COTIZACIÓN PARA

CREMIL
Caja de Retiro de las Fuerzas Militares

RENOVACIÓN DE SUSCRIPCIÓN ANUAL DE LICENCIA DEL SOFTWARE "IDEA".

Propuesta Comercial y Técnica

Bogotá D.C. agosto 20 de 2024

Elaborada por AUDISIS LTDA

AUDITORIA INTEGRAL Y SEGURIDAD DE SISTEMAS DE INFORMACIÓN "AUDISIS"
Especializados en Auditoría de Sistemas, Gestión de Riesgos y Seguridad de TI.
Bogotá, D.C. Colombia - Calle 53 No. 27 - 33 Oficina 602 PBX: (57) 601 3470022 –Tels. (57) 601 2556717
E-Mail audisis@audisis.com Web site: www.audisis.com www.softwareaudisis.com
AUDISIS: 36 Años - Fundada en 1.988

Bogotá D.C., 20 de agosto de 2024.

Señores:
CAJA DE RETIRO DE LAS FUERZAS MILITARES.
CREMIL.
Atn. Sr. Andrés Casanova.
Contratista Control Interno.
jcasanova@cremil.gov.co

Atn. Sra. Doris Saboya González.
Profesional de Defensa.
dsaboya@cremil.gov.co
Bogotá D.C.

Respetados Señores:

Para atender su solicitud del día 16 de agosto de 2024, nos complace presentar a su consideración nuestra propuesta económica para ***renovar la suscripción anual de una (1) licencia estándar o usuario único del software IDEA Versión* 12.3,** cuyo vencimiento es el próximo **30 de septiembre de 2024.**

Atentamente solicitamos confirmar por este medio el recibo de esta comunicación.

Quedamos atentos a sus inquietudes y noticias.

Cordialmente,

Edwin Gómez S.
Ing. Soporte Software IDEA.

Tabla de contenido

1. PROPUESTA ECONÓMICA. 5

1.1 RENOVACIÓN DE LICENCIA POR SUSCRIPCIÓN ANUAL DEL SOFTWARE IDEA. 5

1.2 SERVICIO DE SOPORTE Y ACTUALIZACIÓN DEL SOFTWARE IDEA VERSIÓN 12.3. 5

1.3 RENOVACIÓN DE LA SUSCRIPCIÓN ANUAL DEL SOFTWARE IDEA. ..6

1.4 CONDICIONES COMERCIALES. 7

2 PROPUESTA TÉCNICA. 7

2.1 PRESENTACIÓN DEL SOFTWARE IDEA 12.3. 7

2.1.1 Alcance del Componente SMART ANALYZER FINANCIAL para Auditoria a Estados Financieros......9

2.1.2 Componente Excepciones Excepcionales – Asientos de Cierre Año Fiscal. 14

2.2 VALOR AGREGADO QUE GENERA LA ADQUISICIÓN Y DISPONIBILIDAD DEL SOFTWARE IDEA. 15

2.3 ELEMENTOS DEL SOFTWARE IDEA 12.3 QUE RECIBE EL SUSCRIPTOR 16

2.4 REQUERIMIENTOS TÉCNICOS PARA INSTALACIÓN DE LICENCIAS IDEA 12.3 16

3. PERFIL DE "AUDISIS", EL PROVEEDOR DEL SOFTWARE IDEA EN COLOMBIA.....18

3.1 ¿QUÉ ES AUDISIS? 18

3.2 NUESTRA MISIÓN. 19

3.3 NUESTRA VISIÓN 19

3.4 NUESTROS VALORES 19

3.5 EL ENFOQUE DE NUESTROS SERVICIOS 20

3.6 NUESTROS SERVICIOS PROFESIONALES Y SOLUCIONES DE SOFTWARE PARA AUDITORIA Y GESTION DE RIESGOS. 21

3.6.1 SERVICIOS PROFESIONALES ESPECIALIZADOS EN AUDITORÍA DE TIC, GESTIÓN DE RIESGOS Y SEGURIDAD DE TIC. 21

3.6.2 SOLUCIONES DE SOFTWARE PARA AUTOMATIZAR LA AUDITORÍA. 31

3.6.3 SOFTWARE PARA AUTOMATIZAR LA GESTION DE RIESGOS OPERACIONALES. 34

4 PERFIL DE CASEWARE, EL FABRICANTE DEL SOFTWARE IDEA 35

4.1 ¿QUÉ ES CASEWARE? 35

4.2 MISIÓN 35

4.3 VISIÓN 36

4.4 PRODUCTOS Y SERVICIOS 36

1. PROPUESTA ECONÓMICA.

1.1 RENOVACIÓN DE LICENCIA POR SUSCRIPCIÓN ANUAL DEL SOFTWARE IDEA.

ÍTEMS	CONCEPTO	CANTIDAD	Costo Unitario COP	Valor TOTAL COP
1	Renovación Suscripción anual de licencia IDEA Monousuario Estándar versión 12.3. Periodo de renovación: 2024/09/30 a 2025/09/30 **Ver Nota 1.**	1	$ 7.324.800,00	$ 7.324.800,00
SUBTOTAL:				$ 7.324.800,00
VALOR IVA:			19,0%	$ 1.391.712,00
TOTAL:				**$ 8.716.512,00**

Nota 1:

La licencia CaseWare IDEA Estándar (Standalone) es monousuario y su código de identificación está asociada al equipo en el que instala. Todas las acciones relacionadas con la administración de licencias, como registrar, renovar y anular licencias se realizan mediante el Administrador de licencias CaseWare IDEA el cual se instala con CaseWare IDEA. Este tipo de licencia no requiere autenticación de los usuarios.

1.2 SERVICIO DE SOPORTE Y ACTUALIZACIÓN DEL SOFTWARE IDEA VERSIÓN 12.3.

La adquisición de la licencia de IDEA por suscripción anual, incluye servicio anual de soporte técnico y actualización durante la vigencia de la suscripción. Este consiste de:

a) Atención y Soporte por tres fuentes de servicios ubicados en: Colombia (AUDISIS), Costa Rica (CaseWare Latinoamérica) y Canadá (CaseWare Inc.).

El soporte de primer nivel es ofrecido por funcionarios de AUDISIS especializados en IDEA; los soportes de segundo y tercer niveles se ofrecen por CASEWARE Latinoamérica en Costa Rica y CASEWARE el proveedor del software en Canadá. Las líneas telefónicas, Internet y los correos electrónicos de AUDISIS están disponibles permanentemente en horario laboral hábil de lunes a viernes de 8:00 AM a 5:00 PM, para recibir sus solicitudes escritas de soporte sobre el uso, operación y funcionamiento del software IDEA. AUDISIS dará respuesta a sus solicitudes dentro de las 48 horas siguientes al recibo de la solicitud de servicio.

b) Acceso a ***Passport.*** IDEA incluye el derecho de acceso a este portal de servicio técnico, desde el aplicativo IDEA y provee acceso gratuito a numerosos recursos e información práctica para el mejor aprovechamiento la potencia de IDEA 12.3 Entre los recursos disponibles se destacan tutoriales en vídeo, documentación, guías de instalación, manuales y otra documentación, así como componentes de importación optativos, funciones personalizadas, más de 100 scripts listos para usar, acceso a seminarios web.

