AVISO IMPORTANTE

La presente información fue elaborada por Restrepo Oramas SAS con propósitos exclusivamente académicos, teniendo como base la experiencia profesional adquirida en los últimos 17 años, lo cual permitió realizar un juicioso análisis y conceptualización sobre los documentos originales de las normas ISO. Restrepo Oramas SAS, no se hace responsable sobre cualquier tipo de decisión tomada con base en la información de carácter académico incluida en esta presentación.

El presente documento es para uso exclusivo de quien recibe de manera directa esta información por parte de Restrepo Oramas SAS; quedando prohibida la reproducción, difusión o diseminación total o parcial.

Se recomienda adquirir las normas oficiales ISO en las entidades autorizadas para su venta.

BDO RESTREPO ORAMAS SAS www.ro-sas.com

PRESENTACIÓN DEL EQUIPO

- ✓ Nombre
- ✓ Cargo y área
- ✓ Experiencia en Seguridad de la Información.
- ✓ Expectativas del curso
- ✓ Algo más que nos quiera contar

Ver video VISA

Carlos A. Restrepo Oramas

Experto Gestión Integral de Riesgo

(Auditor Líder ISO 9001, CISA, CISM, CGEIT, CRISC, CBCP, Lead Implementer ISO 22301, ISO 27001, ISO 20000 Lead Auditor ISO 22301, ISO 27001, ISO 20000, ISO 18001,Risk Manager ISO 31000, ITIL V3, Cobit 5)

Profesional con mas de 25 años de experiencia, desempeñando cargos directivos en empresas de reconocido prestigio internacional tales como VISA, Synapsis, IQ Outsourcing, Superintendencia Financiera de Colombia y Deloitte. Carlos Restrepo hace parte del comité Técnico 287 de ISO Internacional, encargado de revisar y actualizar la norma internacional para gestión de riesgos ISO 31000. Adicionalmente, como reconocimiento por promover la cultura de riesgo en 15 países de Latinoamérica, fue nominado por el diario especializado en economía y negocios "Portafolio" como el mejor docente año 2016, convirtiéndose a la fecha en el latinoamericano que más cursos de certificación internacional en riesgo y auditoria ha dictado en el mundo, en los últimos 96 meses (112 en 16 países).

Su capacidad de combinar conocimiento y experiencia como conferencista, catedrático, consultor, auditor, implementador de Sistemas de Gestión Integral de Riesgo; así como ejercer su rol de Gerente de Procesos y Riesgos en VISA y consultor ERS en Deloitte; le han permitido obtener la máxima calificación en calidad y satisfacción para la totalidad de los entrenamientos ejecutivos realizados en México, Costa Rica, Honduras, Nicaragua, Guatemala, Panamá, El Salvador, República Dominicana, Colombia, Venezuela, Perú, Bolivia, Chile, Ecuador, Paraguay y Argentina.

(57) 3003161468 personal_carlos@yahoo.com.ar

ACERCA DE LA ENTIDAD CERTIFICADORA

ERCA
APPROVED TRAINING COURSE

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

METODOLOGIA DE EVALUACIÓN

- ✓ Evaluación del candidato

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

METODOLOGIA DE EVALUACIÓN

- ✓ Actividades de evaluación
  - Participación activa
  - Solución de caso
  - Evaluación intermedia
  - Evaluación final

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

METODOLOGIA DE EVALUACIÓN

- ✓ Actividades de evaluación

Participación activa

- 5 puntos sobre la evaluación final

Solución de caso de estudio

- 6 puntos sobre la evaluación final

Examen final

- 10 puntos sobre la evaluación final

Puntaje mínimo para aprobar el curso son 15 puntos

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

OBJETIVO GENERAL

- ✓ Adquirir o fortalecer los conocimientos y habilidades necesarias para realizar de manera efectiva una auditoria al Sistema de Seguridad de la Información SGSI, con base en estándares internacionales y mejores prácticas del mercado.

