IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI - Basado en la Norma ISO 27001: 2022

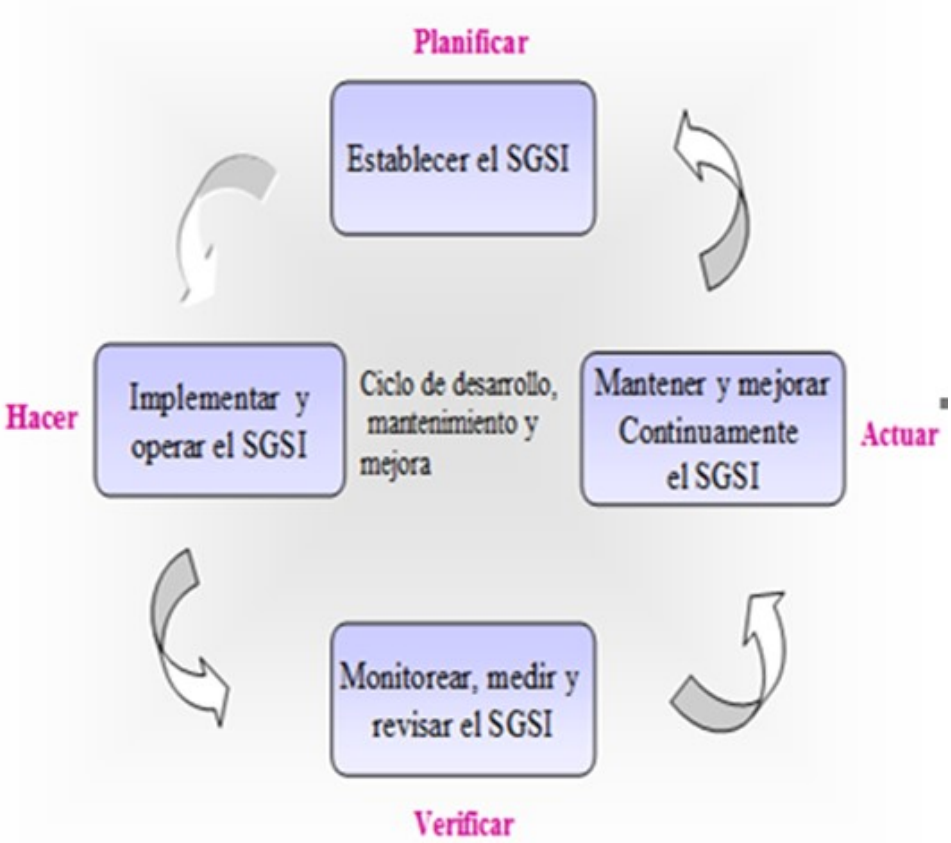
Contenido:	Pág.

PRESENTACIÓN

La información es el activo más valioso de cualquier organización, por lo que representa, no por su valor registrado en libros de contabilidad (no está registrada). Como sistema nervioso de cualquier organización, la información es indispensable para soportar la toma de decisiones, el control y el manejo de las operaciones de negocio y cumplimiento normativo, por lo que debe protegerse en sus componentes de integridad, disponibilidad y confidencialidad.

Sin información no es posible la continuidad de las operaciones y si la **información no es confiable, segura y cumple con las normas aplicables,** la toma de decisiones, el control y otras actividades administrativas se exponen a riesgos de la mayor severidad y a consecuencias desastrosas para la organización.

Ciclo PHVA del Sistema de Gestión de Seguridad de la Información (SGSI)



Para satisfacer las necesidades de seguridad, ciberseguridad y privacidad de la información, surgieron los estándares ISO / IEC 27001:2022, ISO 27002:2022, ISO 27003: 2017, ISO 27005: 2022, ISO27032:2023 e ISO 27701:2022. El primero proporciona los requerimientos para establecer, implementar, operar, monitorear y mejorar un **Sistema de Gestión de seguridad, la ciberseguridad y la privacidad de la información (SGSI)** en los procesos de la organización, armonizado con otros sistemas de gestión.

La ISO 27005:2022 provee guías para la Gestión de Riesgos de Seguridad, ciberseguridad y privacidad de la Información (ISRM), específicamente soportando los requerimientos del sistema de gestión de seguridad de la información definida por ISO 27001.

La ISO 27032:2023, provee una explicación de la relación entre la seguridad en internet, en la web y la ciberseguridad, estos controles son fundamentales para las organizaciones que tienen activos de información en el ciberespacio. Finalmente, la ISO 27701:2022 especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente un Sistema de gestión de información de privacidad (PIMS) en forma de una extensión de la ISO 27001 e ISO 27002 para la gestión de la privacidad dentro del contexto de la organización.

La aplicación de estos estándares posibilita a las Organizaciones sin importar su tamaño o sector al cual pertenecen, alcanzar un nivel adecuado de seguridad, ciberseguridad y privacidad de la información mediante la aplicación de un sistema de gestión basado en la implementación de políticas de seguridad de la información, gestión de riesgos, controles y mejora continua que les permita garantizar la *confidencialidad, integridad y disponibilidad* de su información y la de sus Clientes.

