| PROGRAMA DE FORMACIÓN | Atención comercial y operación en seguros |
| --- | --- |

| COMPETENCIA | 220501114. Sistematización de datos masivos. | RESULTADOS DE APRENDIZAJE | 220501114-04. Evaluar la calidad de la información obtenida de acuerdo con requerimientos de la organización.  220501114-05. Optimizar los modelos construidos de acuerdo con el concepto del usuario. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 8 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Validación de información y optimización del modelo desarrollado |
| BREVE DESCRIPCIÓN | En este componente formativo, se van a desarrollar conceptos generales sobre los diferentes aspectos legales en la validación de datos; de igual manera, cómo cuidar la seguridad de la información, junto con la identificación de problemas y cómo corregirlos; finalmente, alcanzar la optimización del uso de los recursos y la implementación de los procesos, con la utilización de datos masivos. |
| PALABRAS CLAVE | Derechos de autor, seguridad de la información, *Big data*, ingeniería de requisitos. |

| ÁREA OCUPACIONAL | Finanzas y administración |
| --- | --- |
| IDIOMA | Español |

TABLA DE CONTENIDOS

1. **Validación datos legales y seguridad de la información**

1.1 Derechos de autor: políticas de confidencialidad

1.2 Seguridad de la información

1.3 Técnicas de gestión de datos masivos

**2. Optimización del modelo de gestión de datos masivos**

2.1 Ingeniería de requisitos

2.2 Políticas de seguridad de la información

**INTRODUCCIÓN**

| Cuadro de texto |
| --- |
| Apreciado aprendiz, bienvenido a este componente formativo, en el que conocerá acerca de los derechos de autor, los métodos de representación en la ingeniería de requisitos, la seguridad de la información y las técnicas de la gestión de datos masivos, lo que le permitirá adquirir una visión más amplia e identificar, con claridad, los diferentes aspectos legales al utilizar datos y velar por la seguridad de la información. Por otra parte, conseguirá identificar problemas a la hora de implementar procesos y logrará corregirlos optimizando el uso de los recursos.  En el siguiente video conocerá, de forma general, la temática que se estudiará a lo largo del componente formativo. |

| **Tipo de recurso** | Video motion | | | |
| --- | --- | --- | --- | --- |
| **NOTA** |  | | | |
| **Título** | Introducción | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| Escena 1 | Equality Company | Validación de Identidad | N/A | En este componente formativo, se abordarán temáticas relacionadas con la validación de la información en las organizaciones y la optimización de un modelo que le permitirá gestionar datos de forma masiva. | Validación de la información |
| Escena 2 | Derechos de Autor - My Brand | Legal Solutions | N/A | Para iniciar, se presenta la protección de los derechos de autor y la propiedad intelectual, que son los pilares del desarrollo de la protección del patrimonio, ya sea de las personas o de las empresas. Cuando se abordan desarrollos propios de *software*, en las organizaciones se habla específicamente de los derechos de autor**.** Es de resaltar que, además de proteger los activos creativos de las empresas, se torna necesario generar una cultura de protección de los derechos morales y, asimismo, motivar al interior de la empresa, la creatividad y la innovación. | Derechos de autor |
| Escena 3 | La Seguridad de la Información: Historia, Terminología y Campo de acción |  Desde Linux | N/A | Por otro lado, se entiende que la **prevención** es la clave primordial de la **seguridad informática**, porque es imperativo evitar el robo, alteración, o acceso a la información, en las áreas de la empresa. Adicionalmente, permite detectar amenazas de virus y riesgos en los sistemas de información internos.  Hoy en día, las empresas cuentan con datos muy sensibles en su base de datos, tales como: grabaciones de llamadas telefónicas, información financiera y las inversiones, clientes, entre otras, que actualmente son el objetivo de los piratas informáticos que desean alterar la ciberseguridad corporativa. Por lo anterior, las empresas desde sus departamentos de sistemas, deben considerar a estas bases de datos como un activo de protección. | Seguridad de la información |
| Escena 4 | Curso Online de Ingeniería de requisitos: Software orientado al negocio -  La Oficina de Proyectos de Informática | N/A | También se presentará **la ingeniería de requisitos**, como un componente clave para poder medir la calidad de los sistemas informáticos que son utilizados y desarrollados por los equipos de sistemas. Esta se puede expresar como un conjunto de pruebas que el sistema debe transitar para cumplir con los requisitos especificados y asegurarse que se encuentre en buen estado y, finalmente, si pasa las pruebas, su operación es válida y funciona correctamente. Una adecuada identificación de las necesidades de ingeniería, garantiza una precisa solución en el área de desarrollo de *software* a la medida. | La ingeniería de requisitos |
| Escena 5 | Bases de datos para Big Data: ¿qué requesitos deben cumplir? | N/A | Para terminar, después de contar con información precisa del modelo y luego que sea validada, se considera que, en el ámbito empresarial, a medida que crece la información y su manejo se vuelve más complejo, es necesario buscar soluciones concretas y, dentro de estas, se encuentra la **utilización de técnicas de manejo de datos masivos**.  Las bases de datos son determinantes en la mayoría de las áreas donde los equipos de cómputo se utilizan para almacenar grandes cantidades de datos, sobre empresas que los usuarios conocen. Además, la información extraída de los datos almacenados debe utilizarse, de alguna forma, para la gestión, planeación, administración y la toma decisiones dentro de la empresa.  Las principales utilidades que las bases de datos brindan a las empresas son:  - Agrupación y almacenamiento de datos para su negocio en un solo lugar.  - Facilitar el intercambio de datos entre varios miembros de la empresa.  - Evitar redundancias y mejorar la organización de las actividades.  Conscientes que su disciplina y estudio de esta temática, generará mejores resultados en el cumplimiento de sus metas, le deseamos éxito en su trabajo profesional. | Técnicas de gestión de datos masivos |
| **Nombre del archivo** | **133305\_v1.mp4** | | |  |

1. **Validación datos legales y seguridad de la información**

| Cuadro de texto |
| --- |
| Para dar inicio al estudio del contenido sobre la validación de datos legales, es importante decir que, primero se debe abordar la temática de **la confidencialidad de la información**, la cual hace referencia a un conjunto de reglas que limita el acceso o impone restricciones en el uso de ciertos tipos de información y suele ejecutarse a través de acuerdos y políticas de confidencialidad. Esta información puede estimarse de dos maneras:   * **La información con preocupaciones de baja confidencialidad** puede considerarse "pública" o no amenazante si se expone más allá de su audiencia prevista. * **La información con preocupaciones de alta confidencialidad,** se considera secreta y debe mantenerse confidencial para evitar el robo de identidad, el compromiso de cuentas y sistemas, daños legales o de reputación, y otras consecuencias graves.     **Imagen: 133305\_i1** |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Ahora bien, **la confidencialidad de los datos** consiste en proteger los datos contra el acceso, la divulgación o el robo no intencionales, ilegales o no autorizados. | |