   Adicionalmente, este portal incluye Acceso **directo a nuevas versiones del software y actualizaciones gratuitas**. A través de Passport puede acceder a información sobre nuevas funciones y mejoras del programa, así como a actualizaciones, nuevas versiones y manuales de IDEA.

c) **Acceso a IDEA Lab**. En IDEA Lab encontrará prototipos funcionales que puede probar y luego compartir su opinión con la comunidad de usuarios de IDEA. Entre estos encontrará recursos Python, macros de IDEAScript y Apps de SmartAnalyzer. Estos prototipos tienen diferentes objetivos: compartir ideas, probar nuevas soluciones y obtener la opinión de los usuarios.

1.3 RENOVACIÓN DE LA SUSCRIPCIÓN ANUAL DEL SOFTWARE IDEA.

La renovación de la suscripción a IDEA debe realizarse con un mes de anticipación a la fecha de vencimiento de la licencia en uso. El software IDEA da un preaviso con 60 días de anticipación para que se inicie la renovación antes de la fecha de vencimiento y así evitar contratiempos por la desactivación del servicio del software IDEA.

La renovación del licenciamiento del software IDEA por suscripción anual implica que antes de finalizar el año de vigencia deberán pagar el costo de la suscripción por un nuevo año de acuerdo con la lista de precios oficiales vigentes en el mercado.

1.4 CONDICIONES COMERCIALES.

Plazo de entrega del Software: Dentro de los diez (10) días calendario contados a partir de la fecha de pedido.

Plazo de pago de la factura: Contado.

Forma de Pago: Transferencia de Fondos a cuenta de AUDISIS.

Validez de la cotización: Cuarenta y cinco (45) días calendario.

2 PROPUESTA TÉCNICA.

2.1 PRESENTACIÓN DEL SOFTWARE IDEA 12.3.

IDEA es una poderosa herramienta para análisis, extracción y auditoría de datos, de origen Canadiense, fácil de utilizar (amigable e intuitiva). Provee numerosas funciones para analizar datos, clasificarlos y generar información para soportar la **toma de decisiones basadas en datos**. Además, para auditores, analistas de fraudes y aseguramiento de calidad, es útil para verificar la calidad e integridad de la información de bases de datos y archivos de computador e identificar y analizar fraudes.

Software líder en el mundo para Analítica de Datos y Automatización de Técnicas de Auditoria Asistidas por Computador (CAATs), con las cuales los auditores pueden implantar los enfoques *de Auditoría Continua y Auditoría Agile.* Otras características de IDEA que agregan valor para la Empresa y las Auditorías Internas, Revisorías Fiscales y Auditores Financieros, son las siguientes:

- IDEA provee funcionalidades para importar (copiar datos de archivos externos de distinta procedencia) datos de archivos de computador de diferentes formatos (texto, CVS, ODBC, Excel, PDF, reportes, AS400, SAP) e ilimitado número de registros, generar estadísticas de campos de datos (numéricos, fecha y hora); realizar operaciones aritméticas, comprobar cálculos, utilizar funciones pre construidas de análisis financiero y manejo de campos, extraer y agrupar registros según criterios especificados por el usuario, identificar registros repetidos y omisiones de secuencia de registros, comparar, unir y agregar archivos, utilizar cinco tipos de muestreo estadístico, identificar operaciones sospechosas de fraude y lavado de activos.

- Provee numerosas funcionalidades de análisis de datos, útiles para verificar la integridad y calidad de los datos de las bases de datos, de acuerdo con las reglas del negocio y las normas regulatorias.

- Es una herramienta que ***genera rutinas de software ejecutable y reutilizable (SCRIPTS)***, con las cuales se automatizan las pruebas de auditoría y se programa su ejecución de acuerdo con los planes de la auditoría, utilizando técnicas de auditoría asistidas con el computador (CAATs). De esta manera se puede migrar hacia el enfoque de **auditorías continuas o con repeticiones (iteraciones) más frecuentes, para** analizar datos de archivos de fechas y hora muy cercanas a tiempo real (tiempo de la auditoria = tiempo de los eventos).

- Genera reportes y gráficos con los resultados de las pruebas y análisis realizados (visualización de datos - dashboards).

- Exporta archivos y envía correos electrónicos desde el software IDEA.

La licencia de uso del software IDEA i Provee un módulo de **pruebas de auditoría financiera prefabricadas (Smart Analyzer Financial)**, para cinco operaciones de las Empresas:

a) En el **Mayor General o diario**, identificar asientos inusuales (17 pruebas),
b) En **Cuentas por Cobrar**, identificar asientos inusuales en facturación y deudores (8 pruebas).

c) En **Cuentas por Pagar**, identificar asientos inusuales en acreedores y operaciones (17 pruebas).
d) En **Inventarios**, crear tablas de ítems de inventario por antigüedad, saldos de Inventario, recalcular saldos y rotación de los elementos (13 pruebas), y
e) En **Activos Fijos**, crear listados, resumen por categorías y recalculo de depreciación (6 pruebas).
f) En **Recursos Humanos**, Hace la verificación de los datos de los empleados de una empresa.
g) En **Nómina**, Hace la verificación de los costes de la nómina por empleado de acuerdo con las deducciones y los deducidos.

2.1.1 Alcance del Componente SMART ANALYZER FINANCIAL para Auditoria a Estados Financieros.

La licencia de uso del software IDEA incluye el componente **SMART ANALYZER FINANCIAL**. Este es una compilación de pruebas de auditoría y reportes básicos (CAATs preconstruidas) para siete (7) operaciones: Mayor General, cuentas por pagar, cuentas por cobrar, inventarios, activos fijos, recursos humanos y nómina.

a) En el **Mayor General o diario**, identificar asientos inusuales (18 pruebas).

Para identificar elementos inusuales en la BD del mayor general o diario. (18 pruebas)

1) Asientos no balanceados
2) Asientos con comentarios específicos.
3) Asientos duplicados.
4) Asientos faltantes.
5) Asientos registrados en fines de semana.
6) Asientos registrados en fechas específicas.
7) Asientos registrados en horas específicas.
8) Asientos por usuario - importes de crédito (mayor general)
9) Asientos por usuario.
10) Resumen por combinaciones de cuenta.
11) Asientos con importes grandes.

