** en un activo, causando un **impacto negativo** en la organización. El riesgo es una combinación de amenaza, vulnerabilidad e impacto.

### ◦ Análisis Cuantitativo vs. Cualitativo /

Existen dos enfoques principales para el análisis de riesgos:

**Análisis Cuantitativo** : Busca **cuantificar** el riesgo, asignándole **valores numéricos** para medir la **pérdida esperada**.

**Ejemplo:** Calcular la "pérdida anual esperada" (ALE - Annualized Loss Expectancy).

Para ello, se necesitan estimaciones de:

- **Valor del Activo (AV - Asset Value):** El valor monetario del activo que se está evaluando.
- **Factor de Exposición (EF - Exposure Factor):** El porcentaje de pérdida del valor del activo que se espera que ocurra si se materializa la amenaza.
- **Tasa de Ocurrencia Anual (ARO - Annualized Rate of Occurrence):** La probabilidad estimada de que la amenaza se materialice en un año.

**Fórmula:**  $ALE = AV * EF * ARO$

**Ejemplo Numérico:** Supongamos que una base de datos de clientes (Activo) tiene un valor de 1 millón de dólares (AV). Se estima que una filtración de datos (Amenaza) podría causar una pérdida del 50% del valor (EF = 0.5). Y se estima que la probabilidad de una filtración de datos en un año es del 10% (ARO = 0.1). Entonces, la pérdida anual esperada (ALE) sería:  $ALE = \$1,000,000 * 0.5 * 0.1 = \$50,000$ . Esto significa que, en promedio, se espera una pérdida de 50.000 dólares al año debido a este riesgo.

**Análisis Cualitativo** : Prioriza los riesgos de forma **subjectiva**, utilizando **categorías** como "Alto", "Medio", "Bajo" o "Crítico", en función de la **probabilidad** y el **impacto** percibidos.

**Ejemplo:** Evaluar el riesgo de "ataque de ransomware" para un servidor web.

- **Probabilidad:** Se puede clasificar como "Media" si se considera que el servidor web está expuesto a internet y existen vulnerabilidades conocidas en el software utilizado.
- **Impacto:** Se puede clasificar como "Alto" si el servidor web es crítico para la operación del negocio y su indisponibilidad causaría pérdidas significativas.
- **Riesgo Cualitativo:** Combinando probabilidad e impacto (por ejemplo, en una matriz de riesgo), se podría clasificar el riesgo general como "Alto" o "Medio-Alto".

**Ventajas del Análisis Cualitativo:** Más rápido y fácil de realizar que el análisis cuantitativo. Útil cuando no se dispone de datos numéricos precisos o cuando se requiere una visión general de los riesgos.

**Desventajas del Análisis Cualitativo:** Más subjetivo y menos preciso que el análisis cuantitativo. La priorización de riesgos puede depender de la percepción individual de los evaluadores.

○ **Herramientas: Matriz de Calor (Heat Map)**

Una **matriz de calor** es una herramienta visual muy útil para representar gráficamente los resultados del análisis de riesgos, especialmente en el análisis cualitativo.

### Funcionamiento:

1. Se crea una **matriz bidimensional**.
2. Un eje representa la **Probabilidad** del riesgo (por ejemplo, de "Muy Baja" a "Muy Alta").
3. El otro eje representa el **Impacto** del riesgo (por ejemplo, de "Insignificante" a "Catastrófico").
4. Cada **celda de la matriz** representa una combinación de probabilidad e impacto.
5. Se **colorean las celdas** según el nivel de riesgo. Normalmente:
  - **Verde:** Riesgo Bajo.
  - **Amarillo:** Riesgo Medio.
  - **Naranja:** Riesgo Alto.
  - **Rojo:** Riesgo Crítico.
6. Los riesgos evaluados se **ubican en la matriz** en función de su probabilidad e impacto, y se visualizan con el color correspondiente.

**Beneficios de la Matriz de Calor:** Permite **visualizar rápidamente** los riesgos más críticos ("calientes", en rojo y naranja) que requieren atención prioritaria. Facilita la **comunicación** de los riesgos a la dirección y a otros stakeholders. Ayuda a **priorizar** las acciones de mitigación, enfocándose en los riesgos más "calientes" primero.

## Ejemplo de Matriz de Criticidad de Activos para Empresa de E-commerce: Solución Propuesta

Esta tabla presenta un **ejemplo de solución** para la tarea de clasificación de activos de una empresa de comercio electrónico de ropa y accesorios online con 100 empleados. Recordemos que la tarea consistía en clasificar los activos según su **criticidad** (Alta, Media, Baja), justificando brevemente la elección para cada uno, considerando el impacto potencial de su pérdida o compromiso en la operación del negocio.

**Nota Importante:** Esta es **solo una posible solución**. La clasificación de criticidad puede ser **subjetiva** y variar ligeramente dependiendo de diferentes interpretaciones y perspectivas sobre el negocio. El objetivo principal del ejercicio es **entender el proceso de análisis de criticidad** y la **lógica detrás de la clasificación**, más que llegar a una respuesta "única y correcta".