**1.1 Derechos de autor: políticas de confidencialidad**

| Cuadro de texto |
| --- |
| Las políticas de confidencialidad tienen mejor relevancia, entre mayor sea la información que manejan las empresas y, al mismo tiempo, la importancia de la misma, por lo que la estrategia de protegerla y darle el adecuado uso, se convierte en buenas prácticas de la gestión de la información. |

| **Tipo de recurso** | Tarjetas Avatar | |
| --- | --- | --- |
| **Introducción** | Las políticas de confidencialidad son necesarias para: | |
| Asegurarse que los empleados, clientes y usuarios, comprendan cómo se utilizan sus propios datos personales y quién tiene acceso a ellos. | | **Imagen: 133305\_i2** |
| Aclarar cómo los empleados deben manejar la información confidencial que se les revela durante el curso de su empleo. | | **Imagen: 133305\_i3** |
| Dar a conocer que la falta de protección y seguridad de la información confidencial, no solo puede conducir a la pérdida de negocios o clientes, sino que también se abre al peligro que la información confidencial se utilice para cometer actividades ilegales o inmorales. | | **Imagen: 133305\_i4** |

| Cuadro de texto |
| --- |
| Por otra parte, es importante que las organizaciones conozcan cuándo deben crear las políticas de confidencialidad y qué elementos la deben de conformar para, de esta forma, garantizar un adecuado manejo de la información y que esta no se advierta vulnerada por terceros. |

| **Tipo de recurso** | Slider Presentación | |
| --- | --- | --- |
| **Introducción** | Por esta razón, se presentan algunos puntos que se recomienda tener en cuenta con respecto a las políticas de confidencialidad. | |
| **El alcance**  Las organizaciones establecen políticas de confidencialidad, principalmente, para cumplir con la ley (protección de datos personales y confidencialidad del paciente), y para proteger su ventaja competitiva. | | **Imagen: 133305\_i5** |
| **¿Qué se considera información confidencial?**  Según la organización, la información confidencial puede incluir datos bancarios, resultados de pruebas de pacientes, resultados de exámenes de alumnos, cantidades en la nómina, fórmulas secretas, listas de clientes y contactos, contraseñas, entre otros. | | **Imagen: 133305\_i6** |
| **Medidas de confidencialidad implementadas**  Cómo se manejan los datos personales y cómo los trabajadores deben manejar la información personal que se les revela. Algunos ejemplos podrían incluir guardar bajo llave o asegurar la información confidencial en todo momento, establecer acuerdos de no divulgación y no guardar documentos confidenciales cuando ya no se necesiten. | | **Imagen: 133305\_i7** |
| **Excepciones**  Cuándo se puede divulgar información confidencial por razones legítimas (en caso de una inquietud de protección, si lo exige la ley o para la seguridad pública), y qué procedimiento se tiene que seguir en estas ocasiones. | | **Imagen: 133305\_i8** |
| **Consecuencias disciplinarias por incumplimiento de la política de confidencialidad**  Acción disciplinaria, despido y, potencialmente, acción legal. | | **Imagen: 133305\_i9** |

| Cuadro de texto |
| --- |
| Las empresas e instituciones en sus procesos de operación y funcionamiento, utilizan información altamente sensible de ser reservada y de uso exclusivo de las organizaciones y sus usuarios. |

| **Tipo de recurso** | Carrusel de tarjetas | |
| --- | --- | --- |
| **Introducción** | A continuación, se enlista una serie de ejemplos concerniente a la información confidencial. | |
| **Imagen: 133305\_i10** | | |
| Nombres, fechas de nacimiento, direcciones, datos de contacto (del personal, clientes, pacientes, alumnos, etcétera). | | **Imagen: 133305\_i11** |
| Datos bancarios personales e información de tarjetas de crédito. | | **Imagen: 133305\_i12** |
| Imágenes del personal, alumnos o clientes, que confirman su identidad y pueden vincularse a información personal adicional. | | **Imagen: 133305\_i13** |
| Información de nómina de trabajadores. | | **Imagen: 133305\_i14** |
| Resultados de exámenes médicos. | | **Imagen: 133305\_i15** |
| Iniciativas o proyectos de la empresa. | | **Imagen: 133305\_i16** |
| Información y listas de clientes. | | **Imagen: 133305\_i17** |
| Información de las cuentas financieras de la empresa. | | **Imagen: 133305\_i18** |
| Información relativa a la propiedad intelectual, invención o patente. | | **Imagen: 133305\_i19** |
| Contraseñas e información de TI relacionadas. | | **Imagen: 133305\_i20** |

**1.2 Seguridad de la información**

| Cuadro de texto |
| --- |
| La seguridad de la información se refiere a los principios, las prácticas y las políticas que tienen como objetivo proteger los datos digitales y otros tipos de información. Las responsabilidades incluyen establecer un conjunto de procesos comerciales que protegen los activos de información, independientemente de cómo se formatee, transmita, procese o almacene la información. No obstante, la información siempre podrá estar vulnerable y recibir un **ataque cibernético,** el cual sucede cuando hay un intento deliberado y malicioso de acceder al sistema de información, ya sea de la organización o de un particular.  Con frecuencia, el objetivo de los ataques es financiero pero, algunos que han sido realizados, indican que su fin es el de destruir los datos. Los actores maliciosos muchas veces buscan rescates u otras ganancias financieras, pero los ataques pueden llevarse a cabo por una variedad de motivos, incluyendo razones políticas.    **Imagen: 133305\_i21** |

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | Para conocer más sobre los ataques cibernéticos, a continuación se presentan los más comunes. |
| **Imagen: 133305\_i22** | |
| ***Malware***  Es un término que se utiliza para describir el *software* malicioso, como *spyware*, *ransomware*, virus y gusanos. El malware ingresa a las redes a través de vulnerabilidades. El *software* malicioso, generalmente se instala cuando un usuario hace *clic* en un enlace malicioso o en un archivo adjunto de un correo electrónico. Una vez dentro del sistema, el malware puede:   * Bloquear el acceso a componentes críticos de la red *(ransomware*). * Instalar malware adicional o *software* malicioso. * Desde la unidad, obtener información de forma encubierta, transfiriendo datos (*spyware*). * Destruir ciertos componentes y renderizar el sistema a inoperable. | |
| ***Phishing***  Es la práctica de enviar comunicaciones engañosas, generalmente por correo electrónico, que parecen provenir de una fuente confiable. Su propósito es robar o acceder a datos confidenciales, como las tarjetas de crédito y contraseñas de inicio de sesión, así como también instalar malware en la computadora de la víctima. El *phishing* es cada vez más común como práctica fraudulenta. | |
| ***Man-in-the-middle* (MitM)**  También conocido como espionaje, ocurre cuando un atacante compromete una transacción entre dos partes. Si un atacante interfiere con su tráfico, puede filtrar y robar sus datos.  Las dos maneras de vulnerar la seguridad:  1. El *Wi-Fi* público no seguro, permite que un atacante se interponga entre el dispositivo de su visitante y su red. El visitante, sin saberlo, proporciona toda la información al atacante.  2. Una vez que el malware está en el dispositivo, el atacante puede instalar un *software* que maneja toda la información de la víctima. | |
| **Ataque de denegación de servicio**  Un ataque de denegación de servicio inunda un sistema, servidor o red con tráfico, consumiendo recursos y ancho de banda. Como resultado, el sistema no podrá procesar solicitudes legítimas. Los atacantes también pueden usar múltiples dispositivos comprometidos para lanzar este ataque. Esto se conoce como ataque de denegación de servicio distribuido (DDoS). | |
| **Inyección SQL**  La inyección de lenguaje de consulta estructurado (SQL), ocurre cuando un atacante inyecta un código malicioso en un servidor que usa SQL, lo que hace que el servidor revele información que normalmente no revelaría. Un atacante puede realizar una inyección SQL simplemente enviando un código malicioso al cuadro de búsqueda de un sitio *web* vulnerable. | |
| ***Exploit* de día cero**  Un *exploit* de día cero ocurre después que una vulnerabilidad se ha divulgado públicamente en la red y antes que se implemente un parche o corrección. Los atacantes apuntan a las vulnerabilidades descubiertas durante este tiempo. La detección de amenazas de vulnerabilidad de día cero, requiere una conciencia constante. | |
| **Acceso a DNS**  La tunelización DNS utiliza el protocolo DNS para comunicar el tráfico que no es DNS a través del puerto 53. Envía tráfico HTTP y de otros protocolos a través de DNS. Hay varias razones válidas para usar la tunelización DNS. Sin embargo, también existen razones maliciosas para usar un servicio VPN de túnel DNS. Se pueden usar para disfrazar el tráfico saliente como DNS, ocultando datos que normalmente se comparten a través de una conexión a Internet. Las consultas de DNS se manipulan con la intención maliciosa de extraer datos del sistema comprometido, a la infraestructura del atacante. También se puede usar para devoluciones de llamadas de comando y control, desde la infraestructura del atacante, al sistema comprometido. | |

