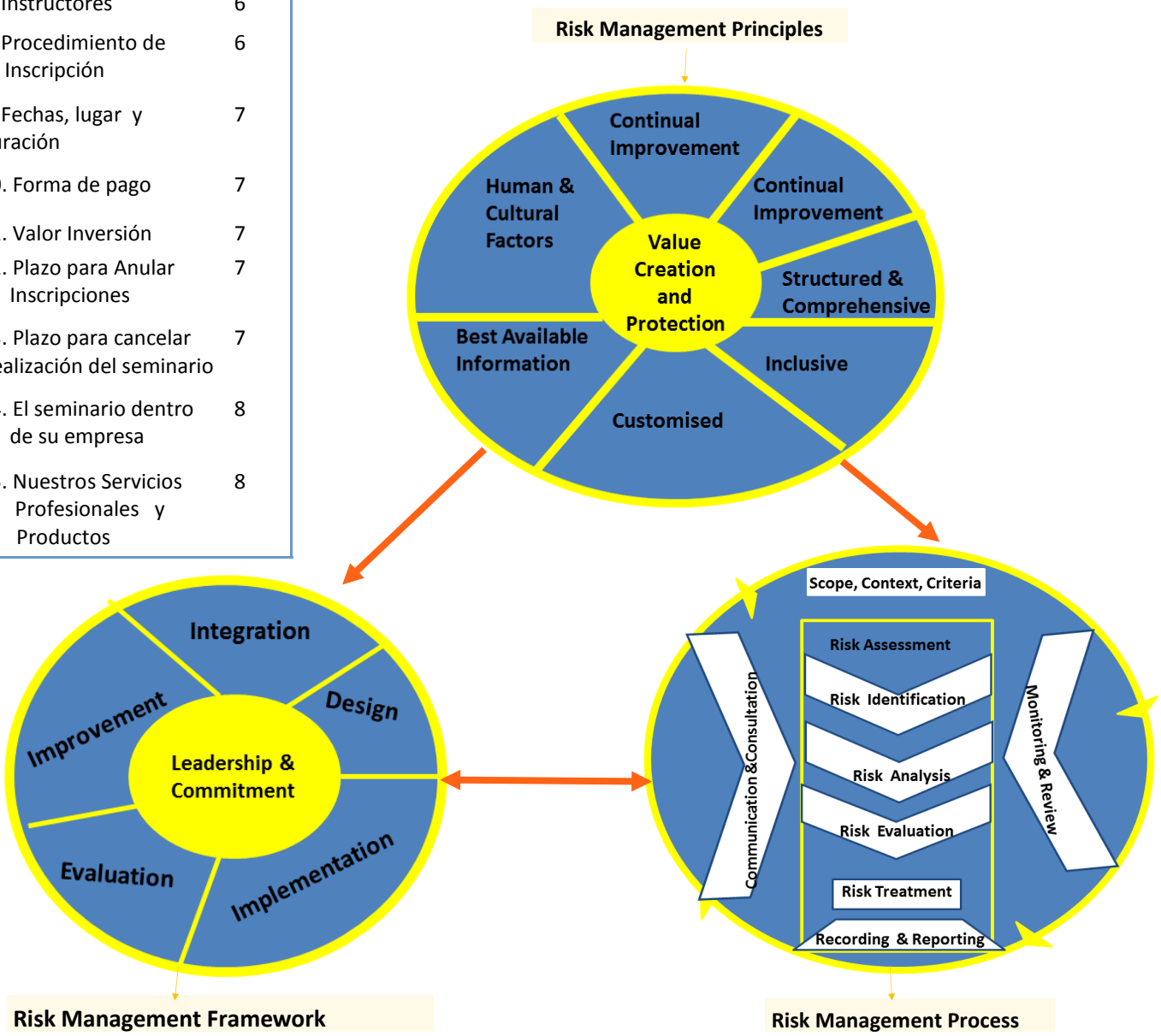
Seminario – Taller
GESTIÓN DE RIESGOS EMPRESARIALES (GRE).

PRESENTACIÓN

La Gestión de Riesgos Empresariales (GRE) es un proceso estratégico de las organizaciones, destinada a hacer frente a todo tipo de riesgos en todas las actividades y funciones del negocio: estratégicas y operativas, misionales, de soporte, asegurables y no asegurables, actuales y emergentes. Tanto los riesgos estratégicos y como los no estratégicos pueden ser de severidad significativa; sin embargo, los riesgos estratégicos tienden a tener características particularmente desafiantes porque atacan o amenazan la misión central o producto de la organización y no son transitorios o esporádicos, sino que constituyen la continua realidad a futuro.