12) Asientos con importes redondeados.
13) Asientos con importes que terminan en 999.
14) Resumen por número de cuenta.
15) Asientos por período y fuente del asiento.
16) Asientos por período.
17) Saldos de cuenta por fuente del asiento.
18) Saldos de cuenta por período

b) **En Cuentas por Cobrar**:

Para identificar asientos inusuales en facturación y deudores (12 pruebas):

1) Deudores con saldos acreedor.
2) Resumen operaciones del deudor.
3) Operaciones cercanas a una fecha específica.
4) Búsqueda campo duplicado.
5) Antigüedad por fecha de vencimiento.
6) Antigüedad por fecha de factura.
7) Deudores con valores totales mayores al límite del crédito.
8) Deudores con saldos mayores al límite del crédito.
9) Operaciones por ID de usuario
10) Operaciones con fechas especificadas
11) Operaciones registradas en fines de semana
12) Operaciones registradas en horas especificadas

c) **En Cuentas por Pagar**:

Para identificar elementos inusuales en cuentas por cobrar (16 pruebas):

1) Antigüedad por fecha de factura.
2) Facturas o pagos duplicados.
3) Acreedores con saldo deudor.
4) Acreedores con totales de facturas mayores al límite aprobado.
5) Acreedores con saldos mayores al límite aprobado.
6) Resumen operaciones acreedor.
7) Facturas sin número de orden de compra
8) Operaciones registradas en fines de semana.
9) Operaciones cercanas a una fecha especificada.
10) Operaciones registradas en fechas especificadas.
11) Operaciones registradas en horas especificadas.
12) Operaciones por ID de usuario.
13) Operaciones con importes redondeados.
14) Búsqueda campos duplicados. cuentas por pagar
15) Antigüedad por fecha de factura
16) Antigüedad por fecha de vencimiento

d) **En Inventarios.**

Crear tablas de ítems de inventario por antigüedad, saldos de Inventario, recalcular saldos y rotación de los elementos (13 pruebas),

1) Antigüedad por fecha de recepción y saldo final de existencias.
2) Antigüedad por fecha de recepción y costo unitario.
3) Recalcular saldo del inventario.
4) Calcular rotación del Inventario.
5) Calcular rotación unitaria.
6) Costo unitario cero o negativo.
7) Cantidad Negativa.
8) Resumen por ubicación del inventario.
9) Valores del inventario grandes.
10) Productos recibidos cerca de una fecha especificada.
11) Precio de venta inferior al costo unitario.
12) Comparación precio de venta con costo unitario.

13) Búsqueda campo duplicado.

e) **En Activos Fijos**.

Crear listados, resumen por categorías y recalculo de depreciación (9 pruebas).

1) Incorporaciones activas fijos.
2) Resumen categoría de activos.
3) Recalcular depreciación lineal.
4) Recalcular depreciación lineal II.
5) Recalcular depreciación decreciente.
6) Recalcular depreciación decreciente II.
7) Depreciación superior al costo.
8) Búsqueda campo duplicado.
9) Incorporaciones de Activos Fijos

f) **Recursos Humanos**

Crea listados, resumen por Empleado válido y no válido, hoja de vida, por periodo, datos básicos, datos bancarios. (17 pruebas)

1) Empleados duplicados potenciales: nombre.
2) Empleados con edad insuficiente o excesiva.
3) Datos que faltan o no son válidos: direcciones de correo electrónico
4) Datos que faltan: número de seguridad social.
5) Empleados con un nivel retributivo inusual para su grupo retributivo y centro de costes
6) Empleados que se marcharon durante el período actual
7) Empleados duplicados: número de seguridad social.
8) Resumen por años de servicio.
9) Empleados con un nivel retributivo inusual para su grupo retributivo.
10) Datos que faltan: cuenta bancaria.
11) Datos que faltan o no son válidos: números de teléfono.

12) Empleados duplicados potenciales: dirección.
13) Empleados con nombres no válidos.
14) Datos que faltan: fecha de nacimiento.
15) Empleados contratados durante el período actual.
16) Empleados duplicados: cuenta bancaria.
17) Empleados que se marcharon en un plazo de 120 días a partir de su fecha de inicio.

g) **Nómina.**

Crea listados de los Empleados con y sin deducciones (15 pruebas)

1) Empleados que trabajan una cantidad excesiva de horas o días
2) Empleados con comisión y comisión excesiva
3) Transacciones con el mismo número de seguridad social durante el mismo período
4) Niveles retributivos por grupo y centro de costes
5) Transacciones sin número de seguridad social
6) Sin empleados en el mes anterior
7) Sin empleados en el mes actual
8) Retribución especial inusualmente alta por grupo
9) Realización de perfil por centro de costes
10) Realización de perfil por grupo retributivo
11) Salario base inusualmente alto para el grupo del empleado
12) Empleados con horas extraordinarias y un exceso de horas o días
13) Cambios inusuales en el pago base del salario
14) Empleados sin deducciones o con deducciones sospechosas
15) Ratio de deducciones inusuales

2.1.2 Componente Excepciones Excepcionales – Asientos de Cierre Año Fiscal.

Estas pruebas de auditoría financiera, prefabricadas en IDEA, permiten extraer todos los asientos registrados cerca de la fecha de cierre de año fiscal. Genera los siguientes reportes:

Prueba 01 - Asientos sin cuadrar
Prueba 02 - Asientos duplicados potenciales por usuario
Prueba 03 - Asientos duplicados potenciales
Prueba 04- Asientos registrados en fines de semana
Prueba 05 - Asientos registrados en días poco usuales
Prueba 06 - Asientos registrados en horas poco usuales
Prueba 07- Asientos registrados a finales del año fiscal
Prueba 08 - Asientos con fecha retroactiva
Prueba 09 - Asientos con cantidades redondeadas
Prueba 10 - Asientos con dígitos recurrentes
Prueba 11 - Asientos con palabras clave de interés
Prueba 12 - Asientos con descripciones cortas o sin descripción
Prueba 13 - Combinaciones de registros de cuentas poco usuales
Prueba 14 - Combinaciones de cuentas complejas Prueba 15 - Cuentas poco usuales para el tipo de documento
Prueba 16 - Asientos con lo opuesto a los normales debe y haber
Prueba 17 - Asientos registrados por usuarios poco usuales
Prueba 18 - Asientos con cantidades de valor alto
Prueba 19 - Primeros dos dígitos de la ley de Benford
Prueba 20 - Suma de la ley de Benford
Prueba 21 - Segundo orden de la ley de Benford
Prueba 22 - Últimos dos dígitos de la ley de Benford
Prueba 23 - Detección de valores atípicos - Aprendizaje automático
Prueba 24 - Debe y haber incorrectos

2.2 VALOR AGREGADO QUE GENERA LA ADQUISICIÓN Y DISPONIBILIDAD DEL SOFTWARE IDEA.

Valor Agregado o Valor Percibido que se obtiene de adquirir y utilizar en sus auditorías el software IDEA se describe a continuación:

a) La disponibilidad de un Software de Analítica de Datos de categoría mundial para aplicar numerosas "buenas y mejores prácticas" de análisis de datos, generar conocimientos de valor para la organización y soportar "decisiones basadas en Datos" en las auditorías internas y de Estados Financieros.

b) La disponibilidad de una herramienta para automatizar el uso de Técnicas de Auditoría Asistidas por Computador (CAATs), orientadas a satisfacer necesidades específicas de la auditoría. *Estas CAATs son repetibles y reutilizables en diferentes periodos de tiempo, con solo cambiar el o los archivos de entrada*. De esta manera, el software IDEA facilita la implantación del enfoque de **Auditoría Continua o con iteraciones más frecuentes y Auditoría Agile.**

c) Mejorar la productividad del equipo de auditores (hacer más con menos). *Con el software IDEA y el enfoque de "Auditoría Basada en Datos" se realizará mayor cantidad de pruebas, de mayor alcance y materialidad, sin incrementar los recursos de personal y tiempo disponibles en la Auditoría.*

d) Incrementar la calidad, confiabilidad y eficiencia de las Auditorías, a través del uso del computador como herramienta de auditoría.

e) Satisfacer los lineamientos de la NIA 1009 sobre el uso de CAATs y las Normas de Auditoría del Instituto de Auditores Internos (IIA), especialmente los numerales 1210.A3 y 1220.A2 sobre utilización de herramientas de auditoría asistidas por computador y otras técnicas de análisis de datos.