**Criterios de respaldo y recuperación**

| Cuadro de texto |
| --- |
| Hoy tienen más importancia en las empresas e instituciones, las acciones encaminadas al respaldo y recuperación de la información en cada uno de los procesos de la organización, por lo que se les considera activos muy valiosos.    **Imagen: 133305\_i23**  **¿Qué es una copia de seguridad de datos?**  La copia de seguridad de datos es un método para copiar datos desde una ubicación de almacenamiento principal, a una ubicación de almacenamiento secundaria para proteger sus datos en caso de desastre, accidente o acto malicioso. Los datos son el elemento vital de las empresas modernas, y la pérdida de datos puede causar daños catastróficos e interrumpir las operaciones comerciales. Es por eso que la copia de seguridad de datos es esencial para todas las empresas, grandes y pequeñas.  Por lo general, los datos de respaldo significan todos los datos necesarios para las cargas de trabajo que ejecuta el servidor. Esto puede incluir documentos, archivos multimedia, archivos de configuración, imágenes de máquinas, sistemas operativos y archivos de registro. Esencialmente, cualquier dato que se desee conservar, se puede almacenar como datos de copia de seguridad.  Si bien es posible realizar una copia de seguridad de los datos de forma manual, para garantizar que los sistemas se realicen con regularidad y coherencia, la mayoría de las organizaciones utilizan una solución tecnológica para realizar copias de seguridad de sus datos. |

| **Tipo de recurso** | Infografía interactiva Modal | |
| --- | --- | --- |
| **Texto introductorio** | La copia de seguridad de datos incluye varios conceptos importantes como: | |
|  | | |
| **Código de la imagen** | **133305\_i24** | |
| **Punto modal 1** | Se refiere a un empleado el cual tiene como función asegurarse que los sistemas de respaldo estén configurados correctamente, probarlos periódicamente y asegurarse que los datos críticos, realmente se encuentren respaldados. | **Administrador de copias de seguridad** |
| **Punto modal 2** | Una organización debe decidir sobre una política de copia de seguridad, especificando qué archivos y sistemas son lo suficientemente importantes como para realizar una copia de seguridad y con qué frecuencia se debe realizar la copia de seguridad de los datos. | **Alcance y programación de la copia de seguridad** |
| **Punto modal 3** | RPO se refiere a la cantidad de datos que una organización está dispuesta a perder si ocurre un desastre y está determinado por la frecuencia de la copia de seguridad. Si se realiza una copia de seguridad de los sistemas una vez al día, el RPO es de 24 horas. Cuanto menor sea el RPO, más recursos de red, computación y almacenamiento de datos se requieren, para lograr copias de seguridad frecuentes. | **Objetivo de punto de recuperación (RPO)** |
| **Punto modal 4** | RTO se refiere al tiempo que tarda una organización en restaurar datos o sistemas a partir de una copia de seguridad y reanudar las operaciones normales. Para grandes volúmenes de datos y/o copias de seguridad almacenadas fuera de las instalaciones, la copia de datos y la restauración de sistemas pueden llevar tiempo, y se necesitan soluciones técnicas sólidas para garantizar un RTO bajo. | **Objetivo de tiempo de recuperación (RTO**) |

**Depuración y calidad de datos**

| Cuadro de texto |
| --- |
| La limpieza de datos ha convertido la calidad y la integridad de los datos en una prioridad principal para las organizaciones, lo que facilita la gestión de su confianza en los conocimientos de los datos. Cuando la deficiencia de calidad de los datos no es identificada y validada a tiempo, es posible que se generen ineficiencias operativas, oportunidades desaprovechadas y afectaciones financieras, con lo que se concluye que, una adecuada depuración de datos, es vital para evitar altas pérdidas y afectaciones en la operación. |

| **Tipo de recurso** | Acordeón tipo 1 |
| --- | --- |
| **Introducción** | A continuación, se conocerá más acerca de la depuración de los datos. |
| **Imagen: 133305\_i25** | |
| **Depuración de datos**  La depuración es el primero de los pasos para avanzar en la preparación de los datos, lo que significa que es prioritario identificar y corregir los errores de los datos en su conjunto, de manera que se pueda garantizar que solamente sean enviados los datos limpios y de excelente calidad al el sistema de información, objeto de ser trabajado. | |
| **Importancia en la depuración de datos**  Las tareas de procesamiento y limpieza de datos se convierten en relevantes para que, en los datos clasificados, en un único formato, el *software* de depuración ayude a limpiar y categorizar la información básica, en una etapa más avanzada, relacionada con la limpieza y perfilado de datos que corresponden al análisis de datos; finalmente, esto es lo que posibilita a los analistas encontrar patrones importantes en datos limpios y validados, que permitan apoyar las decisiones comerciales.  A lo anterior se suma que, la actual dependencia hacia las tecnologías y los sistemas de información para la obtención de la información estratégica y de gran relevancia, asimismo la deficiente calidad de los datos, ocasiona un riesgo a la empresa; por lo tanto, al evitar las imprecisiones de los datos, esto hace que la empresa sea más competitiva en el mercado. De lo anterior se concluye, que la empresa debe orientar sus esfuerzos a la rigurosidad en la limpieza de datos, de manera que garantice que los datos son precisos y confiables. | |
| **Diferencia entre depuración de datos y transformación de datos**  Cada vez son más abundantes las cantidades masivas de datos que las empresas manejan en sus operaciones comerciales y empresariales, datos que son almacenados en diferentes formatos y hasta en separados sistemas de información. Lo anterior se debe a que las empresas los crean como almacenes de datos y repositorios centrales, con el objetivo de respaldar, recuperar y analizar la información. En conclusión, la limpieza de datos y la transformación de datos, se definen como dos técnicas que contribuyen a la preparación de los datos comerciales para la integración, creación de informes y su completo análisis.  Uno de los objetivos fundamentales de la depuración de datos, consiste en garantizar la precisión de los mismos, que sean de calidad y se encuentren disponibles para ser analizados y apoyar la toma de decisiones. Un ejemplo clásico en las empresas, es disponer de registros duplicados o información imprecisa, lo que lleva a plantear el interrogante: ¿cómo iniciar la depuración de los datos? | |
| **Revisión de los datos depurados**  Si aún se continúa con algunos datos que pueden ser inconsistentes, es posible que se deba a uno o algunos de los siguientes problemas:   * Duplicaciones debido a múltiples fuentes de datos no coincidentes. * Errores de ingreso de datos, con faltas de ortografía e inconsistencias. * Datos incompletos o campos faltantes. * Errores de puntuación o símbolos no conformes. * Datos desactualizados. * La limpieza de datos toma estos problemas y, utilizando una variedad de métodos, limpia los datos y garantiza que coincidan con las reglas comerciales. | |
| **Características de los datos limpios**  Se utilizan varias características y atributos de datos para medir la limpieza y la calidad general de los conjuntos de datos, incluidos los siguientes: precisión, consistencia, integridad, oportunidad, uniformidad y validez.  Los equipos de administración de datos crean métricas de calidad de datos para rastrear esas características, así como también asuntos como las tasas de error y la cantidad total de errores en los conjuntos de datos. Muchos también intentan identificar el impacto comercial de las problemáticas de calidad de los datos y el valor comercial potencial de solucionarlos en parte, a través de encuestas y entrevistas, con ejecutivos comerciales. | |