Este seminario permitirá a los asistentes conocer la metodología y los factores de éxito necesarios para implantar el Sistema de Gestión de Seguridad, ciberseguridad y privacidad de la Información (SGSI) basado en la norma ISO/IEC 27001: 2022.

Durante 3 días, los instructores compartirán experiencias y vivencias sobre teoría y la práctica de la implantación de un SGSI en empresas de diferentes tamaños y grados de sofisticación, y darán respuesta a las inquietudes de los participantes respecto a los problemas y desafíos que se presentan en la ejecución del proyecto de implantación y mantenimiento.

Propuesta de valor

Al finalizar el seminario, los participantes estarán en capacidad de:

- Preparar el plan de implantación del SGSI, definir la estructura del proyecto y obtener la aprobación de la Gerencia.
- Identificar el contexto organizacional base para el diseño del SGSI
- Soportar y documentar las actividades críticas del proyecto de implantación del SGSI.
- Identificar, evaluar severidad, controlar y monitorear los riesgos inherentes a los activos de información para asegurar que estos activos se mantienen protegidos dentro de límites aceptables de seguridad, ciberseguridad y privacidad de la información.
- Definir las políticas y procedimientos del SGSI.
- Administrar el cambio de cultura organizacional en la empresa con respecto a la Seguridad, ciberseguridad y privacidad de la Información.

- Realizar las auditorías internas del SGSI y promover el mejoramiento continuo del SGSI.
- Tramitar las actividades necesarias para obtener la certificación del SGSI .

1. OBJETIVOS DEL SEMINARIO

- Presentar la metodología para implantar el Sistema de Gestión de seguridad, ciberseguridad y privacidad de la información (SGSI) dentro de la organización, en concordancia con la norma ISO / IEC 27001:2022.
- Desarrollar habilidades en los participantes para gestionar adecuadamente los riesgos inherentes a la seguridad, ciberseguridad y privacidad de los activos de información y la elección de los controles eficaces y eficientes para mitigarlos.
- Desarrollar habilidades para definir y documentar políticas y procedimientos del SGSI.
- Conocer herramientas de software para apoyar la implantación y mantenimiento del SGSI.

2. A QUIENES ESTÁ DIRIGIDO

Gerentes de Tecnología de Información y Comunicaciones, Gerentes de Riesgos, Gerentes de Seguridad de la información, Jefes de Planeación, Administradores de Seguridad Informática, Oficiales de Seguridad, Auditores Internos, Revisores Fiscales y Auditores de Sistemas.

3. MODALIDAD, FECHAS, DURACIÓN Y HORARIO

MODALIDAD: VIRTUAL

FECHAS: Noviembre 18 al 25 Noviembre de 2024

DURACIÓN: 24 horas - 4 horas por día

HORARIO: Lunes a viernes de 8:00 am - 12:00m

4. TEMAS DEL SEMINARIO

DIA 1

1. INTRODUCCIÓN AL SGSI - 3 horas

- La Familia de Normas ISO 27000
- Definición y elementos del sistema de gestión de seguridad, ciberseguridad y privacidad de la información (SGSI)
- Los 4 dominios de la Norma ISO 27001: 2022 y sus controles
- Razones y beneficios de adoptar la ISO 27003
- El modelo PHVA del SGSI.

2. METODOLOGÍA PARA IMPLANTAR EL SGSI - parte 1 (5 horas)

- Fases y actividades de la metodología para implantar el SGSI (Norma ISO 27003)
- Obtener aprobación de la Gerencia para implantar el SGSI.
- Identificar el contexto organizacional para el diseño del SGSI
- Definir Alcance, Límites y Política del SGSI.

DIA 2

3. METODOLOGÍA PARA IMPLANTAR EL SGSI - parte 2 (8 horas)

- Análisis de Requerimientos de Seguridad de la Información.
- Evaluación de Riesgos y Planeación del Tratamiento de Riesgos – Normas ISO 27005 e ISO 31000:2018.
- Selección de Objetivos de Control y Controles requeridos – Norma ISO 27001: 2022
- Elaboración de la declaración de aplicabilidad SoA
- Determinar Efectividad de los controles y las métricas.

DIA 3

4. METODOLOGÍA PARA IMPLANTAR EL SGSI- parte 3 (6 horas)

- Plan de Implementación del SGSI.
- Monitoreo y Auto- aseguramiento del SGSI.
- Desarrollo de Competencias Organizacionales.
- Planeación de la Auditoría Interna al SGSI
- Redacción del manual de Seguridad de Información.

5. AUDITORÍAS INTERNAS AL SGSI

6. EL PROCESO DE CERTIFICACIÓN INTERNACIONAL (2 horas)

5. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

presentación de los temas por parte de los instructores utilizando filminas, desarrollo de ejercicios de aplicación y recapitulación de las principales ideas de cada tema.