BDO RESTREPO RAMAS... www.ro-sas.com

OBJETIVOS ESPECÍFICOS

- ✓ Generar valor a la organización mediante la aplicación de técnicas de auditoria orientadas a evaluar la efectividad y eficiencia sobre aspectos claves y determinantes de seguridad de la información en la organización.
- ✓ Incrementar la competencia del equipo de auditoria interna, mediante la participación en este tipo de capacitaciones adquiriendo nuevos conocimientos y enterándose de experiencias reales que permitan impulsar la mejora continua en la práctica de auditoria.

BDO RESTREPO RAMAS... www.ro-sas.com

OBJETIVOS ESPECÍFICOS

- ✓ Respaldar el conocimiento y habilidad mediante una certificación como Auditor Interno ISO 27001:2013, expedida por una empresa de reconocimiento internacional.
- ✓ Prepararse para recibir una auditoria externa a Sistema de Gestión de Seguridad de la Información SGSI.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

AGENDA

INTRODUCCIÓN AL SGSI ISO 27001:2013

- ✓ Conceptos básicos de Seguridad de la Información.
- ✓ Estándares de la familia ISO/IEC JTC 1/SC 27
- ✓ Aspectos generales de la norma ISO 27002:2013.
- ✓ Taller: Glosario de términos ISO 27000:2016

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

AGENDA

REVISIÓN Y ANÁLISIS NORMA 27001:2013

- ✓ Taller: Modelo de Gestión PHVA
- ✓ El Modelo de Gestión PHVA y el SGSI
- ✓ Análisis e interpretación de los requisitos consagrados en las cláusulas 4 a 10 de la ISO 27001:2013.

BDO RESTREPO RAMAS... www.ro-sas.com

AGENDA

REVISIÓN Y ANÁLISIS NORMA 27001:2013

- ✓ Revisión y análisis del anexo A de la norma ISO 27001:2013.

BDO RESTREPO RAMAS... www.ro-sas.com

AGENDA

AUDITORIA CON BASE EN LA NORMA 19011:2012

- ✓ Diseño de un programa de auditoria al SGSI
- ✓ Aspectos fundamentales a ser auditados al SGSI.
- ✓ Métodos de auditoria y su aplicación

AGENDA

AUDITORIA CON BASE EN LA NORMA 19011:2012

- ✓ Elementos a considerar para recolectar evidencia
- ✓ Taller: Fundamentos técnicas de auditoria
- ✓ Administración y mantenimiento de los papeles de trabajo

AGENDA

AUDITORIA CON BASE EN LA NORMA 19011:2012

- ✓ Validación de las NO Conformidades y oportunidades de mejora
- ✓ Redacción de No Conformidades y del informe final
- ✓ Presentación, sustentación y distribución del informe final
- ✓ Taller: Redacción y presentación de NO Conformidades evidenciadas en la auditoria

BDO RESTREPO RAMAS... www.ro-sas.com

AGENDA

- ✓ Conclusiones y cierre de la capacitación
- ✓ Examen final Auditor Interno ISO 27001:2013 (2 horas)

BDO RESTREPO RAMAS... www.ro-sas.com

ACUERDOS LOGISTICOS

- ✓ Horario
- ✓ Descansos intermedios
- ✓ Participación activa
- ✓ Respeto por las diferencias de opinión

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONCEPTOS BÁSICOS

- ✓ Gestión de Integral de Riesgo
- ✓ Apetito al Riesgo
- ✓ Principales interesados
- ✓ Grado de Madurez
- ✓ Práctico, familiar, efectivo, cumplible.
- ✓ Documentar lo necesario

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

INTRODUCCION ISO 27001:2013

- 0. INTRODUCCIÓN
- 1. ALCANCE
- 2. REFERENCIAS NORMATIVAS
- 3. TÉRMINOS Y DEFINICIONES
- 4. CONTEXTO DE LA ORGANIZACIÓN
- 5. LIDERAZGO
- 6. PLANIFICACIÓN
- 7. SOPORTE
- 8. OPERACION
- 9. EVALUACIÓN DE DESEMPEÑO
- 10. MEJORA