| Cuadro de texto |
| --- |
| La mejor alternativa para poder verificar **la calidad de datos** es utilizando herramientas de ETL (*Extract Transform Load*); en primera instancia, cabe mencionar que la transformación y la depuración de datos, son conceptos diferentes; por otra parte, no obstante, son variadas las herramientas ETL que ofrecen características avanzadas de depuración, creación de perfiles y transformación de datos en la gestión de datos complejos; asimismo, en la migración de datos y la gestión de los mismos. |

**1.3 Técnicas de gestión de datos masivos**

| Cuadro de texto |
| --- |
| Las técnicas de gestión de datos masivos permiten, de manera efectiva, dar un manejo apropiado a la información que sirva de base para la toma de decisiones y la disposición de información de calidad en cualquier momento.  La gestión de los datos masivos, comprende el manejo y uso de las políticas, los procedimientos y las tecnologías que son utilizados para la recopilación, almacenamiento, administración, organización, recopilación y entrega de grandes cantidades de datos. En ese sentido, incluye la depuración de datos, la migración, la integración y la preparación para la generación de informes y sus posteriores análisis. |

| **Tipo de recurso** | Tarjetas Avatar | |
| --- | --- | --- |
| **Introducción** | La *Big data* hace referencia a los almacenes de datos que se caracterizan por las "3 V". | |
| Altos volúmenes de información. | | **Imagen: 133305\_i26** |
| Alta velocidad de procesamiento. | | **Imagen: 133305\_i27** |
| Amplia variedad en técnicas de gestión. | | **Imagen: 133305\_i28** |

| Cuadro de texto |
| --- |
| Por otra parte, se encuentra estrechamente vinculada con el tema de gestión del ciclo de vida de los datos (DLM), el cual hace referencia a un enfoque basado en políticas para determinar qué información se debe almacenar, en qué lugar del entorno de TI de una organización y cuándo se pueden eliminar los datos de manera segura. Debido a que el *Big data* puede almacenar, procesar y gestionar la información de muchas organizaciones, este se encuentra en constante crecimiento y puede llegar a superar su capacidad, e incluso presentar otras contingencias. |

| **Tipo de recurso** | Rutas / Pasos. Verticales 1 |
| --- | --- |
| **Introducción** | Así mismo, a continuación, se hace énfasis en algunos tipos de contingencias que se pueden presentar. |
| **Imagen: 133305\_i29** | |
| **Botón 1** | **Silos de datos**  Algunas áreas o departamentos dentro de una empresa, pueden usar diferentes aplicaciones para almacenar información en diversas bases de datos que contienen información similar, pero muchos de los datos en las bases de información no son homogéneos. Considerar el caso de un minorista que almacena las direcciones de los clientes en su base de datos de *marketing*, base de datos de servicio al cliente, base de datos de contabilidad y base de datos del sitio web de comercio electrónico. En otras palabras, si solo una de estas bases de datos contiene información ligeramente diferente sobre un cliente en particular, la dirección del cliente puede aparecer como "Avenida" y en la otra base de datos como "Calle". El resultado es que se pueden enfrentar conflictos en los correos electrónicos duplicados, falta de seguimiento, registros de errores de servicio al cliente, facturación duplicada e informes inexactos. |
| **Botón 2** | **Almacenes de datos en crecimiento**  La gestión de *Big data* se dificulta porque, la dimensión de los datos trabajados, son de gran tamaño y con tendencia al crecimiento. Tomando de referencia el caso de la dirección del cliente, es muy fácil corregirlo en una empresa pequeña con apenas un centenar de clientes. Por lo anterior, el error es fácil de identificar y, por ende, darle una solución de manera inmediata. Pero con minoristas y mayoristas y con millones de clientes y petabytes de datos, se necesitan diferentes soluciones**.** Con frecuencia es mover datos, de una base de datos a una solución de análisis y se requiere algo de tiempo por la gran cantidad de información. |
| **Botón 3** | **Alta complejidad de datos y su arquitectura**  Los datos comerciales no se almacenan en varios silos, crecen constantemente y pueden volverse muy complejos. Las organizaciones, normalmente tienen datos estructurados (datos que residen en bases de datos) y datos no estructurados (datos que residen en documentos de texto, imágenes, videos, archivos de audio, presentaciones, etc.), y estos datos son compartidos por la organización o miles de aplicaciones propias. Su sistema permite escribir y leer desde varias bases de datos. Como resultado, se vuelve difícil catalogar los tipos de datos que existen en los sistemas de almacenamiento de una organización. |
| **Botón 4** | **Asegurar la calidad de los datos**  Estas oportunidades de mejora, dificultan que las organizaciones garanticen la confiabilidad y precisión de los datos. Como se mencionó anteriormente, los silos de datos no sincronizados dificultan que los administradores determinen qué datos son correctos. Otro factor que limita la calidad de los datos es el error humano. |
| **Botón 5** | **Dotación de personal inadecuado**  Otro gran problema que complica la gestión de datos es la falta de personal cualificado. Pocos científicos de datos o algunos profesionales de *Big data* pueden cubrir todas las ofertas de trabajo actuales. Vale la pena señalar que los salarios pueden estar por encima del promedio del mercado. |
| **Botón 6** | **Falta de apoyo ejecutivo**  Otro problema con la gestión de datos a gran escala, son los gerentes y ejecutivos que no entienden la importancia y el valor de una buena gestión de datos. La tecnología de análisis predictivo y la inteligencia artificial, pueden atraer mucha atención y presupuesto, pero el proceso mundano de mover y limpiar datos es menos emocionante. Sin embargo, este problema parece haber disminuido algo. |
| **Botón 7** | **Incorporación de una cultura amigable con los datos**  El paso de una cultura de toma de decisiones basada en la intuición, la opinión o la experiencia, a una cultura basada en datos, es un cambio relevante para todas las empresas. Este cambio de mentalidad entre los empleados y gerentes llevará tiempo; inclusive, la mayoría de los expertos están de acuerdo en que la gestión eficaz de *Big data* se toma su tiempo. |

**2. Optimización del modelo de gestión de datos masivos**

| Cuadro de texto |
| --- |
| La gestión de requisitos (RM) es un desafío para muchas empresas, en gran parte debido a la ambigüedad que implica el desarrollo de *software*. En primer lugar, se deben comprender los requisitos del cliente. En segundo lugar, se obliga a coincidir esos requisitos, con los procesos críticos.  Los clientes tienen una larga lista de objetivos al crear un nuevo *software*, y RE proporciona un marco para cumplir esos objetivos. Las necesidades importantes se inventan y se transforman en un conjunto detallado de requisitos. El desarrollo de requisitos dicta las futuras actividades de desarrollo y crea un modelo para el éxito.    **Imagen: 133305\_i30** |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| Los términos "gestión de requisitos" e "ingeniería de requisitos" normalmente se usan indistintamente, pero son diferentes. RM es una parte de la ingeniería de requisitos, y hacerlo bien marca la diferencia. | |