6. MATERIAL PARA LOS PARTICIPANTES

Se entregará material escrito en medio magnético con las ayudas utilizadas por los expositores y los talleres y casos de estudio.

7. VALOR DE INVERSIÓN POR PARTICIPANTE

Pagos antes del seminario	Pagos después del seminario
$2.231.000 + IVA COP	$2.442.000 + IVA COP

Descuentos por inscripción	
Clientes de servicios y productos de AUDISIS	5%
Tres o más inscritos de la misma empresa	7,5%
Miembros de ISACA e IIA – Certificar	5%

Forma de pago

En cheque a nombre de AUDISIS o transferencia de fondos a la cuenta corriente número 07511792-9 del Banco de Bogotá. Sucursal Galerías.

8. PROCEDIMIENTO DE INSCRIPCIÓN

Descargar de la página **http://www.audisis.com/FormularioSeminariosAUDISIS.docx** el formulario de inscripción, diligenciarlo y enviar a AUDISIS al correo **audisis@audisis.com**.

9. PLAZO PARA ANULAR LAS INCRIPCIONES

La anulación de inscripciones solo se aceptará por escrito, hasta cinco (5) días calendario antes de la realización del seminario. Después de este plazo, solamente se aceptará cambio de las personas inscritas.

10. PLAZO PARA CANCELAR LA REALIZACIÓN DEL SEMINARIO

La realización del seminario estará sujeto a la inscripción de un número mínimo de participantes. Cuando este número no se obtenga, AUDISIS informará con anticipación de 3 días hábiles la no realización o aplazamiento del seminario.

11.EL SEMINARIO DENTRO DE SU EMPRESA (IN COMPANY)

Ofrecemos la posibilidad de desarrollar el seminario para grupos de funcionarios de su empresa, presencial, en sus instalaciones o en el sitio que la empresa seleccione.

Contáctenos:
Correo: audisis@audisis.com
Tels: (57) 601-2556717– PBX: (57) 601-3470022 (57) 601-3099764
Celular: 310-2690175

12.CERTIFICADO DE ASISTENCIA

A los participantes que participen en el 80% o más de las sesiones del seminario se entregará certificación de asistencia.

13. REQUISITOS DE CONOCIMIENTOS Y HERRAMIENTAS DE COMPUTADOR

- Conocimientos básicos de seguridad de la información.
- Disponibilidad de un computador portátil para instalar los casos de estudio y realizar los talleres.

14. INSTRUCTORES

Euclides Cubillos M. - Gerente de Auditoría / Consultoría de AUDISIS.

Ingeniero de Sistemas. MBA, Magister en Dirección y Administración de Empresas. Título de Posgrado en Auditoría de Sistemas. CISA (Certified Information Systems Auditor). Experto en Seguridad y Auditoría de sistemas. 34 años de experiencia profesional en Auditoría de TI y Gestión de Riesgos.

Expresidente de la Asociación Colombiana de Auditores de Sistemas (ACDAS) y fundador y expresidente del ISACA Capítulo de Bogotá. Fue fundador y director de la Especialización en Auditoría de Sistemas de la Universidad Católica de Colombia y catedrático en Postgrados de Auditoría y Revisoría Fiscal en las Universidades Nacional de Colombia, Central de Bogotá, Antonio Nariño, El Rosario, Santo Tomás de Aquino (Bucaramanga), Universidad Militar, UNAB, FUNDEMA (Manizales), Santiago de Cali, Libre de Colombia (Bogota y Cali), Jorge Tadeo Lozano y Corporación Universitaria de la Costa (Barranquilla). Autor de varias publicaciones sobre Controles y Auditoría de Sistemas. Ha sido conferencista invitado a las Jornadas de ISACA capítulos de Bogotá y Medellín y al LATINCACS de México.

ALVARO MAURICIO ROMERO. Consultor Seguridad Informática y Análisis forense, AUDISIS.

Experto en Tecnología y Seguridad Informática con certificaciones como auditor líder BS ISO/IEC 27001:2005 Information Security Management System otorgada por el BSI British Standards Management System, CEH (Certified Ethical Hacker & Countermeasures) otorgada por el organismo internacional ECCOUNCIL y en proceso de certificación como profesional de continuidad del negocio CBCP y CISSP. Auditor interno norma ISO 9001 versión 2000. Cuenta con más de 18 años de experiencia en administración y auditoria de plataformas de Tecnología y seguridad informática en entidades financieras nacionales e internacionales. Ha participado en la gerencia de proyectos relacionados con el Diseño, implementación y administración de Sistemas de Gestión de Seguridad de la Información, Sistemas de gestión de Riesgos, Planes de Continuidad de Negocios y Recuperación del sistema, y auditorias basadas en riesgos en Organizaciones

nacionales e internacionales del sector servicios y financiero.

