CONTESTE LAS SIGUIENTES PREGUNTAS

(PUEDE OBVIAR LO CONCERNIENTE A PROGRAMACIÓN PARALELA)

**1-A PARTIR DE QUE AÑO SE DISPARA EL CONCEPTO DE BIG DATA?**

Entre 1984 y 2007 se impuso su concepto al ámbito científico y de negocios restringidos. A partir del 2007 se difundió con criterio tecnológico económico.

Específicamente en 2001 Laney realizó un trabajo relacionado con el Big Data donde menciona las 3 V: Volumen, Variedad y Velocidad.

**2-CUAL SERIA UNA DEFINICION INICIAL?**

Podemos definirlo como grandes cantidades de datos que se convergen de distintas tecnologías para influenciar las organizaciones, la sociedad, las redes sociales, el internet de las cosas, la geolocalización y el cloud computing.

El Big Data cambia la cultura en la toma de decisiones.

**3-CUAL SERIA UNA DEFINICION INICIAL DE CIENTIFICO DE DATOS?**

Es una persona con habilidades serias en diversas disciplinas técnicas como las ciencias de la computación, el análisis, las matemáticas, el análisis funcional, el análisis matricial, la generación de modelos y la estadística. Además debe ser un buen comunicador capaz de entender un problema de negocios, transformarlo en un plano analítico, ejecutar un plan y dar una solución de negocios.

**4-CUAL SERIA LA ESTRUCTURA QUE MANEJA GRANDES DATOS?**

Principalmente tendremos las fuentes de donde obtenemos esos datos, que pueden ser la Web, la social media, la interconexión de objetos Machine2Machine, los sensores IOT, la biometría, entre otros.

Los datos obtenidos pueden clasificarse en tres categorías:

1- Datos Estructurados: provienen principalmente de bases de datos relacionales.

2- Datos Semiestructurados: provienen de archivos HTML, XML, etc.

3- Datos No Estructurados: pueden ser de audio, video, fotografías, etc.

Estos datos se guardarán en almacenes de datos y se utilizará un entorno (como puede ser Hadoop) para procesar y analizar los grandes volúmenes de datos, especialmente los semiestructurados y los no estructurados.

Finalmente, se utilizarán herramientas de analítica para mostrar esa información a quien sea necesario para dar soporte a la toma de decisiones. Estas herramientas pueden ser de informes (reporting), de consultas, de visualización (dashboards), entre otras.

**5-CUALES SON LAS CARACTERISTICAS (LAS 4) DE BIG DATA?**

1- Volumen

2- Velocidad

3- Variedad

4- Veracidad

**6-NOMBRE UNA IMPLICACIÓN EMPRESARIAL DE BIG DATA**

El Big Data es fundamental para las empresas que deseen mantenerse competitivas en el mercado. Es esencial tomar la mayor cantidad de datos posibles tanto sobre cómo funciona la empresa como datos del entorno para aumentar la productividad de la misma y estar al tanto de los posibles cambios que puedan afectar el cumplimiento de las metas.

**7-NOMBRE TRES FUENTES DE DATOS VOLUMINOSAS**

1- La Web.

2- Las redes sociales.

3- Los medios de comunicación.

**8-NOMBRE DOS TIPOS DE BIG DATA Y DESCRÍBALOS**

1- Web y Medios Sociales: son datos generados de páginas web o de redes sociales como Twitter o Facebook,, que nos permiten obtener datos de clientes actuales o potenciales, sus preferencias e intereses.

2- M2M y Internet de las Cosas: son datos obtenidos al capturar un evento en particular (como puede ser la velocidad, humedad, etc.) al realizar lecturas en etiquetas RFID, en medidores inteligentes, sensores o señales GPS.

3- Transacciones de grandes cantidades de datos: son datos transaccionales provenientes de las distintas áreas de una organización como los registros de facturación.

4- Biometría: se refiere a la identificación automática de personas basada en sus características anatómicas o trazos personales. Incluye huellas digitales, iris, escaneo de retina, reconocimiento facial y de voz, genética y ADN.

5- Generado por humanos: son datos extraídos de correos electrónicos, notas de voz, documentos, faxes, etc.