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

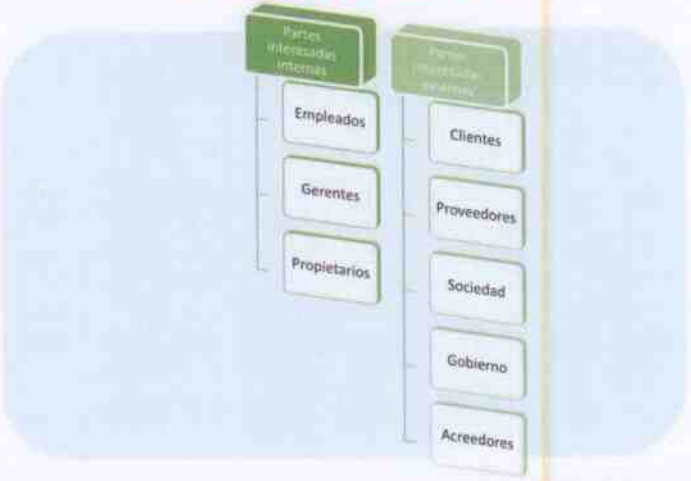
FAMILIA ISO/IEC JTC 1/SC 27

www.iso.org

✔ ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements	60.60	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27001:2013/Cor 1:2014	60.60	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls	60.60	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27002:2013/Cor 1:2014	60.60	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27004:2009 Information technology – Security techniques – Information security management – Measurement	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC TR 27008:2011 Information technology – Security techniques – Guidelines for auditors on information security controls	90.92	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27010:2012 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications	60.60	35.040	ISO/IEC JTC 1/SC 27
✔ ISO/IEC 27011:2008 Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	90.92	35.040	ISO/IEC JTC 1/SC 27

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

PARTES INTERESADAS



CONTENIDO DE LA NORMA

0. INTRODUCCIÓN
   - 0.1 GENERALIDADES
   - 0.2 COMPATIBILIDAD CON OTRAS NORMAS
1. OBJETO Y CAMPO DE APLICACIÓN
2. REFERENCIAS NORMATIVAS
3. TÉRMINOS Y DEFINICIONES
4. CONTEXTO DE LA ORGANIZACIÓN
   - 4.1 DESCRIPCIÓN DE LA ORGANIZACIÓN Y SU CONTEXTO
   - 4.2 ENTENDIMIENTO DE LAS NECESIDADES Y EXPECTATIVAS DE LOS INTERESADOS
   - 4.3 DETERMINAR EL ALCANCE DEL SISTEMA DE GESTIÓN

CONTENIDO DE LA NORMA

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO
5.2 POLÍTICA
5.3 ROLES, RESPONSABILIDADES Y AUTORIDAD

6. PLANIFICACIÓN

6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDAES
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA ALCANZARLOS

CONTENIDO DE LA NORMA

7. SOPORTE

7.1 RECURSOS
7.2 COMPETENCIA
7.3 TOMA DE CONCIENCIA
7.4 COMUNICACIÓN
7.5 INFORMACIÓN DOCUMENTADA

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL
8.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO DE LA NORMA

9. EVALUACIÓN Y DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN
9.2 AUDITORIA INTERNA
9.3 REVISIÓN POR LA DIRECCIÓN

10. MEJORA

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS
10.2 MEJORA CONTINUA

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

0. INTRODUCCIÓN

0.1 GENERALIDADES

La adopción de un SGSI es una decisión estratégica.

Considerar necesidades y objetivos de la organización, requisitos de seguridad, procesos organizacionales así como el tamaño y estructura de la organización.

Aplicación de un proceso de gestión de riesgo dando confianza a las partes interesadas.