Principles, Framework and risk management Processs from ISO 31000: 2018



Este seminario presentará el marco metodológico para implantar ó revisar la implantación la Gestión de Riesgos Empresariales (GRE), particularmente *para identificar, analizar, valorar, controlar, monitorear y mejorar continuamente los Sistemas de Gestión de Riesgos en las empresas* (estratégicos, operativos, de LA / FT, financieros, legales, de salud ocupacional, ambientales, de seguridad de la información, informáticos, de proyectos, etc).

Según Suzanne Labarge, Jefe de riesgos del Royal Bank of Canadá, "el riesgo en sí mismo no es malo. Lo que sí es malo es que el riesgo esté mal administrado, mal interpretado, mal calculado o incomprendido". De hecho, muchos se están dando cuenta que el riesgo crea oportunidad, la oportunidad crea valor y, por último, el valor crea riqueza para los accionistas. Cómo administrar de la mejor forma los riesgos para obtener ese valor se ha convertido en una pregunta crítica.

El seminario enfatizará en los procedimientos de *identificación y análisis de riesgos inherentes* y *en la necesidad de estandarizar el lenguaje de riesgos y controles y de modernizar el enfoque de control (implantar el enfoque preventivo y proactivo en lugar del enfoque reactivo o A Posteriori),* como factores críticos para asegurar que el SGE satisfaga los objetivos esperados, en concordancia con estándares internacionales y nacionales de Control Interno (COSO 2013, COBIT y MECI) y con otros sistemas de gestión (de calidad, Seguridad de la Información, Planeación de Continuidad del negocio).

PROPUESTA DE VALOR

Al finalizar el seminario los participantes estarán en capacidad de:

a) Definir o revisar el framework o marco de referencia de la Gestión de Riesgos Empresariales (GRE), armonizándolo con el Sistema de Gestión de la Calidad (ISO 9001), el sistema de Gestión de Seguridad de la Información (ISO 27001) y el Sistema de Control Interno de la Organización.

b) Definir ó revisar el universo de riesgos de la Empresa (portafolio de categorías de riesgo aplicables), que servirá de base para identificar y gestionar los riesgos inherentes en los diferentes procesos y sistemas de información de la organización.

c) Determinar la estructura de organización y de soporte tecnológico requeridos para la gestión eficaz de riesgos en la empresa.

d) Por cada proceso o sistema de la empresa: identificar, analizar, valorar, controlar y monitorear los eventos de riesgo inherentes que pueden presentarse.

e) Definir e implantar estándares y buenas prácticas en la empresa para identificar, analizar y documentar los riesgos inherentes.

f) Definir e implantar estándares y buenas prácticas en la empresa para identificar, documentar y diseñar los controles necesarios por cada evento de riesgo inherente.

g) Establecer criterios y buenas prácticas para medir la **efectividad** (eficacia y eficiencia) de los controles que se establezcan para reducir la severidad de los riesgos inherentes a niveles aceptables de riesgo residual.

h) Aplicar el *enfoque de los tres anillos de seguridad* para controlar los riesgos inherentes.

i) Generar indicadores de gestión de riesgos en cada proceso o sistema de la Empresa y a nivel de toda la organización.

j) Determinar y evaluar las características que debe satisfacer una herramienta de "software especializado" para apoyar la gestión de riesgos de la Empresa.

1. OBJETIVOS DEL SEMINARIO

- Transferir conocimientos y procedimientos *para Gestionar los Riesgos inherentes de diferentes tipos (operativo, financiero, legal, de salud ocupacional, ambientales, informáticos, tecnológicos, de proyectos, etc),* en función de los objetivos de la organización (estratégicos, operacionales, de información y cumplimiento con normas y regulaciones).

- Proveer la metodología y "buenas prácticas" para *identificar, analizar, valorar la severidad o nivel de riesgo, controlar y monitorear los eventos de riesgo inherentes,* en diferentes "Sistemas de Gestión de Riesgos" aplicables a las organizaciones, sobre la base de un lenguaje común y lineamientos de los marcos de referencia ISO 31000:2018 y ERM.