**9-QUE ES UN INDICADOR KPI?**

Son métricas e indicadores clave de rendimiento o desempeño que proporcionan valor añadido al proceso de toma de decisiones.

**10-QUE SON LOS CHIPS RFID Y NFC?**

Son las tecnologías de identificación por radiofrecuencia.

Una etiqueta RFID se coloca en objetos como alimentos, ropa, libros o medicamentos y al ser leída envía una señal retornando información. Se suelen usar en el etiquetado de productos, en el control de stock, etc.

La NFC en cambio se caracteriza en la comunicación entre objetos cercanos para intercambiar información en cantidades pequeñas para identificar o validar a un usuario. Algunos ejemplos son el pago por celular y los controles de acceso.

**11-A QUE SE CONOCE COMO INTERNET DE LAS COSAS?**

Es la interconexión digital de los objetos cotidianos con la Internet. Está conectado con las etiquetas RFID y permite la conexión entre objetos.

Se puede utilizar para rastreo, contabilización, reducción de desperdicio, entre otras cosas. También permite recopilar patrones de uso para aumentar la eficiencia en la producción.

**12-CONCRETAMENTE, CUAL ES LA IMPORTANCIA DE LOS DATOS DE TEXTO?**

Es una de las fuentes de datos más comunes y más grandes del Big Data. Podemos encontrarla en correos, mensajes de texto, blogs, tweets, entre muchos otros.

Este requiere primero un análisis sintáctico y una asignación de significados a las palabras y componentes del texto para luego deducir la información con la minería de textos.

**13-SE PUEDE GENERAR UNA ETIQUETA QUE ETIQUETE EL SENTIMIENTO?**

Si. Una nueva aplicación del procesamiento del lenguaje natural, la lingüística computacional y la analítica de texto permite la identificación y la extracción de información subjetiva.

Este puede identificar el sentimiento o los deseos de un correo electrónico

**14-QUE HACEN LOS SENSORES?**

Los sensores son una pieza clave en el internet de las cosas (IOT). Estos son capaces de monitorear el entorno en forma ubicua y autónoma creando entornos inteligentes.

En los últimos años los sensores se han incrustado en distintos dispositivos, máquinas y sistemas para su utilización.

**15-CUALES SON LOS DATOS NO ESTRUCTURADOS?**

Son datos que no tienen estructura interna identificable.

**16-LOS GPS SON FUENTE DE DATOS?**

Si. De los GPS podemos obtener datos de posicionamiento global específicamente necesarios para la logística. Se puede utilizar en aplicaciones donde se envían las coordenadas a un servidor que las almacena para ver la localización actual de un usuario, seguir el monitoreo de una ruta, etc.

**17-CUAL ES LA RELACION ENTRE IoT Y LA TECNOLOGIA RFID?**

IoT está estrechamente relacionado con la tecnología RFID porque ambos posibilitan la representación digital de los objetos. Se pueden conectar con otros objetos y datos de bases de datos. Por lo tanto, permite rastrear, contabilizar, reducir el desperdicio, las pérdidas y los costos.

**18-COMO SE ANALIZAN LAS REDES SOCIALES?**

La utilización de las redes sociales facilita comprender el valor total que la influencia de un cliente de una red social puede tener. Este conocimiento puede ayudar en la toma de decisiones de inversión en ese cliente. La rentabilidad de la influencia colectiva que un cliente puede aportar puede ser mayor que su rentabilidad individual.

La identificación de clientes muy conectados al sitio web de una empresa puede ayudar a determinar con precisión dónde centrar los esfuerzos que influyan en la imagen de la marca.

También debe analizarse el modo en que están conectadas las organizaciones para poder analizar el comportamiento de los departamentos y de sus empleados.

**19-QUE SON LOS SMART GRIDS?**

Un Smart Grid (o red inteligente) es un sistema de gestión, información y comunicaciones aplicadas a la red eléctrica cuyo objetivo es aumentar la conectividad, la automatización y coordinación entre productores, proveedores y consumidores en la red de distribución. Tiene sistemas de monitorización, comunicación y generación más sofisticados que facilitan servicios más consistentes y mejores métodos de recuperación de cortes de energía y otros problemas clásicos.