SGSI como parte de los procesos de la organización,

SGSI considerada en el diseño de procesos, sistemas y controles

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

0. INTRODUCCIÓN

0.2 COMPATIBILIDAD CON OTRAS NORMAS

Estructura útil para las organizaciones que decidan poner en funcionamiento un único sistema de gestión que cumpla simultáneamente los requisitos de dos o más normas del sistemas de gestión

DESARROLLO DE LA NORMA

1. OBJETO Y CAMPO DE APLICACIÓN

Requisitos para planificar, establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI aplicables Al contexto dela organización.

Requisitos para la evaluación y tratamiento de riesgos adaptados a las necesidades de la organización

Cuando se declara conformidad con esta norma No se acepta excluir requisitos de la cláusula 4 a 10.

DESARROLLO DE LA NORMA

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 Descripción de la organización y su contexto

DEBE determinar aspectos externos e internos pertinentes al propósito y que afecten el logro de objetivos del SGSI.

ISO 31000:2009 Cláusula 5.3

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

4. CONTEXTO DE LA ORGANIZACIÓN

4.2 Entendiendo necesidades y expectativas de las partes interesadas

Al establecer el SGSI se DEBE determinar:

- ✓ Las partes interesadas pertinentes al SGSI.
- ✓ Los requisitos de estas partes interesadas
- ✓ Requisitos legales y reglamentarios

(Documentados, actualizados, comunicados)

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

4. CONTEXTO DE LA ORGANIZACIÓN

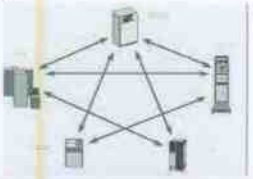
4.3 Determinar el alcance del SGSI

Se DEBE determinar los límites y la aplicabilidad del SGSI

Tener en cuenta aspectos internos y externos (Numeral 4.1)
Los requisitos (numeral 4.2)

Interfaces y dependencias con otras organizaciones

Disponible como información documentada



BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

4. CONTEXTO DE LA ORGANIZACIÓN

4.4 Sistema de Gestión de Seguridad de la Información SGSI

Se DEBE establecer, implementar, mantener, y mejorar continuamente el SGSI

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

5. LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección DEBE

Establecer una política de seguridad de la información y objetivos compatibles con la estrategia.

Integración de los requisitos de seguridad de la información con los procesos de negocio.

Asignar recursos

Comunicar la importancia de la gestión efectiva del SGSI

DESARROLLO DE LA NORMA

5. LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección DEBE

Promover la mejora continua

Lograr los objetivos previstos del SGSI

Apoyar roles directivos demostrando liderazgo en su área de aplicación

DESARROLLO DE LA NORMA

5.3 POLÍTICA

5.2 Política

La alta dirección DEBE establecer una política de Seguridad de la Información, la cual DEBE

- ✓Ser adecuada para el propósito de la organización
- ✓Proporcionar el marco para establecer los objetivos de Seguridad de la Información
- ✓Incluir un compromiso para satisfacer los requisitos aplicables
- ✓Incluir un compromiso de mejora continua del SGSI

BDO RESTREPO RAMAS www.ro-sas.com

DESARROLLO DE LA NORMA

5.2 POLÍTICA

La Política DEBE

- ✓Estar disponible como información documentada
- ✓Ser comunicada dentro de la organización
- ✓Estar disponible para las partes interesadas, según sea apropiado

BDO RESTREPO RAMAS www.ro-sas.com

DESARROLLO DE LA NORMA

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES

La alta dirección DEBE asegurarse que las responsabilidades y autoridades se asignen y sean comunicadas dentro de la organización

La alta dirección DEBE asignar responsabilidad y autoridad para:

✓Asegurar la conformidad del SGSI con esta norma

✓Informar sobre el desempeño del SGSI a la alta dirección

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.1.1 Acciones para direccionar riesgos y oportunidades

Se DEBE considerar en la planeación los aspectos mencionados en el numeral 4.1 y requisitos del numeral 4.2 de esta norma y determinar los riesgos y oportunidades para asegurar que el SGSI logre los resultados, prevenga o reduzca los efectos no deseados y logre el mejoramiento continuo.