f) Recibir transferencia de conocimientos y tecnología de Auditoría para ser más *eficientes y productivos y proveer mayor confianza en sus resultados y mejorar el servicio a sus clientes.*

g) *Incrementar o ganar mayor respecto y credibilidad profesional de los auditores, a través de resultados obtenidos con el uso del computador como herramienta de auditoría.*

2.3 ELEMENTOS DEL SOFTWARE IDEA 12.3 QUE RECIBE EL SUSCRIPTOR

El suscriptor recibirá los siguientes elementos, como se describen a continuación:

a) Link para descargar el instalador del Software ejecutable de la versión 12.0 para Windows en español.
b) Administrador de licencias de CaseWare IDEA (instalado con IDEA)
c) Código de autorización de Licencia para la instalación del Software IDEA
d) Documentación del software:
   - Manuales: Los siguientes manuales se instalan con IDEA y están disponibles en formato PDF.
     - Tutorial de IDEA
     - Tutorial de Report Reader
     - Tutorial de SmartAnalyzer
     - Caso práctico de Métodos estadísticos avanzados
   - Guía de introducción a IDEA Cloud Share
   - Guía de instalación de IDEA: Incluida en el paquete de instalación.
   - Guía de usuario del Administrador de licencias de CaseWare IDEA: Incluida en el paquete de instalación.
   - Ayuda en línea: Accesible desde las opciones de Ayuda en los menús de opciones de IDEA. Muchos cuadros de diálogo de tareas también ofrecen ayuda contextual.
e) Derecho a recibir soporte para la operación y uso de IDEA durante la vigencia de la licencia.

2.4 REQUERIMIENTOS TÉCNICOS PARA INSTALACIÓN DE LICENCIAS IDEA 12.3

IDEA 12.3 es una aplicación de 64-bits que solo se puede ejecutar en sistemas operativos WINDOWS de 64 bits. A continuación, se muestran los sistemas operativos Windows compatibles y el software compatible necesario para ejecutar IDEA.

Importante: Debe tener instalados los paquetes de actualizaciones y servicios más recientes de Windows.

Sistemas operativos Windows compatibles.

La siguiente tabla muestra los sistemas operativos Windows compatibles, y los productos IDEA compatibles con máquinas virtuales, conexiones a escritorio remoto y servidores Citrix o Terminal.

Sistemas operativos	Producto	[1]Máquinas virtuales	[2]Escritorio remoto	[3]Servidor Citrix/ [4]Terminal
*Windows 7 Windows 8.1 Update 1 Windows 10	IDEA Standard	✗	✓	✗
	IDEA Network	✓	✓	✓
	IDEA Educational	✓	✓	✓
Windows Server 2012 R2 Update 1 Windows Server 2016 Windows Server 2019	IDEA Standard	✗	✗	✗
	IDEA Network	✓	✓	✓
	IDEA Educational	✓	✓	✓

* A partir del 14 de enero de 2020, Microsoft Corporation finalizó su servicio técnico para Windows 7. IDEA 12.3 es la última versión que será compatible con Windows 7.

1) Una máquina virtual es una instalación de Windows que necesita un hipervisor para ejecutarse.
2) Escritorio remoto es el uso del Protocolo de escritorio remoto (RDP) en una máquina física o virtual.
3) El uso del paquete Citrix para implementar una sesión única, varias sesiones o imágenes para comercialización. Se admiten Citrix Apps y Desktops 7 1912.
4) Un servidor de terminal permite a los usuarios conectarse simultáneamente a través de RDP a una sola máquina física o virtual.

Software compatible

Si las siguientes aplicaciones no están ya instaladas en su sistema, el programa de instalación de IDEA las instalará automáticamente:

a) Microsoft .NET Framework 4.7.1
b) Microsoft Visual C++ 2010 SP1 (64 bits, 32 bits) Redistributable Package
c) Microsoft Visual C++ 2013 (64 bits) Redistributable Package
d) Microsoft Visual C++ 2015 (64 bits) Redistributable Package
e) Microsoft Access Database Engine 2016 (64 bits) Redistributable. Microsoft Access Database Engine 2016 (64 bits) Redistributable no se instala si se detectan software o controladores Microsoft Office de 32 bits en su equipo.

Derechos de administrador

Para instalar IDEA y sus herramientas asociadas se necesitan privilegios de administrador.

Los siguientes son los requerimientos de hardware para el software IDEA.

Hardware	Mínimo	Recomendado
Procesador	64 bits, Multi-core	64 bits, Multi-core
RAM	8 GB	16 GB
Espacio en disco	100 GB	500 GB
Tipo de disco		SSD (Solid State Drive)

3. PERFIL DE "AUDISIS", EL PROVEEDOR DEL SOFTWARE IDEA EN COLOMBIA

3.1 ¿QUÉ ES AUDISIS?

AUDISIS LTDA, **Auditoría Integral y Seguridad de Sistemas de Información Ltda.**, es una firma de Auditores – Consultores Gerenciales, constituida legalmente el 23 de septiembre de 1.988, mediante escritura pública No. 5962 de la Notaría 4 del círculo de Bogotá, con registro vigente en la Cámara de Comercio de Bogotá bajo el número de matrícula 346900.

3.2 NUESTRA MISIÓN.

Nuestra misión es la prestación de servicios profesionales especializados en gestión de riesgos y control interno de tecnología de información (TI), seguridad informática, auditoría en sistemas de información y auditoría integral en procesos de negocios y servicios automatizados, utilizando metodologías y herramientas de software propias, software de seguridad y auditoría de categoría mundial, personal permanentemente capacitado y altos estándares de calidad.

Nuestros servicios buscan facilitar y hacer más eficiente, efectivo, seguro y confiable el manejo de la información de nuestros clientes, aplicando las mejores prácticas universalmente aceptadas (beat practices) para las actividades de Gobierno, Control y Auditoría de Sistemas de Información.

3.3 NUESTRA VISIÓN

Nuestra visión es posicionarnos a nivel nacional entre las primeras empresas prestadoras de servicios profesionales especializados en **gestión de riesgos, diseño de control interno organizacional, seguridad informática, auditoría en tecnología de información (TI) y auditoría integral en procesos de negocios**, con capacidad permanente de adaptación a los cambios y la creación, uso, representación y comercialización de herramientas de gestión de riesgos y de auditoría asistidas por computador, para satisfacer las necesidades del mercado.

3.4 NUESTROS VALORES

Como Asesores - Consultores Gerenciales estamos siempre comprometidos con los valores éticos que garantizan la satisfacción de las necesidades de nuestros clientes con honestidad, objetividad, integridad, diligencia, confidencialidad, equidad y respeto por los derechos humanos.

Los cuatro (4) valores compartidos de AUDISIS son los siguientes:

- **Integridad**
- **Excelente Valor a los mercados y a los clientes**
- **Compromiso de uno para con el otro (mutuo)**
- **Fortaleza a partir de la diversidad cultural**

Independencia

AUDISIS pretende que su comportamiento profesional esté permanentemente regido por una actitud de independencia, sin la cual la propia firma no podría seguir existiendo. En este sentido, la firma evita involucrarse en la prestación de cualquier tipo de servicio en el que por un posible conflicto de interés o cualquier otra circunstancia, su imparcialidad de criterio y objetividad pudieran verse afectadas.