- Proveer estrategias para proyectar a mediano y largo plazos, *la perdurabilidad y mejoramiento continuo* de los diferentes sistemas de gestión de riesgos aplicables a la Empresa.

2. A QUIÉN VA DIRIGIDO (PARTICIPANTES)

El seminario está dirigido a Directivos, Ejecutivos y Supervisores de Empresas de los sectores privado y público, con responsabilidades en Gestión de Riesgos, Diseño de Controles, Gestión de Seguridad de la Información, Aseguramiento, Control interno, Auditoría Interna, Revisoría Fiscal y Auditoria de Sistemas.

3. TEMAS DEL SEMINARIO

DÍA 1

1. **MARCO DE REFERENCIA DEL SISTEMA DE GESTIÓN DE RIESGOS EMPRESARIALES.**

- Generalidades de la Gestión de la Gestión de Riesgos Empresariales bajo la norma ISO 31000:2018.
- Generalidades de la Gestión de la Gestión de Riesgos Empresariales bajo el marco de trabajo ERM.
- Generalidades sobre tipos de Sistemas de Gestión de Riesgos (SARO, SARLAFT y otros).
- La Gestión de Riesgos Empresariales y los Sistemas de Gestión (ISO 9001, ISO 27001, ISO 14000 y otros).
- Definición del Portafolio ó Universo de Riesgos de la Empresa - Ejercicio.

2. METODOLOGIA PARA IMPLANTAR LA GESTION DE RIESGOS EN LA ORGANIZACIÓN – PARTE 1: EL FRAMEWORK DE LA GESTIÓN DE RIESGOS

- Definición (contenido) del Framework o marco de Trabajo de la Gestión de Riesgos en la Empresa.
- Diseño y Estructura de las Políticas de Gestión de Riesgos.
- Como se distribuyen las responsabilidades por la Gestión de Riesgos en las Empresas.
- El Ciclo PHVA de la Administración de Riesgos por cada proceso o sistema de la Empresa.
- Etapas de la Metodología de implantación del sistema de gestión de riesgos por procesos.
- Presentación del Caso de Estudio del Seminario: Gestión de Riesgos para un proceso del modelo de operación de la Empresa

DÍA 2.

3. METODOLOGIA PARA IMPLANTAR LA GESTIÓN DE RIESGOS – PARTE 2: IDENTIFICACIÓN Y ANALISIS DE RIESGOS POR PROCESO.

- Definición de Contexto interno y externo del Proceso
- Caracterización del proceso objeto de la gestión de riesgos.
- **Taller 1:** Priorización de categorías del Universo de Riesgos de la Empresa aplicables al proceso – Aplicación del principio de Pareto y del Poder del 3.
- Construcción del Cubo de Riesgos del proceso.
- **Taller 2:** Identificación de los Eventos de Riesgo Inherentes que pueden presentarse en el proceso
- **Taller 3:** Análisis y documentación de los eventos de riesgo inherentes (amenazas) que pueden presentarse. Análisis de los siete (7) elementos del riesgo.
- Elaboración de Mapas /Matrices de Riesgos Inherentes.
- **Taller 4:** Definición de objetivos de Control para el proceso.
- Definición de Acciones de Respuesta a Riesgos.

4. METODOLOGIA PARA IMPLANTAR LA GESTIÓN DE RIESGOS – PARTE 3: CONTROL Y TRATAMIENTO DE RIESGOS.

- Enfoques Preventivo- Proactivo y Reactivo de los Controles.
- Clasificaciones útiles de los controles
- Criterios para diseñar controles efectivos por evento de riesgo inherente.
- **Taller 5:** Diseño de controles por evento de riesgo .
- Cómo identificar los controles establecidos en el proceso (construcción y aplicación del cuestionario CSA –Control Self Assessment).
- Criterios para determinar efectividad (Eficacia + Eficiencia) de los Controles establecidos por evento de riesgo.
- **Taller 6:** Evaluar efectividad de los Controles por Evento de Riesgo Inherente (los tres anillos de seguridad, nivel de automatización y discrecionalidad, costo beneficio)
- Elaboración del Mapa de Riesgos Residuales – antes de tratamientos.
- Diseño, implantación y seguimiento del Plan de Tratamiento de Riesgos.
- Elaboración del Mapa de Riesgos Residuales – Después de tratamientos.

DIA 3.