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.1.1 Acciones para administrar riesgos y oportunidades

Se DEBE planear:

- ✓Acciones para administrar estos riesgos y oportunidades
- ✓Integrar e implementar las acciones
- ✓Evaluar la eficacia de esas acciones

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.1.2 Evaluación de riesgo de seguridad de la información

Se DEBE definir y aplicar un proceso de evaluación de riesgo de seguridad de la información que:

- ✓ Establezca y mantenga criterios de riesgo (aceptación , evaluación)
- ✓ Resultados consistentes válidos y comparables de los riesgos
- ✓ Identifique riesgos y asigne propietario
- ✓ Analice riesgos (probabilidad/ impacto)
- ✓ Evalúe riesgos (criterios de riesgo – priorización)

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.1.3 Tratamiento de riesgos de seguridad de la información

Se DEBE definir y aplicar un proceso de tratamiento de riesgo de seguridad de la información que:

- ✓ Seleccione las opciones apropiadas
- ✓ Determine todos los controles necesarios
- ✓ Contemplar todos los controles del anexo A
- ✓ Producir una declaración de aplicabilidad
- ✓ Formular plan de tratamiento / aprobado por el dueño del riesgo y aceptación del riesgo residual.

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.1.3 Tratamiento de riesgos de seguridad de la información

Se DEBE conservar información documentada acerca del proceso de tratamiento.

BDO RESTREPO RAMAS... www.ro-sas.com

REFLEXION !

Cuando no hay suficiente claridad sobre los Riesgos...