**2.1 Ingeniería de requisitos**

| Cuadro de texto |
| --- |
| El cumplimiento de los requerimientos de ingeniería hace parte fundamental para garantizar una efectividad en el desarrollo del *software* o aplicaciones en las organizaciones; en este sentido, es garantía de contar un resultado validado y en correcto funcionamiento. |

**Métodos de representación**

| Cuadro de texto |
| --- |
| Los métodos de representación utilizan símbolos predefinidos para transformar visual y gráficamente los pasos de un proceso, sus tareas y actividades, sus agentes, entradas y salidas para que el proceso se pueda entender y analizar completamente. Los métodos de representación permiten una mejor visualización de los modelos a través de flujos, diagramas, estructuras o secuencias. |

| **Tipo de recurso** | Pestañas o tabs horizontales | |
| --- | --- | --- |
| **Introducción** | A continuación, se explican cada uno de estos métodos de representación. | |
| **Modelado y notación de procesos comerciales (BPMN)** | El modelado y notación de procesos comerciales, se utiliza para crear gráficos que simplifican la comprensión del proceso mercantil. Es una técnica popular utilizada por los analistas de negocios para coordinar la secuencia de mensajes entre diferentes participantes, en un conjunto relacionado de actividades.  BPMN (modelado y notación de procesos comerciales) es una representación gráfica del proceso comercial, utilizando objetos simples, lo que ayuda a la organización a comunicarse de forma estándar. Varios objetos utilizados en BPMN incluyen:   * Objetos de flujo. * Conectando objetos. * Carriles de natación o piscinas. * Artefactos. | **Imagen: 133305\_i31** |
| **Diagramas de flujo** | Los diagramas de flujo representan el flujo secuencial y la lógica de control de un conjunto relacionado de actividades. Son útiles tanto para miembros técnicos, como no técnicos.  Los diagramas de flujo de datos muestran cómo un sistema procesa los datos en términos de entradas y salidas. Los componentes del diagrama de flujo de datos incluyen: proceso, caudal, tienda y terminador.  Un diagrama de flujo de datos lógicos muestra las actividades del sistema, mientras que un diagrama de flujo de datos físicos, muestra la infraestructura de un sistema. Se puede diseñar un diagrama de flujo de datos en las primeras etapas del proceso de obtención de requisitos de la fase de análisis, dentro del ciclo de vida de desarrollo del sistema SDLC, para definir el alcance del proyecto. Para facilitar el análisis, un diagrama de flujo de datos, se puede desglosar en sus subprocesos conocidos como "DFD nivelado". | **Imagen: 133305\_i32** |
| **Diagrama de Gantt** | Estos diagramas proporcionan una representación visual de las tareas, junto con sus cronogramas programados. Ayudan a los analistas de negocios a visualizar las fechas de inicio y finalización de todas las tareas de un proyecto.  Un diagrama de Gantt es una representación gráfica de un cronograma que ayuda a coordinar, planificar y realizar un seguimiento de tareas específicas en un proyecto. Representa el lapso de tiempo total del objeto, desglosado en incrementos. Representa la lista de todas las tareas a realizar en el eje vertical mientras que, en el eje horizontal, enumera la duración estimada de la actividad o el nombre de la persona asignada a la actividad. Un gráfico puede demostrar muchas actividades. | **Imagen: 133305\_i33** |
| **Diagramas de actividad de roles- (RAD)** | El diagrama de actividad de roles es similar a la notación de tipo de diagrama de flujo. En este diagrama, las instancias de roles son participantes del proceso, el cual tiene un estado inicial y uno final. RAD requiere un conocimiento profundo del proceso o de la organización para identificar roles. Los componentes de RAD incluyen: actividades, eventos externos y estados.  Los roles agrupan las actividades en unidades de responsabilidad, de acuerdo con el conjunto de tareas que están desempeñando. Una actividad puede llevarse a cabo aisladamente con un rol, o puede requerir coordinación con actividades en otros roles.  Los eventos externos son los puntos en los que ocurren los cambios de estado.  Los estados son útiles para mapear las actividades de un rol a medida que avanza de un estado a otro. Cuando se alcanza un estado particular, indica que se ha logrado un objetivo determinado.  RAD es útil para apoyar la comunicación, debido a que es fácil de leer y presenta una vista detallada del proceso y permite actividades en paralelo. | **Imagen: 133305\_i34**  **Textos de imagen:**  **Orden del cliente**  **Recibir pedido (proveedor) *marketing***  **Enviar pedido (proveedor) *marketing***  **Orden del cliente**  **Verificar disponibilidad (controlador). Centro de distribución**  **No disponible**  **Ponerse en contacto con el *marketing* del cliente (proveedor)**  **Imprimir factura (distribuidor). Envío**  **Envío producto (distribuidor). Envío** |
| **Redes de Petri coloreadas (CPN)** | Las redes de Petri coloreadas o CPN, son un lenguaje orientado gráficamente para la especificación, verificación, diseño y simulación de sistemas. Las redes de Petri coloreadas son una combinación de gráficos y texto. Sus componentes principales son: lugares, transiciones y arcos dirigidos y marcas o fichas que ocupan posiciones dentro de los lugares.  Los objetos de las redes de Petri tienen una inscripción específica como:  **Lugares.** Tiene inscripción como: nombre, conjunto de colores, marcado inicial.  **Transición.** Tiene una inscripción como: nombre (para identificación) y Guard (la expresión booleana consiste en algunas de las variables).  **Arcos.** Tiene inscripción como: *Arc*, cuando se evalúa la expresión del arco, se obtiene un conjunto múltiple de colores de token. | **Imagen: 133305\_i35** |
| **Técnica de flujo de trabajo** | La técnica de flujo de trabajo es un diagrama visual que representa uno o más procesos comerciales para aclarar la comprensión del proceso o para hacer recomendaciones de mejora del proceso. Al igual que otros diagramas como los diagramas de flujo, la actividad UML y el mapa de procesos, la técnica de flujo de trabajo es la técnica más antigua y popular. El proceso consta de cuatro etapas:   * Recopilación de información. * Modelado de flujo de trabajo. * Modelado de procesos de negocio. * Implementación, verificación y ejecución. | **Imagen: 133305\_i36** |