5. **METODOLOGIA PARA IMPLANTAR LA GESTIÓN DE RIESGOS – PARTE 4: MONITOREAR LOS RIESGOS Y CONTROLES ESTABLECIDOS.**

- Asignación de responsabilidades por ejecución y supervisión de los controles.
- Elaboración de Guías de Monitoreo / Auto-aseguramiento de Controles (Control Self Assessment)
- **Taller 7:** Aplicación y procesamiento de Guías Monitoreo de eventos de riesgo y controles establecidos. Generación de Indicadores de gestión de riesgos por proceso.
- Elaboración del Plan de Acciones de Mejoramiento como resultado de cada monitoreo.
- Mantenimiento / Actualización del Sistema de Administración de riesgos

6. **OTROS COMPONENTES DEL SISTEMA DE GESTION DE RIESGOS EMPRESARIALES.**

- El Mapa de Riesgos Consolidado de la Organización (consolidación de perfiles de riesgo de los procesos).
- El Registro de Eventos de Riesgo Ocurridos (RERO).
- El Plan de Continuidad del Negocio – BCP (El estándar ISO 22301: 2012)
- La Auditoría a los Sistemas de Gestión de Riesgos Empresariales.
- Estructura de organización y soporte tecnológico requerido para la Gestión de Riesgos.

7. **HERRAMIENTAS DE SOFTWARE DE GESTIÓN DE RIESGOS EXISTENTES EN EL MERCADO.**

4. METODOLOGÍA PARA EL DESARROLLO DEL SEMINARIO

El seminario está estructurado en la modalidad de Taller y se desarrollará de manera interactiva entre el facilitador y los participantes, con presentaciones de los temas por parte del facilitador, apoyadas en casos y experiencias del mundo real.

Los talleres del seminario se desarrollarán alrededor de la implantación de la Gestión de Riesgos para un proceso del modelo de operación de la Empresa.

Se realizarán también ejercicios para afianzar los conceptos y desarrollar habilidades para aplicarlos utilizando y formatos diseñados para el uso de la metodología.

5. MATERIAL PARA LOS PARTICIPANTES

Se entregará material escrito en medios magnéticos, con las ideas claves del seminario, formatos de la metodología de administración de riesgos y enunciados de los ejercicios y talleres.

6. CERTIFICACIÓN.

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

7. INSTRUCTORES

Euclides Cubillos M. – **Gerente de Auditoría / Consultoría de AUDISIS**., Ingeniero de Sistemas. Maestría en Dirección y Administración de Empresas. Título de Posgrado en Auditoría de Sistemas, Certificaciones CISA (Certified Information Systems Auditor), COBIT, Auditor ISO 27001, Auditor Líder de Calidad. Experto en Gestión de Riesgos, Seguridad y Auditoría de sistemas. Autor de dos herramientas de software para asistir las actividades de gestión de riesgos y auditoría: CONTROLRISK (Gestión integral de riesgos y diseño de controles) y AUDIRISK (Auditoria basada en riesgos para procesos y sistemas de información). 35 años de experiencia profesional. Ex presidente de la Asociación Colombiana de Auditores de Sistemas (ACDAS) y fundador y ex presidente 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, América, Central de Bogotá, Antonio Nariño, El Rosario, Santo Tomás de Aquino (Bucaramanga), Universidad Militar, UNAB, FUNDEMA (Manizales), Santiago de Cali, Libre de Colombia (Bogotá 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 y al LATINCACS de México.

Alvaro Mauricio Romero -Lead Auditor BS ISO/IEC 27001:2013 -Certified Ethical Hacking CEH Profesional experto en Tecnología y Seguridad de la información con certificaciones como auditor líder BS ISO/IEC 27001:2013 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, CISSP (Certified Information Systems Security Professional) y auditor interno norma ISO 9001 versión 2000. Cuenta con más de 20 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 ante desastres, auditorias basadas en riesgos, pruebas de ethical hacking y análisis de vulnerabilidades en Organizaciones nacionales e internacionales del sector servicios y financiero. Por más de 15 años docente en Seminarios, diplomados y especializaciones de Seguridad Informática y análisis forense informático 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.

8. PROCEDIMIENTO DE INSCRIPCIÓN

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

9. FECHAS, LUGAR Y DURACIÓN

LUGAR: Bogotá, D.C.— GHL Hotel Capital.