BDO RESTREPO RAMAS... www.ro-sas.com

QUEDAMOS EN MANOS DEL AZAR¡¡¡

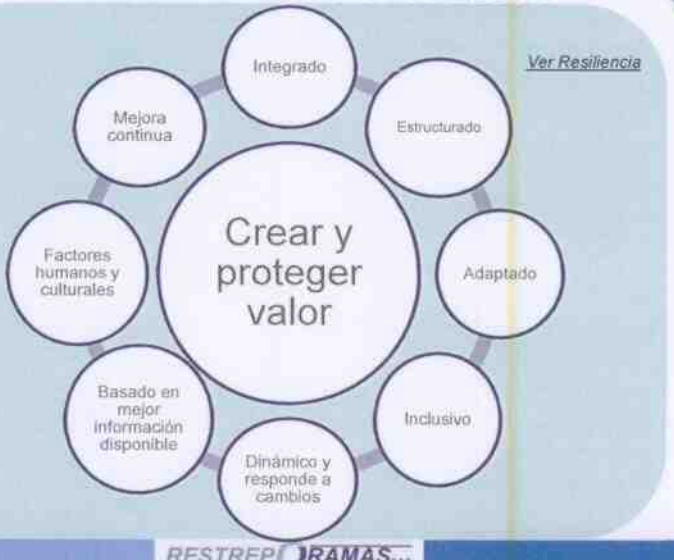
BDO RESTREPO RAMAS... www.ro-sas.com

DEFINCIÓN DE RIESGO ISO 31000:2009

RIESGO: Efecto de la incertidumbre sobre los objetivos

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

PRINCIPIOS ISO 31000:2018



Ver Resiliencia

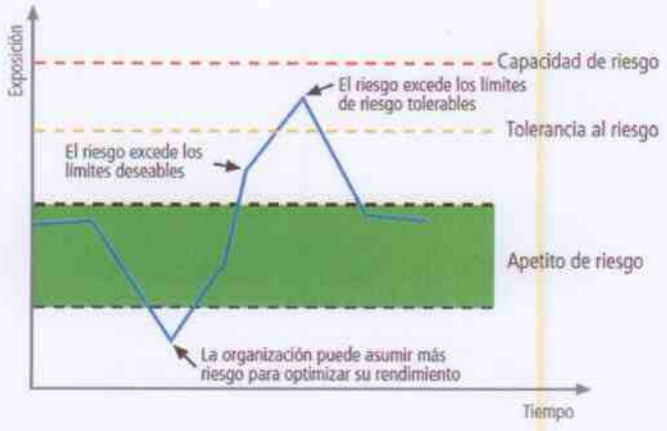
BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

REFLEXION !

Cuando no hay suficiente claridad sobre los Riesgos...

BDO RESTREPO RAMAS... www.ro-sas.com

APETITO AL RIESGO



BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.2 Objetivos de Seguridad de la Información y planes para alcanzarlos

DEBE establecer los objetivos en las funciones y niveles pertinentes

Los objetivos de seguridad de la información DEBEN:

- ✓Ser coherentes con la política
- ✓Ser medible (si es posible)
- ✓Tener en cuenta los requisitos aplicables y los resultados de evaluación y tratamiento de riesgo
- ✓Ser comunicados
- ✓Controlarse y actualizarse según corresponda

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

6 PLANIFICACIÓN

6.2 Objetivos de Seguridad de la Información y planes para alcanzarlos

Al planificar el logro de objetivos la organización DEBE determinar:

- ✓Lo que se va hacer
- ✓Los recursos requeridos
- ✓Quien será responsable
- ✓Cuando se finalizará
- ✓Cómo se evaluaran los resultados.

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

7 SOPORTE

7.1 Recursos

Se DEBE determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar el SGSI

7.2 Competencia

Se DEBE:

- ✓Determinar las competencias necesarias
- ✓Asegurar que las personas son competentes
  (Educación, entrenamiento, experiencia)
- ✓Adquirir las competencias necesarias y evaluar su eficacia.
- ✓Mantener evidencia documentada

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

7.3 Toma de conciencia

Las personas DEBEN ser conscientes de:

- ✓La política de Seguridad de la Información
- ✓Su contribución a la eficacia del SGSI, incluyendo beneficios de mejora de desempeño
- ✓Las implicaciones de las no conformidades

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

7.4 Comunicación

Se DEBE determinar la necesidad de comunicación interna y externa incluyendo:

- ✓Contenido
- ✓A quien se comunicará
- ✓Cuándo comunicar
- ✓Quien debe comunicar
- ✓Procesos para llevar a cabo la comunicación.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

7.5. Información documentada

7.5.1 El SGSI DEBE incluir:

- ✓La información documentada requerida por la norma.
- ✓La información documentada que determine la organización Como necesaria para el SGSI.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

7.5. Información documentada

7.5.2 Creación y actualización

Se DEBE asegurar

- ✓Identificación y descripción (título, nombre, fecha, autor, número)
- ✓Formato, medios de comunicación, revisión y aprobación adecuada y pertinente

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

7.5. Información documentada

7.5.3 Control de la información documentada

Se DEBE controlar la información documentada asegurando que:

- ✓Este disponible y sea apropiada para su uso (donde y cuando se necesite)
- ✓Esté adecuadamente protegida

Para en control DEBE tener en cuenta:

- ✓Distribución, acceso, recuperación, uso, retención, eliminación
- ✓Almacenamiento, conservación, legibilidad
- ✓Control de cambios, prevenir uso información obsoleta.
- ✓Retención y disposición
- ✓Información de origen externo identificada y controlada.