**Proceso de ingeniería de requisitos**

| Cuadro de texto |
| --- |
| El proceso de ingeniería de requisitos tiene muchas trampas potenciales. El proceso sirve como una brújula que lo guía para determinar los entregables exactos y hacerlo con mayor precisión. Todas las partes importantes están en la misma página sobre qué pasos deben tomarse para lograr el resultado deseado. |

| **Tipo de recurso** | Infografía interactiva Punto caliente | |
| --- | --- | --- |
| **Texto introductorio** | A continuación, se presentan los cuatro pasos del proceso de ingeniería de requisitos. | |
|  | | |
| **Código de la imagen** | **133305\_i37** | |
| **Punto caliente 1** | Consiste en familiarizarse con todos los detalles importantes relacionados con el proyecto. El cliente brinda detalles sobre sus necesidades y aporta antecedentes críticos. Estudia esos detalles y también se familiariza con tipos similares de soluciones de *software*. Este paso proporciona un contexto importante para el desarrollo. | **Obtener requisitos** |
| **Punto caliente 2** | La verificación garantiza que el *software* esté construido según los requisitos del cliente. Por el contrario, la validación garantiza que el *software* esté implementando las funciones correctas. Si los requisitos no pasan por la etapa de validación, existe la posibilidad de reformulaciones costosas y que requieran mucho tiempo. | **Verificación y validación** |
| **Punto caliente 3** | Durante la fase de especificación, reúne los requisitos funcionales y no funcionales del proyecto. Durante esta etapa se utiliza una variedad de herramientas, incluidos los diagramas de flujo de datos, para agregar más claridad a los objetivos del proyecto. | **Especificación de requisitos** |
| **Punto caliente 4** | Es un proceso continuo que se ejecuta en paralelo a los otros tres procesos que se acaban de describir. Las funciones a realizar se enfocan en: analizar, documentar y priorizar los requisitos y, adicionalmente, brindar una efectiva comunicación con las partes interesadas. Cualquier requisito que necesite modificación, se maneja de manera eficiente y sistemática. | **Gestión de requerimientos** |

| Cuadro de texto |
| --- |
| Después de conocer el proceso de ingeniería de requisitos, es importante comprender sobre las herramientas que permiten administrar los proyectos de manera efectiva en la ingeniería de requisitos. |

| **Tipo de recurso** | | Pestañas o tabs Verticales |
| --- | --- | --- |
| **Introducción** | | A continuación, se presentan algunas de estas herramientas. |
| **Imagen: 133305\_i38** | | |
| **Jira** | **Jira**  Es una plataforma creada principalmente para el seguimiento y la gestión de proyectos. Sin embargo, Jira también se puede usar para la ingeniería de requisitos junto con Confluence, lo que le permite rastrear y personalizar docenas de tareas y proyectos con sus requisitos, en un momento dado. Los profesionales de gestión de ingeniería pueden hacer un gran uso de esta plataforma para realizar un seguimiento de las tareas del proyecto (problemas) y crear requisitos a nivel de problema.  La integración de Jira con Confluence, brinda mucho control y personalización a los gerentes de ingeniería. Puede crear los flujos de trabajo de varias maneras y permitir que todos vean las páginas de requisites, en línea con los problemas/tareas de Jira que le correspondan. | |
| **Doc sheets** | **Doc sheets**  Es una de las herramientas de ingeniería de requisitos más eficiente, que ayuda a controlar y personalizar todo el ciclo de vida de un proyecto. La herramienta permite administrar la documentación y hace que la trazabilidad sea más fácil y rápida que nunca. | |
| **Requisitos Hub** | **Requisitos Hub**  Es otra herramienta notable para la gestión de ingeniería de requisitos. Esta herramienta está especialmente diseñada para empresas de *software* y tecnología de información TI, donde la gestión de proyectos puede ser extremadamente complicada. La herramienta viene con cientos de plantillas integradas con docenas de categorías de organizaciones, lo que garantiza que encuentre algo que satisfaga sus necesidades.  Requisitos Hub, brinda mucho control en la administración y priorización de tareas, lo que lo convierte en un gerente de ingeniería de calidad sin mucha documentación que manejar. Una de las mejores cosas de Requisitos Hub es acceder a seminarios web, tutoriales y otro material de aprendizaje cuando compra la herramienta. | |
| **DOORS Next** | **DOORS Next**  Es una de las mejores herramientas de ingeniería de requisitos que contribuye a tener credibilidad. La mejor característica de esta herramienta es su interoperabilidad. DOORS Next, funciona perfectamente bien con otras herramientas para la gestión del ciclo de vida, la colaboración y la creación de informes. | |
| **ReqSuite® RM** | **ReqSuite® RM**  ReqSuite® RM es una herramienta de ingeniería de requisitos, fácil de aprender que ofrece mucho soporte y personalización. Está diseñada específicamente para gerentes de ingeniería que se ocupan de muchos proyectos en un momento dado, por lo que no tienen que pasar meses aprendiendo la herramienta en sí.  La mejor característica de ReqSuite® RM es su sencilla curva de aprendizaje y su facilidad de uso; es perfecta para organizaciones más pequeñas y nuevas empresas. | |
| **Requisitos modernos** | **Requisitos modernos**  Es otra excelente herramienta de ingeniería de requisitos, diseñada para satisfacer las necesidades de las empresas de tecnología moderna. La herramienta proporciona una extensión integrada para Azure DevOps, que muchas organizaciones usan para crear aplicaciones modernas.  Los requisitos modernos, al igual que Jira, tienen una excelente interfaz de usuario y pueden proporcionar bastante automatización en la gestión de proyectos. Lo mejor es que esta única aplicación cubre casi todas las necesidades de los directores de ingeniería. No hay que descargar varias aplicaciones para administrar documentos, colaborar con informes y realizar un seguimiento del rendimiento de un proyecto. | |
| **Spira Team** | **Spira Team**  Está diseñado para realizar un seguimiento del progreso de los proyectos, gestionar los requisitos de ingeniería y controlar la calidad. Esta herramienta se utiliza tanto para la gestión de requisitos, como para el aseguramiento de la calidad, donde se puede rastrear fácilmente el ciclo de vida de un proyecto.  SpiraTeam viene con algunas integraciones que puede usar para la gestión de proyectos, pruebas unitarias y seguimiento de errores. Estas integraciones y la facilidad de uso de esta herramienta de requisitos de ingeniería, la convierten en una solución integral para las organizaciones modernas. | |

**2.2 Políticas de seguridad de la información**

| Cuadro de texto |
| --- |
| Una política de seguridad (también denominada política de seguridad de la Información o política de seguridad de TI), es un documento que detalla las reglas, las expectativas y el enfoque general que utiliza una organización para mantener la confidencialidad, la integridad y la disponibilidad de sus datos.  Las políticas de seguridad existen en muchos niveles diferentes, desde construcciones de alto nivel que describen los objetivos y principios generales de seguridad de una empresa, hasta documentos que abordan problemas específicos, como el acceso remoto o el uso de *Wi-Fi.*  Una política de seguridad se usa con frecuencia, junto con otros tipos de documentación, como los procedimientos operativos estándar. Estos documentos trabajan juntos para ayudar a la empresa a lograr sus objetivos de seguridad. La política define la estrategia general y la postura de seguridad, y los demás documentos ayudan a construir una estructura en torno a esa práctica. Se puede pensar en una política de seguridad como una respuesta al "qué" y al "por qué", mientras que los procedimientos, estándares y directrices, responden al "cómo".  Lo invitamos a ver el siguiente video, donde se amplía la temática sobre seguridad eficaz. |