3.5 EL ENFOQUE DE NUESTROS SERVICIOS

AUDISIS presta sus servicios profesionales con un enfoque PROACTIVO y PREVENTIVO, orientado a LA PREVENCION DE RIESGOS CRITICOS y la implantación de la cultura de AUTOCONTROL. De esta manera ayuda a modernizar el control interno y la auditoría de los servicios y productos de las empresas.

El enfoque preventivo de nuestros servicios se transfiere a nuestros clientes a través de todos nuestros servicios y productos, buscando siempre la modernización de la cultura de control, el establecimiento de una sólida conciencia de seguridad y la creación de una actitud positiva en los empleados, como base para emprender la transición hacia el autocontrol y el mejoramiento continuo de la calidad.

3.6 NUESTROS SERVICIOS PROFESIONALES Y SOLUCIONES DE SOFTWARE PARA AUDITORIA Y GESTION DE RIESGOS.

3.6.1 SERVICIOS PROFESIONALES ESPECIALIZADOS EN AUDITORÍA DE TIC, GESTIÓN DE RIESGOS Y SEGURIDAD DE TIC.

AUDISIS ofrece siete (7) tipos de **Servicios Profesionales Especializados** en Auditoría a Tecnologías de la Información y Comunicaciones (TIC), Auditoría Interna a Sistemas de Gestión, Gestión de Riesgos y Seguridad en TIC.

1) **AUDITORÍAS A TECNOLOGÍA DE INFORMACIÓN (Basadas en estándares de ISACA, del IIA y NIAs)**
2) **AUDITORÍA INTERNA A SISTEMAS DE GESTIÓN (Basadas en ISO 19011).**
3) **CONSULTORÍA Y ASESORIA EN GESTIÓN DE RIESGOS (Basada en Marcos de Referencia ISO 31000, COSO 2017 y Basilea).**
4) **CONSULTORÍA EN CONTROL INTERNO DE TI, SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD.**
5) **CONSULTORIA EN DISEÑO DE CONTROLES EN PROCESOS DE NEGOCIO Y TI.**
6) **CONSULTORÍA EN INFORMÁTICA FORENSE.**
7) **INTERVENTORIA DE CONTRATOS DE TI Y AUDITORIA DE TI.**

3.6.1.1 AUDITORÍA A SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN (Basada en estándares de ISACA, IIA y NIAs)

La Auditoría de Sistemas o Auditoría a los Servicios TIC (Tecnología de Información y Comunicaciones) "es una especialidad de la auditoría que revisa, verifica y evalúa de manera independiente y objetiva la Seguridad en la Infraestructura de TIC, la Gestión de Servicios de TIC y las Aplicaciones de Computador en funcionamiento que soportan las operaciones de negocio

y de apoyo administrativo de las Empresas, con la finalidad de proveer razonable confianza a la Gerencia y a otras partes interesadas, respecto a que los controles internos establecidos proveen seguridad razonable, eficiencia, eficacia, se cumplen las normas legales y regulatorias, reducen los riesgos del negocio aniveles tolerables y aseguran la satisfacción de los objetivos y necesidades de la organización".

Algunos servicios de Auditoría de TIC ofrecidos por AUDISIS son:

1) Auditorías a la Infraestructura de los Servicios de TIC (también llamada "Auditoria de Controles Generales de TIC").
2) Auditoría a ERPs y Aplicaciones de Negocios (o de Gestión) en estado de Producción o funcionamiento.
3) Servicios de Outsourcing de Auditoría de Sistemas para Auditorías Internas, Firmas de Auditores Financieros y Revisorías Fiscales.
4) Auditorías de Cumplimiento de Normas sobre seguridad de la información y Ciberseguridad establecidas por Organismos de Supervisión y Vigilancia del Estado.
5) Auditorías de Cumplimiento de Normas sobre Protección de datos personales – Habeas Data - establecidas por la leyes y Organismos de Supervisión y Vigilancia del Estado.
6) Realización de Pruebas de Vulnerabilidad / Ethical Hacking.
7) Implantación de Técnicas de Auditoría Asistidas por Computador (CAATs) a la medida de las necesidades de la Empresa, utilizando el software IDEA.
8) Auditoría de TIC a Procesos Electorales para Elección de Dignatarios de Corporaciones Públicas, Presidente y Vicepresidente de la Republica.
9) Auditoría a Procesos de Votación Electrónica en Asambleas de Accionistas o de Asociados en Empresas y de dignatarios a Concejos Directivos y Rector en Universidades.
10) Asesoría para Implantar la Auditoria de Sistemas como función permanente dentro de las Empresas.
11) Selección de Auditores de Sistemas.
12) Servicios de Peritaje y Auxiliares de la Justicia en Asuntos relacionados con TIC
13) Formación y Entrenamiento de Auditores de TIC.

3.6.1.2 AUDITORÍA INTERNA EN SISTEMAS DE GESTIÓN (Basada en ISO 19011)

La **norma ISO 19011: 2018, Directrices para la auditoría de los sistemas de gestión,** define **Sistema de Gestión** así: *"Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos (3.24) para lograr estos objetivos"*

Un sistema de gestión puede tratar una sola disciplina o varias disciplinas, por ejemplo, gestión de la calidad, gestión financiera o gestión ambiental.

Los elementos del sistema de gestión establecen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, las políticas, las prácticas, las reglas, las creencias, los objetivos y los procesos para lograr esos objetivos.

La norma ISO 19011: 2018 define **Auditoría** así: *"Proceso sistemático, independiente y documentado para obtener evidencias objetivas (3.8) y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (3.7)".*

Las auditorías internas según ISO 19011, denominadas en algunos casos *auditorías de primera parte*, se realizan por, o en nombre de la propia organización. Nótese que este concepto difiere significativamente de la definición de **Auditoría Interna según estándares del Instituto de Auditores Internos (IIA)**, el cual dice: "*Es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización, ayudando a cumplir sus objetivos al aportar un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno corporativo".*

La **Auditoría Interna de Sistemas de Gestión** permite a las organizaciones evaluar el estado de cumplimiento de requisitos de normas de gestión (ISO 9001, ISO 45001, ISO/IEC 27001, ISO 14001, Decreto 1072 de 2015 entre otras), además de revisar su nivel de madurez del sistema y los posibles riesgos asociados a los procesos y la efectividad de los controles.

De manera general, uno de los principales beneficios de realizar estas auditorías internas es permitir a los principales responsables de la organización tomar

decisiones con base en la situación de su sistema de gestión, a fin de realizar ciertas reorientaciones, en caso de ser necesario, hacia la consecución de sus objetivos previstos.

Servicios de Auditoría Interna a Sistemas de Gestión ofertados por AUDISIS.

1) Auditoría Interna de Sistemas de Gestión.
2) Auditoría ISO de Sistemas de Gestión Integrados.
3) Consultoría ISO para implantar una certificación ISO.
4) Auditoría Interna al Sistema de Gestión de Seguridad de la Información (SGSI) y al Plan de Continuidad del Negocio (BCP).
5) Formación Auditores Internos ISO.