Se ha desempeñado por más de 10 años como docente en Seminarios, diplomados y especializaciones de Seguridad Informática y Análisis Forenses en Varias Universidades y empresas como la Pontificia Universidad Javeriana, Universidad Manuela Beltrán, Universidad Autónoma, Universidad Piloto, Universidad Militar Nueva Granada y la Escuela de Comunicaciones del Ejercito ESCOM. Entre otros, los seminarios dictados son:

- Seminario taller Implementación de Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001: 2005
- Seminario para auditores internos del SGSI
- Seminario taller de implementación del plan de continuidad del negocio BCP
- Seminario taller de control interno y diseño de controles con énfasis en el cumplimiento de la CE038 SFC y CE023 SSF
- Seminario taller de auditoría basada en riesgos.
- Seminario taller de Ethical hacking y análisis forense informático.

Actualmente es docente en la ESCUELA DE COMUNICACIONES DEL EJERCITO NACIONAL en la especialización de seguridad física y de la información dictando las cátedras de seguridad en sistemas operativos, plan de continuidad del negocio, ethical hacking y análisis forense informático.

Como consultor de AUDISIS ha participado en proyectos de implantación del BCP en DINISSAN y sociedad Colombiana de Anestesiología y Reanimación SCARE y en proyectos de seguridad y auditoría al BCP en FUNDACION DE LA MUJER, FINAGRO, COMFENALCO TOLIMA, FIDUCIARIA BOGOTA, SEGUROS GENERALI, LAFAYETTE, PROENFAR, INIF, HOSPITAL SAN IGNACIO, ICFES y Titularizadora colombiana. También ha sido instructor en cursos y seminarios organizados por AUDISIS.

16. NUESTROS SERVICIOS PROFESIONALES ESPECIALIZADOS Y SOLUCIONES DE SOFTWARE OFRECIDOS POR AUDISIS

SERVICIOS ESPECIALIZADOS EN AUDITORÍA 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.**

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

*"*Es una especialidad de la auditoría que de manera independiente y objetiva revisa, verifica y evalúa los procesos de 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 aplicables, reducen a niveles tolerables los riesgos del negocio y aseguran la satisfacción de los objetivos y necesidades de la organización".

Según ISACA (Information Systems Audit and Control Association), la Auditoría de Sistemas de Información es :

> *"Toda auditoría que comprenda la revisión y evaluación de todos o parte de los aspectos de los sistemas automatizados de procesamiento de información, incluyendo los procesos no automatizados relacionados y las interfaces entre ellos."*

Servicios Profesionales de Auditoría TIC ofrecidos por AUDISIS.

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 Computador (de Negocios o de Soporte Administrativo) en estado de Producción o funcionamiento.
3) Auditoría al Desarrollo de Sistemas.
4) Outsourcing de Auditoría de Sistemas para Auditorías Internas, Firmas de Auditores Financieros y Revisorías Fiscales.
5) Auditorías de Cumplimiento de Normas sobre seguridad de la información y Ciberseguridad establecidas por Organismos de Supervisión y Vigilancia del Estado.
6) Auditorías de Cumplimiento de Normas sobre Protección de datos personales – Habeas Data - establecidas por la leyes y Organismos de Supervisión y Vigilancia del Estado.
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.

2. AUDITORÍA INTERNA A 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 22301, ISO 14001 y Decreto 1072 de 2015 para el SG-SST); 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 Profesionales de Auditoría Interna a Sistemas de Gestión ofrecidos por AUDISIS.

1) Auditoría Interna al Sistema de Gestión de Seguridad de la Información - SGSI , ISO 27001.
2) Auditoría Interna al Sistema de Gestión de Continuidad del Negocio (BCP) – ISO 22301.
3) Auditoría Interna de Sistemas de Gestión ISO 9001, ISO 14000, iS0 45000.
4) Auditoría ISO de Sistemas de Gestión Integrados.
5) Consultoría para obtener Certificación ISO.
6) Auditoria al SG - SST
7) Formación Auditores Internos ISO.

3. CONSULTORÍA Y ASESORIA EN GESTIÓN DE RIESGOS (Basada en marcos de referencia ISO 31000, COSO 2017 y Basilea)

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 Operacionales en los Procesos y Servicios de Tecnología de Información.
2) Implantar la Gestión de riesgos de Seguridad de la Información (ISO 27001) y Ciberseguridad (ISO 27032) .
3) Construir matrices de riesgo para los procesos de la cadena de valor de la Empresa, procesos de TI y Aplicaciones de Computador de Negocio o de Soporte Administrativo.
4) Implantar el Sistema de Administración de Riesgos Operacionales (SARO) en los procesos de la Cadena de Valor de la Empresa.
5) 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.
6) Implantar el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).
7) Auditoría de Cumplimiento a la Operación de los sistemas de Gestión de Riesgos SARO y SARLAFT / SAGRILAFT.
8) Formación y Entrenamiento en Gestión de Riesgos
9) Formación y entrenamiento en Auditoria a Sistemas Gestión de Riesgos SARO Y SARLAFT.

4. CONSULTORÍA EN CONTROL INTERNO DE TI, SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD.

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

Los Controles Generales de TI (ITGC) ó 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 integridad, 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.

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.