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

8 OPERACIÓN

8.1 Planificación y Control en las operaciones

Se DEBE planear, implementar y controlar los procesos necesarios para cumplir numeral 6.1 y lograr los objetivos determinados en 6.2:

- ✓Mantener información documentada como evidencia de la realización de los procesos según lo planificado

DEBE
Controlar cambios previstos y revisar consecuencias de los no deseados tomando acciones correctivas

DEBE asegurar que los procesos contratados externamente estén controlados

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

8 OPERACIÓN

8.2 Evaluación de riesgos de seguridad de la información

DEBE realizarse evaluaciones de riesgos de seguridad de la información a intervalos planificados o ante cambios significativos

DEBE conservar información documentada de los resultados de la evaluación de riesgo

BDO RESTREPO RAMAS... www.ro-sas.com

DESARROLLO DE LA NORMA

8 OPERACIÓN

8.3 Tratamiento de riesgos de seguridad de la información

DEBE implementar el plan de tratamiento de riesgos

DEBE conservar información documentada de los resultados

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

9 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

DEBE evaluar el desempeño de la seguridad de la información y la eficacia del SGSI

DEBE determinar:

- ✓Qué debe ser monitoreado y medido
- ✓Métodos de seguimiento y medición validando resultados
- ✓Los periodos para realizar el seguimiento y la medición
- ✓Quien realizará el seguimiento, medición y quien analiza
- ✓Cuando los resultados deben ser analizados

DEBE mantener la información documentada como evidencia de los resultados

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

9 EVALUACIÓN DEL DESEMPEÑO

9.2 Auditoria interna

DEBEN realizar auditorias internas a intervalos planificados para validar que el SGSI

- ✓Se ajusta a los requisitos propios de la organización y cumple esta norma
- ✓Es eficazmente implementado y mantenido, para lo cual se DEBE
  - ✓Contar con un programa de auditoria que incluya fechas, métodos, responsabilidades, requisitos de planificación y resultados, considerando la importancia de los procesos y resultados anteriores de auditoria.
  - ✓Definir los criterios de auditoria y su alcance
  - ✓Seleccionar auditores objetivos e imparciales
  - ✓Garantizar el reporte de los resultados a la Alta Dirección
  - ✓Mantener evidencia de la implementación del programa y sus resultados

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

9 EVALUACIÓN DEL DESEMPEÑO

9.3 Revisión por la Dirección

La alta dirección DEBE revisar el SGSI a intervalos planificados asegurando idoneidad, adecuación y eficacia

La revisión DEBE incluir:

- ✓Estado de acciones de revisiones anteriores
- ✓Cambios internos y externos que afecten el SGSI
- ✓Información sobre el desempeño y tendencias del plan contemplando las no conformidades, el seguimiento y evaluación de las mediciones y los resultados de la auditoria
- ✓Resultados de la auditoria
- ✓Resultados de la evaluación de riesgo y su plan de tratamiento
- ✓Las oportunidades de mejora

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

DESARROLLO DE LA NORMA

9 EVALUACIÓN DEL DESEMPEÑO

9.3 Revisión por la Dirección

El resultado de la revisión DEBE incluir decisiones orientadas a la mejora continua y posibles cambios junto con:

- ✓Variaciones en el alcance
- ✓Mejora en la eficacia del Plan
- ✓Modificación a los procedimientos y controles respondiendo a eventos que puedan afectar el Plan incluyendo cambios en los requisitos del negocio, reducción de riesgo, condiciones de operación, requisitos legales o contractuales, criterios de aceptación del riesgo, recursos necesarios, financiación
- ✓Cómo es medida la eficacia de los controles

Se DEBE conservar evidencia documentada de la revisión por la dirección, comunicando los resultados del examen por parte de las partes interesadas y tomando las medidas apropiadas.