FECHAS: Marzo 27, 28 y 29 de 2019.

Septiembre 2, 3 y 4 de 2019.

DURACIÓN: 24 Horas.

HORARIO: De 8:00 AM a 12:00 M y de 1:00 PM a 5:00 PM.

10. 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.

11. VALOR INVERSIÓN POR PARTICIPANTE

Pagos antes del Seminario	Pagos **después del Seminario**
COL $ 1.450.000 + IVA	$ 1.515.000 + IVA

Descuentos por Participantes de la misma Empresa	
Hasta 3 Participantes	5 %
4 y 5 Participantes	7.5 %
Más de 6 Participantes	10 %

Miembros de ISACA y DEL IIA: Descuento del 5%

12. PLAZO PARA ANULAR LAS INSCRIPCIONES

Se acepta anulación de inscripciones por escrito, hasta 4 días hábiles antes de la realización del seminario. Después de esta fecha, únicamente se aceptará el cambio de participantes inscritos.

13. PLAZO PARA CANCELAR LA REALIZACIÓN DEL SEMINARIO

AUDISIS se reserva el derecho de cancelar el seminario en caso de no completarse el número mínimo de participantes requerido.

14. EL SEMINARIO DENTRO DE SU EMPRESA

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

Contáctenos: audisis@audisis.com
Tels: (571) 2556717- **PBX:** (571) 3470022

15. NUESTROS PRODUCTOS Y SERVICIOS PROFESIONALES

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.

1. CONSULTORÍA EN CONTROL INTERNO, GESTION DE RIESGOS EMPRESARIALES Y SEGURIDAD EN TECNOLOGIA DE LA INFORMACION (TI).

- Implantación de Sistemas de Control Interno (COBIT, MECI, COSO).
- Implantación de Gestión de Seguridad de la Información (ISO 27001).
- Implantación de Gestión de Riesgos empresariales con base en ISO 31000:2009 (SARO, SARLAFT, Salud y otros).
- Implantación de Planes de Continuidad del Negocio y de Tecnología de Información (ISO 22301).
- Diseño de controles para Sistemas de Información y Procesos de negocio.
- Prevención, detección e investigación de fraudes y delitos informáticos. D
- Desarrollo de programas Antifraude.

2. AUDITORÍAS DE SISTEMAS Y DE PROCESOS DEL NEGOCIO.

- Auditorías de Sistemas de Información “Basada en Riesgos Críticos”.
- Pruebas de Hacking Ético.
- Auditoría Forense.
- Auditoría Basada en Riesgos críticos a procesos de Negocio.

3. OUTSOURCING DE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN PARA AUDITORIAS INTERNAS, REVISO RIAS FISCALES U AUDITORIAS FINANCIERAS.

4. AUTOMATIZACIÓN DE PRUEBAS DE AUDITORÍA A LA MEDIDA DE LAS NECESIDADES DE LA EMPRESA (Desarrollo de CAATs e implementación).

5. NTERVENTORIA EN PROYECTOS DE SISTEMAS, SEGURIDAD Y AUDITORÍA DE SISTEMAS

6. PERITAZGOS EN LITIGIOS DE CONTRATOS DE SERVICIOS PROFESIONALES EN TECNOLOGÍA DE INFORMACIÓN.

7. EDUCACIÓN Y DESARROLLO PROFESIONAL EN CONTROL INTERNO, ADMINISTRACIÓN DE RIESGOS, SEGURIDAD DE TI Y AUDITORÍA DE SISTEMAS.

- Seminarios abiertos virtuales para para participantes de diferentes empresas.
- Seminarios cerrados presenciales o virtuales, dentro de las empresas.

NUESTROS PRODUCTOS

AUDIRISK: Software de Auditoría Basada en Riesgos críticos para Procesos de Negocio, Sistemas y Tecnología de Información.

AUDIT IP: Software de Gestionar el seguimiento a Planes de Mejoramiento Institucional.

CONTROLRISK: Software de Gestión de Riesgos y Diseño de Controles para Procesos de Negocio, Sistemas y Tecnología de Información**.**

IDEA: Software para Análisis, Extracción, Auditoría de Datos y Desarrollo de CAATTs.

WORKING PAPERS: Software de Papeles de Trabajo de Auditoria Financiera.

MONITOR: Software de Monitoreo Continuo y Auditoría Continua de Riesgos y Controles.