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 Información y Ciberseguridad ofertados por AUDISIS:

1) 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 Norma ISO 27001 y de Ciberseguridad (ISO 27032).

3) Realización de Pruebas de Vulnerabilidad / Ethical Hacking.

4) Acompañamiento para Elaborar e Implantar el Plan de Continuidad del Negocio - BCP – basado en la norma ISO 22301.

5) Acompañamiento para Diseñar e Implantar programas de prevención y detección de fraudes (programa antifraude) y anticorrupción a la medida de las organizaciones.

6) Acompañamiento para Diseñar e implantar Controles en procesos de la infraestructura de Tecnología de Información y nuevas aplicaciones de computador, basado en identificación y análisis de riesgos inherentes críticos.

7) Formación y Entrenamiento en Control Interno y Seguridad de TIC.

5. CONSULTORIA EN DISEÑO Y EVALUACION DE CONTROL INTERNO EN TI Y PROCESOS DE NEGOCIO.

El **enfoque proactivo y preventivo** de los controles debería prevalecer sobre el **enfoque Reactivo o A posteriori**. Esto significa que los controles *deberían diseñarse para anticiparse a la ocurrencia de los eventos de riesgo, más que orientarse a detectar la ocurrencia de errores e irregularidades después que estas ocurren,* cuando lo único que puede hacerse es establecer los controles como una reacción a hechos ocurridos (Ex post Facto) o como remedio para que estos no vuelvan a presentarse.

Los controles internos deberían diseñarse antes de iniciar la operación de los procesos y proyectos de la Empresa, *durante las fases de planeación y construcción, no después*, cuando los procesos están en operación y se detecta la ocurrencia de errores, irregularidades o después que se presentan desastres por actos de la naturaleza o provocados por terceros. Por consiguiente, los controles deberían diseñarse e implantarse para reducir la posibilidad de que se materialicen los eventos de riesgo o para reducir su impacto si no pueden evitarse, es decir, *para que actúen antes de que los riesgos ocurran.*

El diseño de los controles debería realizarse con base en las políticas de operación de la Empresa y en el análisis de los eventos de riesgo inherentes negativos que puedan presentarse en

el desarrollo de sus operaciones, con el propósito de reducir la severidad de los riesgos a nivel aceptable o tolerable, de tal manera que los controles establecidos aseguren razonablemente la consecución de los objetivos esperados y evidencien su efectividad para la gestión adecuada de los riesgos.

Servicios de Diseño y Evaluación de Controles Internos ofrecidos por AUDISIS.

1) Implantación de estándares de diseño de controles internos en procesos de negocio y TI.
2) Evaluación del diseño y efectividad de controles internos existentes
3) Acompañamiento en diseño e implantación de Controles, Basado en Análisis de Riesgos, para Procesos de la Cadena de Valor o del modelo de operación de la Empresa y TI.
4) Acompañamiento en identificación de necesidades de control e implantación de controles requeridos en nuevos productos, servicios y sistemas de información automatizados.
5) Formación y Entrenamiento en Diseño e Implantación de Controles en procesos de negocio y TI.

6. 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.

7. INTERVENTORIA EN PROYECTOS DE TIC Y DE AUDITORIA TIC.

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. 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".*

NUESTRAS SOLUCIONES DE SOFTWARE OFERTADAS POR AUDISIS PARA GESTIONAR AUDITORIAS Y ADMINISTRAR DE RIESGOS

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 Información (TI)

1. IDEA: Software de Análisis y Extracción de Datos y Auditoría Continua Basada en Datos.

IDEA (Acrónimo de **I**nteractive **D**ata **E**xtraction and **A**nalysis), es una herramienta con reconocimiento internacional en analítica de datos y auditoría basada en datos. A través de la toma de decisiones basadas en datos, IDEA incrementa la productividad, eficiencia, eficacia y valor agregado de las auditorías.

Adicionalmente, es una herramienta con capacidades para generar programas de computador ejecutables (IDEA scripts) a la medida de las necesidades de las auditorias (internas y de estados financieros) e implantar el enfoque de **auditorias continuas ó más frecuentes,** el cual permite programar la ejecución automática de técnicas de auditoria asistidas con el computador (CAATs) para examinar archivos de datos actualizados en tiempo muy cercano al tiempo real (tiempo de ocurrencia de los eventos auditados = tiempo de la auditoría).

Ofrece una interfaz amigable, funciones específicas de auditoría, importación de datos desde varios formatos (SAP, PDFs, archivos planos, bases de datos relacionales), capacidad para procesar archivos de cantidad ilimitada de registros y más de 100 funciones preconstruídas (funciones @) para analítica de datos.

Este software de origen canadiense, en su estructura básica tiene disponibles más de 100 funciones de análisis de datos y auditoría asistida por computador. Además, para facilitar el análisis de datos en auditoría financiera, IDEA ofrece *SmartAnalyzer Financial*, una plataforma que agrupa aplicaciones inteligentes para auditoría financiera (Libro mayor, Cuentas por Cobrar, Cuentas por Pagar, Inventarios, Activos Fijos) e IDEA Lab, el centro de innovación continua, con complementos que utilizan los últimos avances en Python y técnicas de aprendizaje automático.