| **Tipo de recurso** | Video motion | | | |
| --- | --- | --- | --- | --- |
| **NOTA** |  | | | |
| **Título** | Los siete elementos de una política de seguridad eficaz | | | |
| **Escena** | **Imagen** | **Sonido** | **Narración** | **Texto** |
| Escena 1 | Políticas de seguridad para la pyme - YouTube | N/A | A continuación, se hace una descripción de los **siete elementos de una política de seguridad eficaz.**  Las políticas de seguridad son un componente esencial de un programa de seguridad de la información y deben diseñarse, implementarse y aplicarse adecuadamente. Una política de seguridad efectiva debe contener los elementos que se presentarán detalladamente, a continuación. | Los siete elementos de una política de seguridad eficaz |
| Escena 2 | Fije hábitos y objetivos, no propósitos - IEEC | N/A | **Propósito y objetivos claros**  Esto es especialmente importante para las políticas del programa. Recordar que muchos empleados tienen poco conocimiento de las amenazas a la seguridad y pueden ver cualquier tipo de control de seguridad como una carga. Una declaración de misión, propósito y objetivos claros y detallados en el nivel superior de una política de seguridad, debería ayudar a toda la organización a comprender la importancia de la seguridad de la información. | Propósito y objetivos claros |
| Escena 3 | 4.3 Establecimiento del alcance del Sistema de Gestión de Calidad - ISO  9001:2015 | N/A | **Alcance y aplicabilidad**  Cada política de seguridad, independientemente del tipo, debe incluir un alcance o declaración de aplicabilidad que establezca claramente a quién se aplica la política. Esto se puede basar en la región geográfica, la unidad de negocios, el puesto de trabajo, o cualquier otro concepto organizacional, siempre que esté bien definido. | Alcance y aplicabilidad |
| Escena 4 | Liderazgo y compromiso: las dos funciones principales de la Alta Dirección  en el Sistema de Gestión - Blogdelacalidad | N/A | **Compromiso de la alta dirección**  Las políticas de seguridad están destinadas a comunicar la intención de la alta gerencia, idealmente a nivel de la junta directiva. Sin la aceptación de este nivel de liderazgo, es probable que cualquier programa de seguridad fracase. Para tener éxito, sus políticas deben comunicarse a los empleados, actualizarse regularmente y aplicarse de manera consistente. La falta de apoyo de la gerencia, hace que todo esto sea difícil, sino imposible. | Compromiso de la alta dirección |
| Escena 5 | Formas de alcanzar tus objetivos | N/A | **Políticas realistas y ejecutables**  Si bien puede ser tentador basar la política de seguridad en un modelo de perfección, es bueno recordar que los empleados viven en el mundo real. Es probable que una política demasiado onerosa no sea ampliamente adoptada. Del mismo modo, una política sin mecanismo de aplicación podría ser fácilmente ignorada por una cantidad significativa de empleados. | Políticas realistas y ejecutables |
| Escena 6 | Qué Es Pragmático? - Su Definición Y Significado [2022] | N/A | **Definiciones claras de términos importantes**  Recuerde que la audiencia de una política de seguridad, por lo general no es técnica. Es importante un lenguaje conciso y sin jerga, y cualquier término técnico en el documento, debe estar claramente definido. | Definiciones claras de términos importantes |
| Escena 7 | Técnicas de identificación de riesgos | N/A | **Identificación con exactitud de riesgo de la organización**  El riesgo nunca se puede eliminar por completo, pero depende de la gerencia de cada organización decida qué nivel de riesgo es aceptable. Una política de seguridad debe tener en cuenta este apetito por el riesgo, debido a que afectará los tipos de temas cubiertos. | Identificación con exactitud de riesgo de la organización |
| Escena 8 | Actualice su información (Cvlac) o la de su grupo (Gruplac) en Colciencias  | Universidad Central | N/A | **Información actualizada**  Las actualizaciones de la política de seguridad son cruciales para mantener la eficacia. Si bien es posible que no sea necesario cambiar el programa o la política maestra con frecuencia, debe revisarse periódicamente. Las políticas de problemas específicos deberán actualizarse con mayor regularidad a medida que cambian la tecnología, las tendencias de la fuerza laboral y otros factores. Es posible que también se necesiten nuevas políticas de acceso remoto; es un ejemplo de políticas que se han vuelto relevantes durante la última década. | Información actualizada |
| **Nombre del archivo** | **133305\_v2.mp4** | | |  |

**Normativa sobre la seguridad de la información en Colombia**

| Cuadro de texto |
| --- |
| Teniendo en cuenta las temáticas tratadas anteriormente, como los derechos de autor, la confidencialidad y la seguridad de la información, el *Big data*, las políticas de seguridad, entre otras, se hace necesario conocer cuál es la normativa que rige a dicha información en Colombia. |

| **Tipo de recurso** | Slider Hitos/ Línea de tiempo horizontal | |
| --- | --- | --- |
| **Introducción** | Se presenta un recorrido por la normatividad colombiana referida a la seguridad de la información. | |
| **Ley 23 de 1982** | **Ley 23 de 1982**  Propiedad Intelectual - Derechos de Autor. | **Imagen: 133305\_i39** |
| **Ley 80 de 1993** | **Ley 80 de 1993**  El Estatuto General de Contratación de la Administración Pública. |
| **Ley 527 de 1999** | **Ley 527 de 1999**  Se reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. |
| **Directiva presidencial 02 del año 2000** | **Directiva presidencial 02 del año 2000**  Gobierno en línea. |
| **Ley 594 de 2000** | **Ley 594 de 2000**  Ley General de Archivos. |
| **Ley 962 de 2005** | **Ley 962 de 2005**  “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas”. |
| **Ley 1032 de 2006** | **Ley 1032 de 2006**  Habeas Data y se regula el manejo de la información contenida en base de datos personales. |
| **Ley 1150 de 2007** | **Ley 1150 de 2007**  “Seguridad de la información electrónica en contratación en línea”. |
| **Ley 1273 de 2009** | **Ley 1273 de 2009**  "Delitos Informáticos" protección de la información y los datos. |
| **Ley 1341 de 2009** | **Ley 1341 de 2009**  “Tecnologías de la Información y aplicación de seguridad”. |
| **Ley 1437 de 2011** | **Ley 1437 de 2011**  Código de procedimiento administrativo y de lo contencioso administrativo. |
| **CONPES 3701 de 2011** | **CONPES 3701 de 2011**  Lineamientos de Política para Ciberseguridad y Ciberdefensa. |
| **Ley 1581 de 2012** | **Ley 1581 de 2012**  Protección de Datos Personales. |
| **Ley 1712 de 2014** | **Ley 1712 de 2014**  “De transparencia y del derecho de acceso a la información pública nacional”. |
| **CONPES 3854 de 2016** | **CONPES 3854 de 2016**  Política Nacional de seguridad digital. |

| Tipo de recurso | Cajón de texto de color |
| --- | --- |
| La Ley de Protección de Datos, Ley 1581, tiene por objeto garantizar la seguridad y protección de los datos personales almacenados en diversas bases de datos de entidades públicas o privadas, que realicen cualquier tipo de tratamiento de datos. | |

| Cuadro de texto |
| --- |
| La información personal se puede dividir en los siguientes grupos, según la divulgación más o menos aceptable, o el riesgo que enfrenta la organización en caso de violación de los principios de integridad, confidencialidad y acceso:   * Información pública. * Información semiprivada. * Información privada o confidencial. |