**20-QUE ES UN SMART METER Y CUAL ES SU ESTRUCTURA?**

Un Smart Meter (o contador inteligente) es un medidor eléctrico que reemplaza a los medidores tradicionales y es mucho más funcional. Elimina la necesidad del lector humano capturando los datos de modo automático y periódico.

La estructura de un smart meter tiene tres elementos principales:

* Sistema de medida.
* Memoria.
* Dispositivo de comunicaciones.

**21-NOMBRE DOS DOMINIOS ESTRATEGICOS DE BIG DATA**

* Salud en Estados Unidos.
* Administración pública en Europa.

**22-QUE ES LA CIENCIA DE DATOS?**

La ciencia de datos es una aplicación que extrae nuevos valores a partir de los big data, que éstos sean a su vez su fuente y su principal motor es lo que realmente se llama big data. Se refiere a las técnicas y teorías implicadas en el proceso de adquirir, limpiar, ordenar, procesar, mostrar y almacenar los datos que nos pueden ayudar a detectar problemas en nuestro negocio o a optimizar y mejorar nuestros procesos.

**23-QUE SE PUEDE HACER MEDIANTE LA CIENCIA DE DATOS?**

Mediante la ciencia de datos se puede hacer:

* Recomendación de productos (Amazon).
* Recomendación de personas que podrías conocer (Facebook).
* Sistema de recomendaciones y conocimientos personales (LinkedIn).
* Análisis y mejora de procesos de distribución (Walmart).
* Análisis del tipo de consumidor que actualmente es un usuario para convertirlo en un tipo distinto de consumidor a largo plazo o para mantenerlo como tal (Netflix).
* Analizar cómo interactúan los usuarios con sus juegos para mantenerlos el máximo de tiempo en esa actividad (Zynga).
* Detectar fraudes analizando operaciones bancarias y de tarjetas (Visa, Paypal).

**24-QUE ES BUSINESS INTELIGENCE?**

Business Intelligence es una colección de tecnologías y sistemas de información que soportan la toma de decisiones empresariales o el control operacional, proporcionando información de operaciones internas y externas.

**25-QUE COMPONENTES INCORPORA BI A SU PLATAFORMA?**

Las plataformas BI incorporan componentes de:

* Almacenamiento de datos (bases de datos, data warehouses y data marts).
* Procesamiento analítico en línea (OLAP).
* Minería de datos (minería de textos, minería web, minería social).
* Realización de informes (reporting).
* Interfaces de usuario.
* Herramientas de visualización (dashboads, scoreboards).

**26-QUE ES OLAP?**

OLAP (On Line Analysis Processing) es el procesamiento analítico en línea o análisis multidimensional. Permite a los usuarios la visualización de los datos de diferentes formas usando dimensiones múltiples.

Este sistema se apoya en cubos multidimensionales o bases de datos multidimensionales donde cada aspecto o campo de una información representa una dimensión.

**27-QUE ES LA MINERIA DE SENTIMIENTOS?**

La minería de sentimientos es el proceso de buscar información valiosa en mensajes de texto y otros formatos de medio, centrándose en el análisis de los sentimientos y opiniones para poder descubrir la opinión o el sentimiento de las personas.

**28-QUE ES EL DSS?**

Los sistemas de apoyo a la decisión (DSS) son sistemas que combinan modelos y datos en un intento de analizar problemas semiestructurados y no estructurados, facilitando a los gerentes de negocios y analistas el acceso a datos interactivamente, su manipulación y la realización de los análisis apropiados.

**29-CUALES SON LAS DOS HERRAMIENTAS PARA LA VISUALIZACION DE DATOS?**

Las dos herramientas para la visualización de datos son:

* Sistema de información geográfica (GIS).
* Sistemas de minería de la realidad (Reality Mining).

La minería de la realidad integra GIS y GPS permitiendo extraer información de uso de teléfonos móviles y otros dispositivos inalámbricos.

**30-QUE SON LAS TENDENCIAS SOLOMO?**

Las tendencias de SOLOMO como su nombre lo indica, se refiere a: Social, Location, Mobile. Dichas tendencias ayudaron al crecimiento de Big Data.