Alternativas de Licenciamiento de IDEA.

Se ofrecen tres tipos de licenciamiento por Suscripción Anual.

1) **Licencia IDEA Estándar o Stand Alone Named.** Es una licencia monousuario, asociada al equipo en el que instala el software. Este tipo de licencia no requiere autenticación de los usuarios.
2) **Licencia IDEA NLS VIRTUAL (Network License Server Virtual Named).** Utiliza un servidor de licencias para controlar el acceso a la cantidad de usuarios amparados por la licencia. El análisis de los datos con IDEA se ejecuta en cada equipo y en estos también se almacenan los resultados obtenidos del análisis. Esta modalidad de licenciamiento

monousuario no requiere autenticación de los usuarios; solo se autentica el equipo con derechos de acceso al software IDEA.

3) **Las licencias NLS Concurrente (Network License Server Concurrent).** Son licencias en red de uso simultaneo, requieren de un servidor donde se instala un administrador de licencias, Estas licencias se expiden para el número de usuarios adquiridos por el cliente y permiten su instalación en un número flotante de usuarios. Como ejemplo, una licencia para 5 usuarios se puede instalar en 15 computadores, todos deben estar en la misma red del servidor para poder hacer ping y que el administrador de licencias le asigne una licencia. De los 15 usuarios instalados solo 5 pueden tener el software abierto al mismo tiempo; cuando el sexto usuario intenta abrir el software el sistema le indicara que no hay licencias disponibles y requiere que algún compañero cierre el software para que la licencia vuelva al servidor y alguien más pueda tomarla.

2. AUDIRISK WEB: Software para Gestionar Auditorías Internas y de Sistemas, Basadas en Riesgos Críticos.

Este software satisface los estándares internacionales para el ejercicio profesional de la Auditoría Interna del Instituto de Auditores Internos (IIA) y de ISACA para la Auditoria de Tecnología de Información (TI).

Los estándares para el desarrollo profesional de la Auditoría Interna del Instituto de Auditores Internos (IIA), **definen la Auditoría Interna así**: *"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"*. Nótese que este concepto difiere significativamente de la **Auditoría Interna a Sistemas de Gestión**, la que se desarrolla con base en la norma ISO 19011.

El software AUDIRISK WEB está diseñado para:

1) Este software satisface los estándares internacionales para el ejercicio profesional de la Auditoría Interna del Instituto de Auditores Internos (IIA) y de ISACA para la Auditoria de Tecnología de Información (TI).
2) Los estándares para el desarrollo profesional de la Auditoría Interna del Instituto de Auditores Internos (IIA), **definen la Auditoría Interna así**: *"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". Nótese que este concepto difiere significativamente de la **Auditoría Interna a Sistemas de Gestión**, la que se desarrolla con base en la norma ISO 19011.

3) El software AUDIRISK WEB está diseñado para:

4) ***Ejecutar Auditorías de Cumplimiento*** *de "Normas Legales y Reglamentarias establecidas por Organismos de Supervisión y Vigilancia del Estado. La metodología de auditoría de cumplimiento implantada en el software comprende procedimientos para ejecutar las cuatro (4) fases del proceso de auditoría: a) Planeación de la Auditoría.* Además de fijar objetivos, alcance, cronograma y auditores responsables, incluye la *construcción de Checklists a la medida de la empresa*, para verificar cumplimiento de normas y procedimientos objeto de la auditoría; b) *Ejecución de Pruebas de Cumplimiento* mediante aplicación de los Checklists; c) *Comunicación de Resultados* (el software genera tres informes con los resultados de la auditoría, dirigidos a la administración de la empresa) y d) *Planeación Seguimiento* a implantación de Planes de Mejoramiento para atender los hallazgos de la auditoría.

5) **Ejecutar Seguimiento a Planes de Mejoramiento**, por Hallazgos, oportunidades de mejora y recomendaciones de Auditorías realizadas con AUDIRISK.

6) **Generar indicadores de Gestión de la Auditoría**. El software genera informes de gestión de la Auditoría Interna en fechas de corte que deseen o necesiten los auditores.

Los papeles de trabajo de las auditorías realizadas con AUDIRISK, se conservan y administran en un repositorio denominado *Base de Datos de Conocimientos de Auditoría*. Esta Base de Conocimientos crece continuamente en la medida que se avanza en la realización de auditorías con el software, hasta llegar a convertirse en un repositorio único de toda la información de las auditorías internas y de sistemas realizadas a la Empresa.

El software AUDIRISK Web se puede instalar en la modalidad **Software como Servicio** - **SaaS**, en una red interna o en computadores stand alone.

AUDIRISK se comercializa con dos tipos de licenciamiento: A perpetuidad y por Suscripción Anual.

Tipos de usuarios en el software AUDIRISK Web.