<b>Activo</b>	<b>Criticidad (Alta/Media/Baja)</b>	<b>Justificación</b>
Base de datos de clientes	<b>Alta</b>	Contiene información personal y sensible de clientes (datos bancarios, direcciones, historial de compras). Su filtración generaría graves daños reputacionales, multas por RGPD, y pérdida de confianza. Esencial para la operación del negocio.
Sistema de procesamiento de pagos	<b>Alta</b>	Crítico para la operatividad del negocio online. Su fallo detendría las ventas, generando pérdidas económicas directas e inmediatas. Además, la seguridad es fundamental para evitar fraudes y problemas legales.
Servidor web de la tienda online	<b>Alta</b>	Es la cara visible del negocio online. Su indisponibilidad impide la venta de productos y acceso al catálogo. Impacto directo en ingresos y reputación online.
Servidor de correo electrónico	<b>Media</b>	Importante para la comunicación interna y con clientes (confirmaciones de pedido, atención al cliente). Su caída afecta la eficiencia operativa y la comunicación, pero no detiene la actividad principal del negocio inmediatamente.
Blog corporativo de la empresa	<b>Baja</b>	Principalmente enfocado en marketing y SEO. Su pérdida afecta la estrategia de marketing online y la imagen, pero no paraliza la operación principal del negocio ni expone datos críticos directamente.
Cuenta de redes sociales de la empresa	<b>Baja</b>	Similar al blog, afecta la imagen y comunicación de marketing. Su compromiso podría dañar la reputación, pero el impacto directo en la operación principal es bajo. Recuperable relativamente rápido.
PC de empleados de atención al cliente	<b>Medios de comunicación</b>	Contienen información sensible de clientes (temporalmente en caché, historial de interacciones). Su compromiso puede llevar a filtraciones de datos y afectar la atención al cliente si no pueden operar.
PC de empleados del departamento de marketing	<b>Baja</b>	Principalmente contienen información de marketing y campañas. La pérdida afecta la productividad del departamento y posiblemente planos de marketing, pero no es crítica para la operación del negocio en sí.
Servidor de archivos compartidos internos	<b>Medios de comunicación</b>	Puede contener documentos importantes para la operación interna, pero no es crítico para la venta directa o procesamiento de pagos. La indisponibilidad afecta la productividad interna y podría contener información sensible interna.
Sistema CRM (Gestión de la relación con el cliente)	<b>Alta</b>	Centraliza la gestión de la relación con clientes, historial de interacciones, datos de ventas y análisis de clientes. Su pérdida afecta gravemente la capacidad de gestionar clientes, ventas y estrategias comerciales. Contiene datos sensibles de clientes.

## Contexto y Razonamiento Detallado:

- **Activos de Criticidad Alta:**

- **Base de datos de clientes:** Considerada de criticidad **Alta** debido al **impacto catastrófico** que tendría la filtración de la información sensible que contiene. La pérdida de confianza del cliente, las multas regulatorias y el daño reputacional serán muy graves.
- **Sistema de procesamiento de pagos:** Clasificado como **Alta** criticidad por su **papel fundamental en la generación de ingresos**. Su fallo detendría las ventas online y generaría pérdidas económicas inmediatas, además de riesgos de fraude.
- **Servidor web de la tienda online:** También de criticidad **Alta** ya que es la **"fachada" del negocio online**. Su indisponibilidad impide a los clientes acceder a la tienda y realizar compras, impactando directamente en los ingresos y la reputación.

- **Activos de Criticidad Media:**

- **Servidor de correo electrónico:** Clasificado como **Media** porque aunque es importante para la comunicación, su fallo **no detiene la operación principal del negocio** de forma inmediata. Afecta la eficiencia operativa y la comunicación, pero no es tan crítico como los activos de criticidad Alta.
- **PCs de empleados de atención al cliente:** De criticidad **Media** porque su compromiso **afecta la calidad del servicio al cliente** y podría llevar a la exposición de información sensible. Sin embargo, no paralizan la operación central del negocio.
- **Servidor de archivos compartidos interno:** Criticidad **Media** ya que su indisponibilidad **afecta la productividad interna** y podría exponer información interna sensible. No es crítico para la venta directa al cliente online.
- **Sistema CRM (Customer Relationship Management):** Aunque muy importante, se clasifica como **Alta** debido a su **impacto significativo en la gestión de clientes y estrategias comerciales**, y porque **contiene datos sensibles de clientes**, aunque su impacto no sea tan inmediato en la operación diaria como el sistema de pagos o el servidor web.

- **Activos de Criticidad Baja:**

- **Blog corporativo de la empresa:** De criticidad **Baja** ya que su pérdida afecta principalmente al **marketing y la imagen**, pero no la operación principal del negocio.
- **Cuenta de redes sociales de la empresa:** Similar al blog, de criticidad **Baja** porque impacta en la **imagen y comunicación de marketing**, pero no en la operación principal y es recuperable relativamente rápido.
- **PCs de empleados del departamento de marketing:** Criticidad **Baja** porque la pérdida afecta la **productividad del departamento de marketing**, pero no es crítico para la operación general del negocio online.