**31-CUAL ES LA DEFINICION DE CLOUD COMPUTING?**

Cloud Computing proporciona soluciones de cómputo para la gestión, descubrimiento, acceso y procesamiento de los Big Data para su conversión en conocimiento y el consiguiente soporte a la toma de decisiones. El desplazamiento de los modelos TIC (Tecnología de la información y comunicaciones) tradicionales hacia la nube correrán en paralelo con el crecimiento de Big Data. Es un modelo que permite el acceso ubicuo (omnipresente), adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables compartidos (por

ejemplo redes, servidores, equipos de almacenamiento, aplicaciones y servicios) que pueden ser provisionados y liberados rápidamente con el mínimo esfuerzo de gestión o interacción con el proveedor del servicio.

**32-CUALES SON LOS MODELOS DE CLOUD COMPUTING?**

Los modelos son infraestructura, plataforma y servicio. Es decir, puede ser una aplicación a la que se accede a través del escritorio y se ejecuta inmediatamente tras su descarga o bien un servidor al que se invocará cuando se necesite.en la nube no se instala nada en su escritorio y no se paga por tecnología cuando no se la usa, solo se paga cuando se usa o se ejecuta la aplicación. en la práctica la computación en la nube proporciona un servicio de software o hardware.

**33-EN QUE CONSISTE EL MODELO DE SERVICIO ( IaaS, PaaS, Saas)?**

**Iass:** (infraestructura como servicio) el proveedor ofrece al usuario recursos como capacidad de procesamiento, de almacenamiento, comunicaciones y otros recursos de computación donde el consumidor es capaz de desplegar y ejecutar software específico que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura fundamental de la nube, pero tiene control sobre sistemas operativos, almacenamiento, aplicaciones desplegadas ; y posiblemente, un control limitado de componentes seleccionados de redes(host firewalls etc).

**PasS:** (plataforma como servicio) al usuario se le permite desplegar aplicaciones propias sean adquiridas o desarrolladas por el propio usuario) creadas usando lenguajes y herramientas de programación soportadas por el proveedor. El consumidor no administra ni controla la infraestructura de la nube, incluyendo redes, servidores, sistemas operativos ni almacenamiento de su proveedor. que es quien ofrece la plataforma de desarrollo y las herramientas de programación. El usuario tiene control sobre las aplicaciones desplegadas y es quien mantiene su control, aunque no de toda la infraestructura subyacente.

**Sass:** (software como servicio) al usuario se le ofrece la capacidad de que las aplicaciones infraestructura de la nube , siendo dichas aplicaciones accesibles a través de una interfaz del cliente tal como un navegador web (correo electrónico, gmail o yahoo) o una interfaz de programa.

El usuario carece de cualquier control sobre la infraestructura de la nube, como servidores, sistemas operativos, almacenamiento, incluso sobre las propias aplicaciones, excepto por las posibles configuraciones de usuario o personalizaciones que se le permita realizar.

**34-NOMBRE Y DESCRIBA DOS DE LAS CINCO CARACTERISTICAS DEL MODELO.**

**UBICUIDAD**

Posibilidad ofrecida a los usuarios de acceder a los servicios contratados de Cloud Computing desde cualquier dispositivo ,en cualquier lugar y en cualquier momento, siempre cuando se disponga de conexión a redes de internet.

**ESCALABILIDAD**

Es la propiedad de aumentar la capacidad de trabajo o de tamaño de un sistema sin comprometer el funcionamiento y calidad normales del mismo. Escalabilidad se puede aplicar también a la funcionalidad de un sistema. Si se le pueden agregar funciones nuevas con un esfuerzo mínimo, se dice que el sistema es escalable.

**35-COMO ES EL MODELO DE DESPLIEGUE QUE COSA SE LE OFRECE AL USUARIO O AL CONSUMIDOR EN SaaS, PaaS, IaaS?**

El NIST define 4 modelos de despliegue dentro del entorno de Cloud Computing

**Nubes Públicas:** La denominación de Cloud Público o Nube Pública hace referencia al modelo estándar de Cloud Computing, en donde el prestador de estos servicios pone a disposición de cualquier usuario en Internet su infraestructura, es decir, permite al usuario el uso de su software o hardware en forma libre o mediante el pago de una suma de dinero por el tiempo de uso de los mismos.

**Nubes Privadas:** Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. Las nubes privadas están en una infraestructura en-demanda manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.