3.6.1.3 CONSULTORÍA EN SISTEMAS DE GESTIÓN DE RIESGOS (Basada en ISO 31000 Y COSO 2017)

Según ISO 31000, riesgo es el *"efecto de la incertidumbre en los objetivos"* y un efecto es una desviación positiva o negativa de lo que se esperaba. Las desviaciones positivas o eventos positivos se denominan *oportunidades.* Las desviaciones negativas o eventos negativos se denominan ***amenazas*** y se refieren a eventos accidentales o intencionales que pueden causar daño a uno o más activos y obstaculizar el logro de los objetivos de la organización.

Según ISO 31000, la **Gestión del Riesgo** (traducción del inglés *risk management*) es el conjunto de actividades y métodos coordinados utilizados para dirigir una organización y controlar los muchos riesgos que pueden afectar su capacidad para lograr sus objetivos.

El objetivo de la gestión de riesgos es reducir diferentes riesgos inherentes de un ámbito preseleccionado, a un nivel aceptable por la sociedad. Puede referirse a numerosos tipos de amenazas causadas por actos de la naturaleza, el medio ambiente, la tecnología, el diseño de los procesos, los seres humanos, las organizaciones y la política. Por otro lado, involucra todos los recursos disponibles de los seres humanos o, en particular, de una entidad de manejo de riesgos (persona, grupo de trabajo, organización).

La **gestión de riesgos** es un enfoque estructurado para manejar la incertidumbre relativa a eventos negativos que pueden obstaculizar el logro de los objetivos de la organización, a través de una secuencia de actividades humanas que incluyen *la identificación, el análisis y la evaluación de riesgo*, para luego establecer las estrategias de su tratamiento utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evitar el riesgo (esto es, reducir su probabilidad o impacto a 0), reducir el impacto negativo del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular mediante una decisión informada.

Algunas veces, el manejo de riesgos se centra en la contención de riesgos generados por causas físicas o legales (por ejemplo, desastres naturales o incendios, accidentes, muerte o demandas). Otras veces, la gestión de riesgos enfatiza en aspectos operacionales como son las personas, los procesos y las fallas tecnológicas. Por otra parte, la ***gestión de riesgo financiero*** se enfoca en los riesgos que pueden ser manejados usando instrumentos financieros y comerciales.

La administración de riesgo empresarial o *Enterprise Risk Management* (ERM, por sus siglas en inglés) es un proceso realizado por el consejo directivo de una entidad, la administración y el personal de dicha entidad. Se aplica en el establecimiento de estrategias de toda la empresa, diseñada para identificar eventos potenciales que puedan afectar a la entidad y administrar los riesgos para proporcionar una seguridad e integridad razonable referente al logro de objetivos.

Servicios Profesionales en Gestión de Riesgos ofrecidos por AUDISIS.

1) Implantar la Gestión de Riesgos en los Procesos y Servicios de Tecnología de Información.
2) Implantación procesos de Gestión de riesgos de Seguridad de la Información y Ciberseguridad.
3) Implantar el Sistema de Administración de Riesgos Operacionales (SARO) en los procesos de la Cadena de Valor de la Empresa.
4) Implantar el Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT, SAGRILAFT, SIPLAFT y SIPLA) en las operaciones de negocio de la organización.

5) Implantar el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).
6) Auditoría de Cumplimiento a la Operación (funcionamiento) de los sistemas de Gestión de Riesgos SARO y SARLAFT / SAGRILAFT.
7) Formación y Entrenamiento en Gestión de Riesgos y Auditoria a Sistemas de Gestión de Riesgos.

3.6.1.4. CONSULTORÍA EN CONTROL INTERNO Y SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES (TICs).

El control interno en Tecnología de Información (TI) tiene dos grandes componentes: a) Controles Generales de TI (ITGC) y b) Controles Específicos o Controles de Aplicaciones de Computador de Negocios y soporte administrativo.

Los Controles Generales de TI (ITGC) o controles en la infraestructura de TI se definen como el conjunto de políticas y procedimientos establecidos por el área de TI de la empresa para asegurar continuamente la confidencialidad, la integridad y la disponibilidad de sus recursos, servicios y datos de TI.

La Gerencia de TI de la Empresa debe proveer procesos de soporte y prestación de servicios, desarrollo de sistemas y la infraestructura de TI, como servicio común para toda la empresa (es decir, redes, bases de datos, sistemas operativos y almacenamiento). **Los controles aplicados a todas estas actividades de servicio de TI se conocen como controles generales de TI**. La operación formal de estos controles generales es necesaria para asegurar la confiabilidad a los controles internos que se implantan en las aplicaciones de computador (o sistemas ERPs). Por ejemplo, una deficiente administración de cambios en el área de TI podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de las verificaciones automáticas de integridad de la información.

Las Aplicaciones de Computador son programas de computador desarrollados en la empresa (in house) o adquiridos a terceros, con las cuales se procesa la información de las operaciones del CORE DEL NEGOCIO y de soporte administrativo de las empresas. Por ejemplo: facturación, nómina, cartera, ventas,

cuentas por pagar, compras, activos fijos, inventarios, comisiones, mantenimiento de vehículos, historias clínicas, laboratorio clínico, producción, etc**.**

Los controles internos en las aplicaciones de computador se conocen con el nombre de **controles de aplicación o Controles Específicos** y se refieren a aquellos controles que regulan el *ingreso (entrada), procesamiento y salidas de los datos* en las actividades automatizadas de los procesos del modelo de operación de la empresa. Ejemplos: dígito de autoverificación, test de validez de códigos, verificación visual, test para datos numéricos, test de datos obligatorios, perfiles autorización, autenticación de usuarios, edición de imágenes antes y después de cambios procesados, entre otros. Todos estos controles ayudan a asegurar iintegridad, consistencia, precisión, validez, autorización, edición, segregación automática de funciones incompatibles.

El diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, con base en los requerimientos de negocio definidos, usando los criterios que deben ser satisfechos por la información de negocios (eficacia, eficiencia, integridad, confidencialidad, disponibilidad, confiabilidad y cumplimiento de las normas legales y regulatorias). La responsabilidad operacional de administrar y operar los controles de aplicación no es de TI, sino de los propietarios o responsables de los procesos de negocio.

La Seguridad de la Información.

La norma **ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad",** especifica los requisitos para establecer, implementar, mantener, monitorear y mejorar continuamente un SGSI (Sistema de Gestión de Seguridad de la Información).

La seguridad de la información, que suele abreviarse como **InfoSec**, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción. InfoSec comprende la seguridad física y del entorno, el control de acceso y la ciberseguridad. Suele incluir tecnologías como agente de seguridad de acceso a la nube (CASB), herramientas de engaño, detección y respuesta en el punto de conexión (EDR) y pruebas de seguridad para DevOps (DevSecOps), entre otras.

Los tres pilares o tríada CIA de la seguridad de la información, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD conforman las piedras

angulares de una **protección de la información** sólida, que crean la base de la infraestructura de seguridad de la empresa. La tríada CIA ofrece estos tres conceptos como principios guía a la hora de implementar un plan InfoSec.

Confidencialidad

La privacidad es uno de los componentes principales de InfoSec. Las organizaciones deben tomar medidas que permitan únicamente el acceso de usuarios autorizados a la información. El cifrado de datos, la autenticación multifactor y la prevención de pérdida de datos son algunas de las herramientas que pueden emplear las empresas para ayudar a garantizar la confidencialidad de los datos.