El software provee dos (2) grupos de perfiles de acceso: ***Auditores y Auditados.***

Los AUDITORES tienen acceso a todas las funcionalidades del software –Acceso Completo. Con excepción de los perfiles Gerente de Auditoría y Supervisor de Auditoría, los demás perfiles tienen acceso solo a las auditorías a las que estén asignados.

Los AUDITADOS tienen acceso limitado a las funcionalidades del módulo "***Seguimiento a Implantación de Planes de Mejoramiento por Hallazgos y Recomendaciones de la Auditoría***". Cada usuario AUDITADO tiene acceso solamente a los hallazgos de auditorías que le sean asignados por los AUDITORES.

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

AUDIT IP Web es una herramienta para apoyar y estandarizar el trabajo de las personas que dentro de una Empresa tienen la responsabilidad de planear, coordinar, implantar y ejecutar seguimiento a los planes de mejoramiento que se establecen para atender hallazgos, oportunidades de mejora y recomendaciones de auditorías realizadas a la Empresa por el personal de la Gerencia de Auditoría Interna o por terceros.

AUDIT IP Web está diseñado para gestionar la implantación y seguimiento de Planes de Mejoramiento Institucional que resultan de hallazgos, oportunidades de mejora y recomendaciones de auditorías realizadas a la Empresa por personal de la Gerencia de Auditoría Interna y por terceros, como son las Firmas de Auditoría Externa (Revisoría Fiscal, Auditoría Financiera, Auditoría de Sistemas, etc.), Organismos de control y vigilancia del Estado (Contralorías, Superintendencias, Ministerios, DIAN), Auditorías Internas a sistemas de gestión realizadas por personal de la empresa o por terceros (ISO 9001, ISO 14000, de salud ocupacional, ISO 27001, ISO 22301, etc.) y Auditorías externas realizadas para fines de certificación de Sistemas de Gestión.

El software AUDIRISK Web se puede instalar en la modalidad **Software como Servicio - SaaS**, en una red interna o en computadores stand alone.
AUDIT IP Web se comercializa con dos tipos de licenciamiento: A perpetuidad y por Suscripción Anual.

Tipos de usuarios en el software AUDIT IP Web.

El software provee perfiles de acceso a través de internet para dos (2) tipos de usuarios: a) Coordinadores de Planes de Mejoramiento y b) Implantadores de Planes de Mejoramiento.

A los usuarios **Coordinadores de Planes de Mejoramiento (PM),** AUDIT IP Web provee funcionalidades para ingresar al sistema los hallazgos, oportunidades de mejora y recomendaciones de los auditores y asignar cargos y personas responsables de implantar el plan de mejoramiento. Mediante correos electrónicos generados y enviados por el software, comunican a los implantadores su asignación como responsables de implantar el PM y las credenciales de usuario para acceder al software e ingresar el plan de mejoramiento. Los coordinadores también tienen privilegios para aprobar o desaprobar el plan de mejoramiento ingresado por los implantadores, así como los avances de implantación y los soportes de implantación del PM aportados por los implantadores (papeles de trabajo electrónicos).

Los **usuarios implantadores de PM**, después de recibir los correos de los coordinadores, pueden configurar el contenido de correos electrónicos que serán generados y enviados automáticamente desde el software, para comunicar el ingreso de las Acciones de Mejora (AM) que integran el PM, el ingreso de avances de implantación y aportar los soportes electrónicos de los avances de implantación. Estos soportes se mantienen disponibles en la base de datos de AUDIT IP Web para su consulta posterior cuando sea necesario.

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

5. SMARTEXPORTER: Software para Extraer, Preparar Y Programar Automáticamente Datos de SAP.

Este producto es un complemento del software IDEA, para permitir extraer e importar datos de archivos SAP a IDEA.

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.

6. CONTROLRISK Web: Software para Gestionar Riesgos en Procesos de negocio y Tecnología de Información (TI).

El software CONTROLRISK WEB provee funcionalidades para soportar la **implantación, monitoreo y mejoramiento continuo** del sistema de Administracion de Riesgos Operacionales (SARO), el sistema Administracion de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT), el Sistema de Gestión de Seguridad de la Información (SGSI) y la Gestión de Riesgos por procesos en Entidades del sector público Colombiano, de acuerdo con las normas establecidas por el DAFP.

Las funcionalidades implantadas en el software satisfacen 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 e ISO 27001 y otras normas nacionales de Gestión de Riesgos expedidas por los organismos de control y supervisión del Estado, el Ministerio de Tecnología de Información y comunicaciones (Mintic) y el Departamento Administrativo de la Función Pública (DAFP).