**Nube Comunitaria:** La infraestructura de esta nube es compartida por varias organizaciones y apoya las preocupaciones de una comunidad particular sobre un tema específico, por ejemplo, seguridad, investigación, políticas o cumplimientos. Puede ser administrada por la organización o por un tercero y puede existir dentro de la misma, “on premises” o fuera de la misma, “off premises”.

**Nubes Híbridas:** La infraestructura de la nube está compuesta por dos o más tipos de nubes (privada, pública o comunitaria) que mantienen su propia identidad pero que son unidas por una tecnología propietaria o estándar para permitir la portabilidad de datos y aplicaciones.

**36-QUE SON LOS CODIGOS QR Y BIDI?**

Los códigos QR (QR por su significado en inglés Quick Response, o código de respuesta rápida) son un tipo de códigos de barra. A diferencia de un código de barras convencional, la información está codificada dentro de un cuadrado, el cual permite almacenar gran cantidad de información alfanumérica.

Un código Bidi es un sistema de codificación, parecido a un código de barras, al nivel de estructura se asemeja mucho a un código QR, la diferencia entre estos códigos son los derechos de autor de este último. Los códigos BIDI son privados o de código cerrado, la compañía de telefonía móvil Movistar fue la primera en lanzar este sistema en el año 2008 para hacer publicidad de sus productos, y después se han apuntado otras compañías como Vodafone y Orange.

**37-CUALES SON LAS FUENTES DE BIG DATA?**

El Big Data consiste en acaparar el mayor volumen de información y seleccionar la más relevante, oodemos diferenciar distintos tipos de fuentes en función de distintas características, por ejemplo. su procedencia o de si son fuentes pagas o no.

* **Bases de datos:** las bases de datos tanto relacionales (usan SQL) como no relacionales están consideradas como una de las principales fuentes de datos dada la gran cantidad de datos que son capaces de almacenar.
* **IoT**: con la aparición de todos los dispositivos capaces de conectarse a internet e interactuar de forma autónoma, el Internet de las Cosas se ha posicionado en los últimos años como una de las mejores fuentes de datos.
* **Redes sociales**: Las redes sociales permiten medir las respuestas que dan los usuarios sobre ciertos productos o servicios, lo que se traduce en datos que pueden ser analizados a través de herramientas y por lo tanto, permiten ofrecer una respuesta en tiempo real a los consumidores.
* **CMS**: Son considerados fuentes de datos dada la cantidad de datos generados y asociados a los usuarios, lo cual, permite a muchas empresas nuevas oportunidades de negocios en relación con las acciones que realizan los usuarios en este tipo de plataformas.
* **ERP**: los sistemas de gestión empresarial, se consideran una fuente de datos excelente para llevar a cabo análisis dentro de una empresa con el fin de encontrar posibles riesgos y mejoras dentro de la misma.
* **CRM**: los sistemas que gestionan las relaciones con los clientes. Se consideran una fuente de datos importante ya que permiten atraer nuevos clientes, sobre todo cuando los clientes son la principal fuente de ingresos de las empresas.

**38-CUAL ES LA PRINCIPAL CARACTERISTICA DE HADOOP?**

Hadoop es un framework opensource para almacenar datos y ejecutar aplicaciones en clusters de hardware básicos. Nace como iniciativa de Apache para dar soporte al paradigma de programación Map-Reduce, que fue inicialmente publicado por Google. Proporciona un almacenamiento masivo para cualquier tipo de datos, un enorme poder de procesamiento y la capacidad de manejar tareas o trabajos prácticamente ilimitados. Esto se consigue mediante la ejecución distribuida de código en múltiples nodos (máquinas), cada uno de los cuales se encarga de procesar una parte del trabajo a realizar.

La principal característica de Hadoop es la posibilidad de hacer procesamiento distribuido de datos, esto se consigue con un esquema de almacenamiento distribuido (HDFS) en el que cada nodo almacena un fragmento de la información y una forma de estructurar el tratamiento de los datos que posibilita que cada nodo pueda tratar los datos de su propio nodo.

**39-NOMBRE ALGUNOS TIPOS DE ANALITICA.**

Una de las características más importantes para los analistas de datos es la habilidad de traducir datos en descubrimientos que son claros e importantes para la persona que toma las decisiones. Para esto es importante conocer algunos tipos de analiticas que nos ayudarán a clasificar los datos.