Integridad

Las empresas deben mantener la integridad de los datos a lo largo de todo su ciclo de vida. Las empresas con un sistema de InfoSec bien establecido reconocen la importancia de que los datos sean precisos y fiables y no permiten que los usuarios no autorizados accedan a ellos, los alteren o interfieran de cualquier otro modo en ellos. Las herramientas como los permisos de archivos, la administración de identidades y los controles de acceso de usuario ayudan a garantizar la integridad de datos.

Disponibilidad

InfoSec implica un mantenimiento continuo del hardware físico y la actualización habitual del sistema para garantizar que los usuarios autorizados disponen de acceso fiable y coherente a los datos que necesiten.

La Ciberseguridad.

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales ó *ciberamenazas.* Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías.

La ISO/IEC 27032:2023 es un estándar internacional que se enfoca en la ciberseguridad y la protección de la información en un mundo cada vez más conectado. **Proporciona directrices para garantizar la seguridad de la información en redes y sistemas de información**. Esta norma se aplica a organizaciones de todos los sectores y ayuda a gestionar los **riesgos asociados con las amenazas cibernéticas.**

La ISO/IEC 27032:2023 no solo es una herramienta esencial para fortalecer la ciberseguridad de una organización, sino que también ofrece una serie de **beneficios tangibles y estratégicos**. Desde una mayor **resiliencia ante amenazas** hasta la mejora de la imagen de la empresa y el cumplimiento de regulaciones, esta norma desempeña un papel fundamental en la protección de la información y los activos digitales, al tiempo que contribuye al **éxito a largo plazo de la organización en un entorno empresarial** cada vez más digital y conectado. Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

Servicios Profesionales de Control Interno, Seguridad de la Informacion y Ciberseguridad ofertados por AUDISIS:

1) Acompañamiento para Diseñar e Implantar Políticas, Normas y Procedimientos de Control Interno en Tecnología de Información (TI).
2) Acompañamiento para Implantar los Sistemas de Gestión de Seguridad de la Información (SGSI) basada en la Normas ISO 27001 y de Ciberseguridad (ISO 27032).
3) Acompañamiento para Elaborar e Implantar el Plan de Continuidad del Negocio - BCP –.
4) Acompañamiento para Diseñar e Implantar programas de prevención y detección de fraudes (programa antifraude) y anticorrupción a la medida de las organizaciones.
5) Acompañamiento para Diseñar e implantar Controles, Basado en Análisis de Riesgos, para Procesos de la Cadena de Valor, Procesos de Tecnología de Información y Aplicaciones de Computador.
6) Formación y Entrenamiento en Control Interno y Seguridad de TIC.

3.6.1.5 CONSULTORÍA EN INFORMÁTICA FORENSE.

El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.
La informática forense se refiere a un conjunto de procedimientos y técnicas metodológicas para identificar, recolectar, preservar, extraer, interpretar, documentar y presentar las evidencias de los equipos de computación, de manera que estas evidencias sean aceptables durante un procedimiento legal o administrativo en un juzgado.

La informática es una parte vital en la investigación forense en el ámbito digital, pues está específicamente focalizada en los delitos cometidos mediante dispositivos de computación, como redes, ordenadores y medios de almacenamiento digital, especialmente en aquellos casos que involucran a la tecnología como fuente o víctima de un delito.

La informática forense es esencial para:

- Asegurar la integridad y disponibilidad de la infraestructura de red cuando sucede un incidente de ciberseguridad o ataque informático.
- Identificar y obtener evidencias de los cibercrímenes de manera apropiada.
- Asegurar **la protección adecuada de los datos** y el cumplimiento regulatorio.
- Proteger a las organizaciones para que no vuelvan a suceder en el futuro los incidentes ocurridos.
- Ayudar en la protección de crímenes online, como abusos, bullying…
- Minimizar las pérdidas tangibles o intangibles de las organizaciones o individuos relativas a incidentes de seguridad.
- Soportar el proceso judicial de enjuiciamiento de los criminales.

3.6.1.6 INTERVENTORIA DE CONTRATOS Y PROYECTOS DE TI.

La interventoría a Contratos de TIC consiste en el seguimiento técnico que sobre el cumplimiento de contratos realice AUDISIS, cuando sea contratada para tal fin por Entidades Estatales, porque el seguimiento del contrato supone conocimiento

especializado en la materia, o cuando la complejidad o la extensión del mismo lo justifiquen. No obstante, lo anterior cuando la entidad lo encuentre justificado y acorde a la naturaleza del contrato principal, podrá contratar el seguimiento administrativo, técnico, financiero, contable, jurídico del objeto o contrato dentro de la interventoría.

La Interventoría de Proyectos de TIC se refiere a la prestación de servicios profesionales de aseguramiento de la calidad y/o auditoría técnica, para acompañar y asesorar las actividades de supervisión, vigilancia y control del desarrollo de proyectos de Tecnología de información (TI), en los cuales se considera necesario y conveniente el apoyo de una "veeduría imparcial" que interactúe permanentemente con áreas administrativas, financieras y de gestión de la empresa y con los terceros involucrados en los proyectos. Este acompañamiento se denomina "Interventoría de proyectos".

> "*La interventoría en proyectos de tecnología de información es el conjunto de herramientas, procesos y procedimientos que soportan la gestión de la Empresa para asegurar a los implicados (Stakeholders) de un proyecto de tecnología en particular, que las especificaciones requeridas en su diseño y/o construcción y/o implantación están siendo logradas dentro de los estándares de calidad previstos, en el cronograma base establecido y con los costos presupuestados para tal efecto".*

3.6.2 SOLUCIONES DE SOFTWARE PARA AUTOMATIZAR LA AUDITORÍA.

AUDISIS es fabricante y comercializador de soluciones de software para gestión de auditorías y gestión de riesgos.

A continuación, se presentan cinco (5) soluciones ***de software*** ofertadas por AUDISIS para incrementar efectividad, productividad, confiabilidad y valor agregado de las Auditorías Internas (según estándares del IIA), Auditorías de Sistemas (según estándares de ISACA) y Auditorías Financieras según las NIAs. También se presenta una herramienta (ControlRisk) como solución para estandarizar la implantación de sistemas de gestión de riesgos en la empresa.

1) **IDEA:** Software de Análisis y Extracción de Datos y Auditoría Continua Basada en Datos.
2) **AUDIRISK Web:** Software para Gestionar Auditorías Internas y de Sistemas, Basadas en Riesgos Críticos (Satisface estándares del IIA e ISACA).
3) **AUDIT IP Web:** Software para Gestionar Planes de Mejoramiento por efecto de Auditorías Internas y de Terceros realizadas a la Empresa.
4) **ASD AUDITOR:** Software de Auditoría Financiera y Análisis Financiero
5) **SMARTEXPORTER:** Software para Extraer, Preparar Y Programar Automáticamente Datos de SAP
6) **CONTROLRISK Web:** Software para Gestionar Riesgos en Procesos de Negocio y Tecnología de Informacion (TI)

3.6.2.1 IDEA: Software para Análisis y Extracción de Datos y Automatización de Técnicas de Auditoría.

Incremente el análisis de datos en sus auditorías con las capacidades analíticas de IDEA; este software de origen canadiense, cuenta con más de 100 funciones de análisis de datos y auditoria que responderán a sus necesidades. IDEA le permite acelerar el análisis de datos en auditoría con SmartAnalyzer, una plataforma que agrupa aplicaciones inteligentes para la auditoría financiera (Libro mayor, Cuentas por Cobrar, Cuentas por Pagar, Inventarios, Activos Fijos) e IDEA Lab, el centro de innovación continua con complementos que aprovechan los últimos avances en Python y técnicas de aprendizaje automático.