Para el SARO, el software satisface los siguientes requerimientos:

a) Implantar el ciclo PHVA del proceso de Gestión de Riesgos operacionales en los procesos de la cadena de valor de la Empresa (estratégicos, misionales y de soporte), los procesos de Tecnología de Informacion y las aplicaciones de computador o módulos de ERPs que soportan los procesos CORE del negocio.

b) **Consolidar el Perfil del Riesgo Operacional de la Organización.** El software provee funcionalidades para construir y visualizar *el perfil consolidado por clases de riesgo del SARO en los procesos y áreas organizacionales de la empresa.* Para estas clases de riesgo se generan reportes y gráficos con calificaciones promedio del riesgo inherente (RI), protección ofrecida (PE) por los controles establecidos y riesgo residual (RR). Estos perfiles se visualizan por tipos de procesos (estratégicos, misionales y de soporte) y dentro de éstos por clases de riesgo, por procesos y por áreas organizacionales de la Empresa. El software también provee funcionalidades para generar dos (2) matrices consolidadas de las calificaciones promedio de los eventos de riesgo identificados en todos los procesos de la organización que tengan implantado el SARO: a) **Matriz consolidada de riesgos Inherentes**, con la localización de los códigos de riesgo de todos los procesos de la empresa en las celdas de una matriz de 5x5, "Probabilidad vs Impacto"; **b) Matriz Consolidada de Riesgo Residual,** con la localización de los códigos de riesgo de todos los procesos de la Empresa en las celdas de una matriz de 4 x 5, "Severidad de los riesgos antes de controles Vs niveles de protección ofrecidos por los controles".

c) **Actualizar y Mejorar Continuamente la Gestión de Riesgos implantada para procesos de la cadena de valor, procesos de tecnología de información y los sistemas que soportan las operaciones CORE del negocio y administrativas de la Empresa**. Una vez puesto en operación el sistema de Gestión de Riesgos (SGR) de cada proceso o sistema, el software provee funcionalidades para el mantenimiento y actualización continua de la información de gestión de riesgos. A la base de datos de gestión de riesgos de la Empresa se pueden *adicionar, modificar y suprimir actividades de los procesos, áreas organizacionales y terceros que intervienen en los procesos, eventos de riesgo inherente, controles y cargos de los dueños de proceso* para mantener vigente el sistema de administración de riesgo operativo de cada proceso o sistema. La actualización de la información de gestión de riesgos se pueden realizar en cualquier tiempo, cuando se considere necesario.

d) **Crear y mantener actualizada** la Base de Datos de "Registros de Eventos de Riesgo Operativo Ocurridos (RERO)". El Software provee funcionalidades para que los dueños de los procesos ingresen al sistema la información de los eventos de riesgo materializados y la Gerencia de Riesgos realice **análisis detallado** de los eventos ocurridos y diseñe el plan de correctivo correspondiente. Este análisis verifica la validez y calidad de la documentación del análisis del riesgo existente para cada riesgo materializado, identifica las desviaciones

ocurridas, diseña las acciones de remediación necesarias, asigna los cargos responsables de implantarlas y ejecutar seguimiento a la implantación de las acciones correctivas.

e) **Monitorear periódicamente el Plan de Continuidad del Negocio.** El software provee funcionalidades para ingresar información sobre los controles y estrategias previstas en el Plan de Continuidad del Negocio (BCP) y verificar periódicamente el nivel de preparación de las áreas de la organización para ejecutar los procedimientos de contingencia y recuperación de desastres previstas en el BCP.

f) **Auditar el SARO.** El software provee funcionalidades para que los auditores internos y externos planeen y ejecuten pruebas al SARO. Las pruebas están orientadas a verificar el cumplimiento de las políticas y procedimientos del SARO (el framework) y la calidad de la información de la Base de Datos de Gestión de Riesgos y Controles de la Empresa, el funcionamiento del RERO y del BCP .

Los datos obtenidos en la implantación de la gestión de riesgos de cada proceso o sistema, se conservan y administran en un repositorio denominado *Base de Datos de Conocimientos de Gestión de Riesgos y Controles de la Empresa*. Esta Base de Conocimientos crece continuamente en la medida que se avanza en la implantación de la Gestión de Riesgos en los procesos y sistemas de la Empresa, hasta llegar a convertirse en un repositorio único de toda la información de riesgos y controles de la Empresa.

El software CONTROLRISK puede ser instalado en la modalidad Software como Servicio - **SaaS**, en una red interna o en computadores stand alone.
CONTROLRISK se comercializa con dos tipos de licenciamiento: A perpetuidad y por Suscripción Anual.

Tipos de usuarios en el software CONTROLRISK Web.

CONTROLRISK Web provee perfiles de acceso para tres (3) grupos de usuarios: a) Administradores de Riesgos b) Dueños de Procesos; y c) Auditores.

Los usuarios de perfil **Administradores de Riesgos** tienen acceso a todas las funcionalidades del software, excepto al módulo de auditoría.

Los usuarios de perfil **Dueños de Proceso** tienen acceso a funcionalidades del módulo de Implantación de la Gestión de Riesgos, limitado a uno o más procesos, con permiso para ingresar respuestas a los checklists con los cuales se ejecuta el monitoreo de los riesgos y controles por proceso y a los módulos de monitoreo del Plan de Continuidad del Negocio (BCP) y de Registro de Eventos de Riesgo Ocurridos (RERO);