* **Análisis descriptivo**

El análisis descriptivo se utiliza cuando la organización tiene un gran conjunto de datos sobre eventos pasados o sucesos históricos. Para que estos datos sean útiles, deben simplificarse y resumirse con el fin de que sean entendibles para la audiencia a la que se quieren comunicar.

* **Análisis predictivo**

Al utilizarlos con esta gran masa de datos, podemos pronosticar con cierta probabilidad lo que podría llegar a suceder. El análisis predictivo es, entonces, la aplicación de estas técnicas y modelos matemáticos y estadísticos a los datos históricos que posee la organización.

* **Análisis prescriptivo**

Cuantifica el efecto de cada una de estas acciones para ayudar a tomar las mejores decisiones en pro de buscar los objetivos de negocio de la organización

**40-DENTRO DE ANALITICA DE DATOS, CUALES SON LAS TECNICAS MAS USADAS?**

**Test A/B**

Se denomina así a los experimentos aleatorios con dos variables para medir cuál funciona mejor.

**Crowdsourcing**

Es una técnica de recogida de datos proporcionados por grupo de gente o comunidad grande.

**Media aritmética**

Es la suma de una lista de números dividida por el número de elementos en esa lista y se usa para determinar la tendencia general de un conjunto de datos. Hallar el promedio también sirve para obtener una instantánea rápida de la información, puesto que es fácil de calcular

**Regresión**

Sirve para determinar tendencias a lo largo del tiempo, ya que modela las relaciones entre variables dependientes y explicativas, que generalmente se grafican en un diagrama de dispersión, indicando si los vínculos que existen son fuertes o débiles.

**Minería de datos**

El Data Mining son técnicas que extraen patrones de bases de datos amplias, combinando métodos como la estadística o el Machine Learning.

**41-NOMBRE ALGUNAS METRICAS.**

* CTR (ratio de clicks) es el número de clics que obtiene un enlace respecto a su número de impresiones. Siempre se calcula en porcentaje, y es una métrica que se utiliza normalmente para medir el impacto que ha tenido una campaña digital.
* CAC (coste de adquisición) el coste de adquisición de cliente o CAC es la inversión económica que hemos hecho para conseguir que un consumidor potencial se convierta en una conversión final y adquiera nuestro producto o servicio.

**42-QUE ES EL MOVIMIENTO BYOD?**

Bring Your Own Device (BYOD) es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

**43-QUE SIGNIFICAN LOS TERMINOS CONSUMERIZACION, CROWDSOURCING Y**

**CROWDFOUNDING?**

La **consumerización** es el proceso mediante el cual los usuarios llevan sus propios dispositivos (notebooks, smartphones y tablets) al entorno corporativo y demandan acceso a aplicaciones, datos y servicios para ser productivos, consiste en que los usuarios deciden qué dispositivos, aplicaciones y servicios usan en el trabajo.

El **Crowdsourcing** que es una herramienta para externalizar tareas y así disminuir la carga de trabajo de los miembros de una empresa. Además aporta creatividad y aire fresco a determinados procesos dentro de una organización, ya que ofrece la posibilidad de escuchar e integrar nuevas ideas. El Crowdsourcing busca externalizar o delegar tareas para dejarlas a cargo de un grupo numeroso de personas o comunidad. Esta comunidad, compuesta por profesionales cualificados presentará sus propuestas, ideas y candidaturas.

El **crowdfunding** es una red de financiación colectiva, normalmente online, que a través de donaciones económicas o de otro tipo, consiguen financiar un determinado proyecto a cambio de recompensas, participaciones de forma altruista.

**Criptografía aplicada al trabajo práctico de marketing comercial**

**1-** **Respecto de la autenticación, hay dos cosas que se autentican. ¿Cuáles son?**

Autenticación de entidades y Autenticación de orígenes de datos (incluye la integridad de los datos).

**2-** **¿Cuál es la principal virtud de una función resumen o de hashing? ¿Cuáles son sus aplicaciones?**

Corresponden al aseguramiento de que una información no haya sido alterada por personas no autorizadas o por cualquier otro medio desconocido.  
Concretamente, una función hashing recibe como entrada una cadena de símbolos y da como resultado una cadena de longitud fija, de modo tal que si se altera algún carácter de la cadena de entrada, el nuevo resultado será distinto al original.