**Tratamiento de datos y políticas legales**

| Cuadro de texto |
| --- |
| El tratamiento de datos y las políticas legales contribuyen, de manera significativa, en la gestión de los activos informáticos, dentro del marco legal colombiano. |

| **Tipo de recurso** | Pestañas o tabs horizontales | |
| --- | --- | --- |
| **Introducción** | A continuación, se hace énfasis en la revisión y el cumplimiento del tratamiento de datos y las políticas legales. | |
| **Tratamiento de datos** | Se entiende por tratamiento de datos a todo proceso u operación técnica, automatizada o no, que recopile, registre, almacene, procese, modifique, consulte, utilice, suprima, bloquee o destruya, así como también transfiera datos de comunicaciones, solicitudes, permita la conexión y transferencias. El tratamiento de datos está regulado por los artículos 3, 4 y 6 de la Ley No. 1581 del 2012. | **Imagen: 133305\_i40** |
| **Políticas legales** | El incumplimiento de la ley de protección de datos, expone a sanciones económicas y operativas, pero también se enfrentan problemas de reputación que pueden costarle al negocio, hasta 2,000 SMMLV:   * Suspensión de actividades relacionadas con el tratamiento hasta por seis (6) meses. * Bloqueo temporal de operaciones relacionadas con el tratamiento de datos. * Bloqueo permanente de operaciones relacionadas con el tratamiento de datos sensibles. | **Imagen: 133305\_i41** |

| Cuadro de texto |
| --- |
| Recuerde explorar los demás recursos que se encuentran disponibles en este componente formativo; para hacerlo, diríjase al menú principal, donde encontrará la síntesis, material complementario, entre otros. Adicional, lo invitamos a desarrollar la actividad didáctica para reforzar los conceptos estudiados en el componente formativo. |

**SÍNTESIS**

| **Tipo de recurso** | Síntesis |
| --- | --- |
| Atención comercial y operación en seguros  Síntesis: Validación de información y optimización del modelo desarrollado | |
| **Introducción** | En el siguiente mapa conceptual, podrá conocer cómo está estructurado el presente componente formativo haciendo énfasis en cada una de las temáticas tratadas. |
| **Imagen: 133305\_i42** | |

**ACTIVIDAD DIDÁCTICA 1**

| **Tipo de recurso** | Actividad didáctica. Arrastrar y soltar |
| --- | --- |
| **Título** | Validación de información y optimización del modelo desarrollado |
| Esta actividad le permitirá determinar el grado de apropiación de los contenidos del componente formativo.  De acuerdo con la definición planteada en la columna izquierda, arrastre cada término al lugar que considere correcto de la columna derecha. | **Imagen: 133305\_i42** |
| Conjunto de reglas que limita el acceso o impone restricciones en el uso de algunos tipos de información. | **Confidencialidad de la información** |
| Aseguran que los empleados, clientes y usuarios comprendan cómo se utilizan sus propios datos personales y quién tiene acceso a ellos. | **Política de confidencialidad** |
| Muestran cómo un sistema procesa los datos en términos de entradas y salidas. | **Diagramas de flujo** |
| Diagrama visual que representa uno o más procesos comerciales para aclarar la comprensión del proceso o para hacer recomendaciones de mejora del proceso. | **Flujo de trabajo** |
| Intento deliberado y malicioso de acceder al sistema de información, sea de la organización o de un particular. | **Ataque cibernético** |
| Se refiere a los principios, las prácticas y las políticas, con el ánimo de proteger los datos digitales y otros tipos de información. | **Seguridad de la información** |

**Retroalimentación general positiva:**

¡Felicitaciones! Ha logrado una óptima aprehensión de los conocimientos relacionados con herramientas de analítica de datos, modelos matemáticos y herramientas tecnológicas.

**Retroalimentación general negativa:**

¡Inténtelo de nuevo! Lo invitamos a revisar nuevamente el material de estudio para afianzar los conocimientos presentados. ¡Ánimo!

**MATERIAL COMPLEMENTARIO**

| Tipo de recurso | Material complementario | | |
| --- | --- | --- | --- |
| Tema | Referencia APA del material | tipo | Enlace |
| Técnicas de gestión de datos masivos | Martínez, R. (2017). Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos. *Dilemata*, (24), p. 151-164. <https://dialnet.unirioja.es/servlet/articulo?codigo=6066833> | Artículo | <https://dialnet.unirioja.es/servlet/articulo?codigo=6066833> |
| Ingeniería de requisitos | Carrizo, D. y Rojas, J.(2018). Metodologías, técnicas y herramientas en ingeniería de requisitos: un mapeo sistemático.*Ingeniare. Rev. chil. Ing.,* *26(*3), p.473-485. <https://www.scielo.cl/scielo.php?pid=S0718-33052018000300473&script=sci_abstract> | Artículo | <https://www.scielo.cl/scielo.php?pid=S0718-33052018000300473&script=sci_abstract> |
| **Seguridad de la información** | Ecosistema de Recursos Educativos Digitales SENA. (2022 1 de julio). *Ejemplo de Procesamiento de datos* [video]. Youtube.  <https://www.youtube.com/watch?v=K3U38rfBGWw> | Video | <https://www.youtube.com/watch?v=K3U38rfBGWw> |
| **Técnicas de gestión de datos masivos** | Ecosistema de Recursos Educativos Digitales SENA. (2022 27 de junio). *Técnicas para el análisis de datos [video].Youtube.* <https://www.youtube.com/watch?v=pjTI4UOgkM8&t=51s> | Video | <https://www.youtube.com/watch?v=pjTI4UOgkM8&t=51s> |

**GLOSARIO**

| **Tipo de recurso** | Glosario |
| --- | --- |
| **Diagrama:** | es la representación de un proceso, una actividad, una función, un modelo, se refiere a un concepto que puede ser expresado gráficamente. |
| **DNS:** | son las siglas de *Domain Name System* (Sistema de nombres de dominio), la cual hace referencia a una tecnología para resolver los nombres en las redes. |
| **Flujograma:** | es una representación gráfica a través de convenciones de una actividad o un proceso. |
| **Seguridad pública:** | se refiere a las acciones y estrategias que garantizan la seguridad a los usuarios públicos, tanto de la seguridad física, como de la informática. |
| **SPAM:** | se refiere a la información y comunicados que nos entregan sin nuestra autorización. |
| **Spyware:** | se refiere a programas, aplicaciones o *software* que realizan espionaje en nuestros dispositivos y sistemas de información. |
| **Troyano:** | es una clase de virus que ingresa al sistema para dañarlo o tomar control del mismo. |
| **Tunelización:** | opera a través del encapsulado de paquetes, es decir, incrusta paquetes dentro de otros. Normalmente, se utiliza en redes privadas con el objeto de transmitir datos de manera eficiente. |
| **VPN:** | se refiere a *Virtual Private Network*, que significa una red virtual privada que son utilizadas para brindar seguridad a la información transmitida. |
| **WI-FI público:** | se refiere a una red con conexión a *WI-FI* de acceso al público en general, sin restricciones para su conexión. |

**REFERENCIAS BIBLIOGRÁFICAS**

| **Tipo de recurso** | Bibliografía |
| --- | --- |
| González, J. (2015). *Utilización de las bases de datos relaciones en el sistema de gestión y almacenamiento de datos*. Ediciones Paraninfo. <https://biblioteca.sena.edu.co/F/1Q8IM9F3VLEE48JPJ4AVA2ETB86D2KSICP6VMICY4VJIJR4U8D-21875?func=full-set-set&set_number=005687&set_entry=000001&format=999> | |
| Joyanes, L. (2019). *Inteligencia de negocios y analítica de datos: una visión global de business intelligence & analytics*. Alfaomega. <https://biblioteca.sena.edu.co/F/1Q8IM9F3VLEE48JPJ4AVA2ETB86D2KSICP6VMICY4VJIJR4U8D-22661?func=full-set-set&set_number=005695&set_entry=000002&format=999> | |
| Luis, A. (2018). *Industria 4.0: la cuarta revolución industrial*. Alfaomega.  <https://biblioteca.sena.edu.co/F/1Q8IM9F3VLEE48JPJ4AVA2ETB86D2KSICP6VMICY4VJIJR4U8D-24482?func=full-set-set&set_number=005695&set_entry=000005&format=999> | |