3.6.2.3 AUDIRISK Web: Software para Gestionar Auditorías Internas y de Sistemas, Basadas en Riesgos.

Es un software en tecnología WEB (Cloud Computing) fabricado por AUDISIS, alineado con los estándares internacionales para el ejercicio profesional de la

Auditoría Interna del Instituto de Auditores Internos (IIA), para asistir el desarrollo de las siguientes cuatro (4) actividades principales de las auditorías internas y de sistemas: a) Elaborar el Plan Anual de la Auditoría Interna Basada en la Exposición a Riesgos de los Entes Auditables; b) Desarrollo de Auditorías de Procesos y Sistemas Basadas en Riesgos Críticos; c) Seguimiento a Implantación de Planes de Mejoramiento para atender los Hallazgos y recomendaciones de la Auditoría; y d) Generación de Informes e Indicadores de Gestión de la Auditoría.

3.6.2.3 AUDIT IP Web: Software para Gestionar Planes de Mejoramiento por efecto de Auditorías Internas y de Terceros realizadas a la Empresa.

Es una herramienta Web fabricada por AUDISIS, para gestionar los planes de mejoramiento que surgen de Hallazgos de Auditorías realizadas a la Empresa por la Auditoría Interna y por Terceros..

Por ejemplo: Gestiona los hallazgos y planes de mejoramiento que se elaboren por Auditoría Interna de la Empresa y auditorías realizadas por terceros tales como los siguientes: Firmas de Auditoría Externa (Revisoría Fiscal, Auditoría Financiera, Auditoría de Sistemas, etc.), Organismos de control y vigilancia del Estado (Contralorías, Superintendencias, Ministerios), Firmas certificadoras de Sistemas de Gestión y Auditorías Internas de Sistemas de Gestión (de calidad, ambientales, de salud ocupacional, ISO27001, ISO 22301, etc.

3.6.2.4 ASD AUDITOR: software de auditoría financiera y análisis financiero.

Es una poderosa herramienta de gestión de auditoría y análisis financiero, de origen español, que permite trabajar y dirigir de forma ordenada, eficiente y ágil el proceso de Auditoría financiera desde las actividades previas hasta la finalización y emisión del correspondiente informe. Las auditorías de estados financieros con ASD AUDITOR se ejecutan de acuerdo con las NIAs, en base a riesgos y en los requerimientos de Control y calidad NICC1.

3.6.2.5 SMART EXPORTER: software para Extraer, Preparar y Programar Automáticamente datos de SAP

Es un software de origen alemán, que le permite acceder de forma fácil, flexible y segura a todos los datos relevantes de un sistema SAP, gracias a esto los mismos usuarios pueden extraer los datos que necesitan, mientras el departamento de TI conserva el control de los datos y de los derechos de acceso.

SmartExporter le permite Extraer información de archivos o tablas de un sistema SAP y dejarla en formatos: TXT, CVS, ACCESS, IMD (IDEA), SQL, para ser utilizados en procesos de análisis de datos, Auditorías basadas en datos, migración de datos, o ser fuente de entrada para otras soluciones como: Big Data, BI, Minería de datos, Software estadístico (SAS), entre otras herramientas.

3.6.3 SOFTWARE PARA AUTOMATIZAR LA GESTION DE RIESGOS OPERACIONALES.

3.6.3.1 CONTROLRISK Web: Software para Gestionar Riesgos en Procesos de Negocio y Tecnología de Información.

Es un software en tecnología WEB fabricado por AUDISIS, que provee funcionalidades para implantar y mejorar continuamente la Gestión de Riesgos Empresariales en los Procesos de Cadena de Valor y la Tecnología de la Información de las Empresas, con una visión a corto, mediano y largo plazo; las funcionalidades del software están alineadas con las buenas y mejores prácticas de Gestión de Riesgos y Control Interno recomendadas por ISO 31000: 2018, el marco de referencia ERM (Enterprise Risk Management), COSO 2013, COBIT, ISO 27001 y otras normas nacionales de Gestión de Riesgos expedidas por las Superintendencias y el Departamento Administrativo de la Función Pública (DAFP).

4 PERFIL DE CASEWARE, EL FABRICANTE DEL SOFTWARE IDEA

4.1 ¿QUÉ ES CASEWARE?

“En esta era digital, impulsar la innovación implica transformar la forma en que las personas piensan y actúan. Con esto en mente, estamos comprometidos con tres valores fundamentales: comunidad, excelencia e innovación. Internamente, esto apoya nuestra visión e informa nuestra cultura y comportamiento. Externamente, estos valores nos ayudan a proporcionar a los clientes una mayor eficiencia, calidad y valor”.

Comunidad.

Para funcionar de manera efectiva, promover el liderazgo y alentar el desarrollo, necesitamos ser parte de un sistema más amplio. Nuestro personal, junto con nuestros socios y clientes locales y globales, son parte del pegamento que nos une como comunidad y nos permite trabajar hacia un objetivo más amplio.

Excelencia.

En el corazón de la excelencia, tanto a nivel individual como organizacional, está la cultura. Nos esforzamos por una cultura corporativa que fortalezca, enfoque e involucre a los empleados. Nuestros equipos están equipados con la mentalidad y las habilidades necesarias para desarrollar soluciones de software de vanguardia.

Innovación.

La innovación es vista como el resultado de nuestra comunidad y el estándar de excelencia. Esto requiere una evolución continua. Para lograr esto, proporcionamos la combinación correcta de personas, cultura y enfoque.

4.2 MISIÓN

Para crear oportunidades innovadoras que empujan los límites tecnológicos en la industria, estamos dedicados a la innovación continua para contadores y auditores en prácticas grandes y pequeñas, en corporaciones y gobiernos de todo el mundo.

4.3 VISIÓN

Desarrollamos soluciones de software de vanguardia que cambian el futuro de la auditoría, los informes financieros y el análisis de datos. Para lograr esto, trabajamos continuamente para producir un flujo de mejoras exitosas de productos, innovaciones, adaptaciones y extensiones.

4.4 PRODUCTOS Y SERVICIOS

La siguiente es la relación de productos ofrecidos como Representantes y Distribuidores Exclusivos en Colombia:

Desktop Products

a) IDEA: Es una herramienta de análisis de datos completa, potente y fácil de usar que analiza rápidamente el 100 por ciento de sus datos, garantiza la integridad de los datos y acelera el análisis de datos para permitir auditorías más rápidas y efectivas.

b) SmartExporter: Es una solución de software que le permite acceder de forma fácil y flexible a todos los datos relevantes de un sistema SAP®. Gracias a SmartExporter®, los usuarios pueden extraer ellos mismos los datos de SAP® que necesitan mientras el departamento de TI conserva el control de los datos y de los derechos de acceso. Software compatible con IDEA.

c) Servicios de capacitación para cada uno de los productos.