Algunas de sus aplicaciones son:

* Al publicar archivos en la web, para detectar si fue alterado.
* En informática forense, para detectar si un disco que posee la justicia fue alterado.
* Autenticación remota de usuarios.
* Seguridad en monedas virtuales.
* Firmas digitales.

**3-** **¿Cuál es la debilidad del cifrado simétrico?**

Los métodos simétricos se caracterizan por usar la misma clave para cifrar y descifrar. De esta forma, el emisor y el receptor deben estar comunicados para compartir la clave.  
El problema es la transmisión de esta información sensible, que no solo genera vulnerabilidades, sino que acarrea grandes costos.  
Esto puede solucionarse con un cifrado de clave pública, que resuelve el problema de la distribución segura de la clave y permite la firma digital o la autenticación en sitios web. Es ideal en el comercio electrónico para realizar transacciones seguras.

**4-** **¿Cuáles son las teorías relacionadas con la criptografía?**

* Teoría de la Información: consiste en el estudio de la cantidad de información contenida en los mensajes y llaves, así como su entropía. Sirve para medir la cantidad de información que contienen los mensajes o la información a cifrar.
* Teoría de los Números: se basa en el estudio de las matemáticas discretas y cuerpos finitos que permiten las operaciones de cifrado y descifrado.
* Teoría de la complejidad de algoritmos: consiste en el estudio de la clasificación de los problemas como computacionalmente tratables o intratables. Posibilita conocer la fortaleza de un algoritmo y conocer su vulnerabilidad.

**5-** **¿En qué consisten la Teoría de la Confusión y de Difusión?**

Permiten ocultar o disimular las redundancias en el texto-plano.  
La Teoría de la Confusión disminuye las relaciones entre el texto-plano y el texto cifrado para frustrar los intentos de estudio de este en busca de patrones (conocido como “sustitución”).  
La Teoría de la Difusión disipará la redundancia del texto-plano cambiando el orden del texto-plano en el texto cifrado al cifrar (conocido como “transposición”).

**6-** **Respecto de la Teoría de Números hay un concepto fundamental de aritmética modulas que es el que permite el uso de cifrado asimétrico. ¿Cuál es ese concepto?**

El concepto principal es la **congruencia** que es la base en la que se sustentan las operaciones de cifrado en matemática discreta.

**7-** **Siguiendo con la Teoría de Números existen otros conceptos que se aplican a RSA. ¿Cuáles son?**

El algoritmo RSA establece que para la generación del par de claves pública y privada se deban seleccionar dos números grandes aleatorios del orden de los 200 o más dígitos para calcular su producto.

**8-** **La complejidad algorítmica es mensurada por dos variables, ¿Cuáles son?**

Por la Complejidad de Tiempo (T) y la Complejidad de Espacio o Requerimiento de Memoria (S). Ambas se expresan en función de *n*, siendo este el tamaño de entrada.

**9-** **¿Cuál es el mecanismo entre el emisor y el receptor cuando hablamos de cifrado asimétrico?**

Se utilizan dos claves o llaves criptográficas (una privada y una pública) relacionadas matemáticamente que se combinan. Cuando una entidad cifra un mensaje con la clave privada, este puede ser descifrado mediante la clave pública.  
Esto soluciona el problema de intercambiar claves que posee el método simétrico.

**10-** **¿En qué está basada la seguridad de RSA?**

El algoritmo RSA es el algoritmo de cifrado asimétrico más popular. Este fue creado en 1977 y aun no ha sido crackeado, aunque tampoco haya sido demostrado que sea matemáticamente seguro.  
Hoy se lo considera seguro si se usan llaves de longitud suficientemente alta (suelen ser de 1024 o 2048 bits) y si se usan esquemas de padding seguros. Debe usarse un padding criptográfico como el definido en el estándar PKCS#1 para completar o “paddear” el mensaje previo a la encriptación.  
Su seguridad entonces está basada en la **dificultad de hacer el factoreo de números grandes**.

**Cuestionario de Uso de Certificado Digital**

1. **Grafique o explique la diferencia entre clave pública y clave privada.**

La clave pública es la que el receptor le da al emisor y le pide que use esa clave para cifrar los datos que se quieren transmitir. La clave privada es la que el receptor usará para descifrar la información enviada por el emisor. Solo la clave privada relacionada con la clave pública puede desencriptar ese mensaje.

1. **¿Cuál es la relación u operación matemática (aritmética) que vincula a las claves pública y privada?**

El cifrado se hace utilizando la siguiente fórmula:

c = m^e (mod n)

El descifrado se hace con la siguiente fórmula:

M = c^d (mod n)

Donde:

· m = mensaje original.

· c = mensaje cifrado resultante.

· e = llave pública del receptor.

· d = llave privada del receptor.

1. **Grafique o explique en qué forma se verifica la identidad.**

La identidad se verifica con el mismo mecanismo de clave pública y privada.

1. El emisor envía su clave pública al receptor.

2. El emisor cifra el mensaje con su clave privada.

3. El emisor envía el mensaje cifrado al receptor.

4. El receptor descifra el mensaje con la clave pública del emisor.

De esta forma se verifica la identidad, porque la única forma de descifrar el mensaje con la clave pública es si fue cifrado con la clave privada, y el emisor es el único que la posee.

1. **Grafique o explique la generación de la firma digital y su verificación.**

Se usa el mismo principio que la pregunta anterior. Al mensaje se le hace un hash y se lo cifra con la clave privada del emisor (firma digital). Luego el emisor envía el mensaje junto con la firma digital para que el receptor los descifre con la clave pública y haga la misma operación de hash sobre el mensaje. Si ambos hashes coinciden, se verifica la firma.

1. **Describa los campos de un certificado digital.**

· La versión de formato usado por el certificado.

· El número de serie usado por el certificado.

· El identificador del algoritmo usado para firmar el certificado.

· La entidad que emitió el certificado.

· La fecha inicial y la fecha de caducidad del certificado.

· El nombre del propietario.

· La clave pública del propietario.

· La firma digital de la entidad certificadora que emitió el certificado.

1. **Existen 4 tipos de certificados. Explique 1.**

Certificados de servidor: permiten la identificación de los servidores que utilizan los protocolos de comunicación segura, por ejemplo, SSL. Estos certificados permiten al usuario verificar el servidor o el sitio Web antes de enviarle información confidencial.

1. **¿Cómo es el uso de un certificado personal?**

Un certificado personal se utiliza para dos fines: autenticación del cliente y firma y cifrado de mensajes de correo electrónico. Cuando se accede a un sitio web que requiere la autenticación por medio de certificados, nuestro navegador envía nuestro certificado al servidor web permitiendo así que se verifique nuestra identidad. El certificado personal también lo podemos usar en el programa de correo electrónico para firmar un mensaje, permitiendo al receptor la verificación que el mensaje ha sido enviado efectivamente por nosotros y además que el mensaje no sufrió alteraciones.

1. **Grafique o explique la vida de un certificado.**

Los certificados tienen una vida limitada. Se solicitan, se crean y, después, en algún momento, expiran o son rechazados. Un certificado revocado se incluirá en una lista de certificados revocados que es gestionada por la entidad emisora de certificados; al comprobar un certificado debe verificarse esta lista.

1. **Quiero emitir, revocar y gestionar certificados, convirtiéndome en mi propia entidad emisora. ¿Qué debo hacer?**

La configuración de nuestra propia entidad emisora de certificados requiere como mínimo estos recursos adicionales en nuestro sistema:

· Servidor de certificados: es un servidor habilitado para emitir certificados, gestionar su contenido, definir la política de emisión y de revocación.

· Herramienta para establecer la relación de confianza con el cliente: el cliente no confiará en nosotros porque no nos reconocerán necesariamente como entidad emisora de certificados, lo que mostrará una advertencia en el navegador del usuario. Tenemos que suministrar los medios para establecer esa confianza entre nuestra entidad y nuestros clientes del sitio web instalando el certificado de entidad emisora de certificados en el navegador.

· Una herramienta para emitir certificados de cliente: aunque podemos elegir nuestro propio modo para emitir certificados de cliente, la mejor forma de distribuirlos es por medio de un formulario en línea para solicitar el certificado.