DESARROLLO DE LA NORMA

10 MEJORA

10.1 No conformidades y acción correctiva

Para una no conformidad se DEBE

- ✓Reaccionar
- ✓Tomar las medidas para controlarlas, corregirlas y tratar las consecuencias
- ✓Adoptar medidas para eliminar la causa evitando su repetición, revisando la eficacia de la acción tomada asegurando la actualización del Plan
- ✓Implementar la acción requerida
- ✓Revisar la eficacia de la acción tomada
- ✓Hacer los cambios necesarios al SGSI

Las acciones correctivas DEBEN ser apropiadas, manteniendo documentación de su naturaleza y acciones tomadas, junto con los resultados de cualquier acción correctiva

DESARROLLO DE LA NORMA

10 MEJORA

10.2 Mejora continua

Se DEBE mejorar continuamente la idoneidad, adecuación y eficacia del Sistema de Gestión de Seguridad de Información

BDO RESTREPO RAMAS... www.ro-sas.com

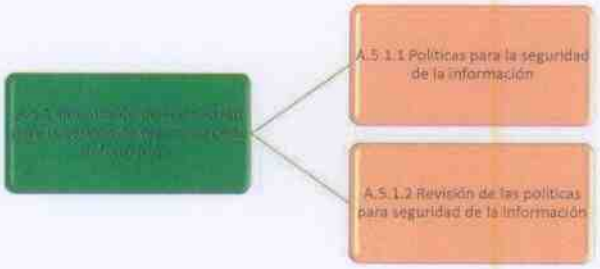
ANEXO A

27001:2013

BDO RESTREPO RAMAS... www.ro-sas.com

A.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.



BDO RESTREPOGRAMAS... www.ro-sas.com

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

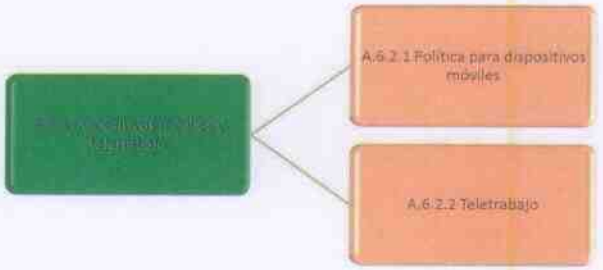
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

Nuevo

BDO RESTREPOGRAMAS... www.ro-sas.com

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

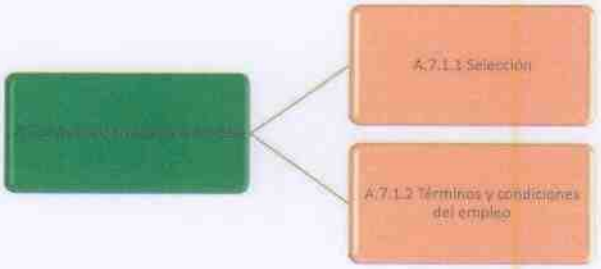
Objetivo: Garantizar* la seguridad del teletrabajo y el uso de dispositivos móviles.



BDO RESTREPO RAMAS... www.ro-sas.com

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

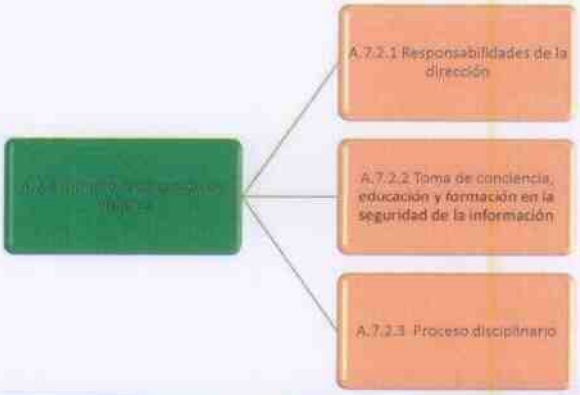
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.



BDO RESTREPO RAMAS... www.ro-sas.com

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

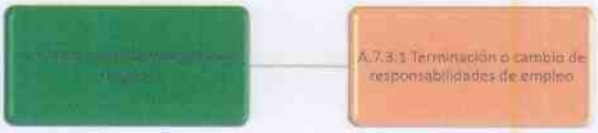
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.



BDO RESTREPO RAMAS... www.ro-sas.com

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

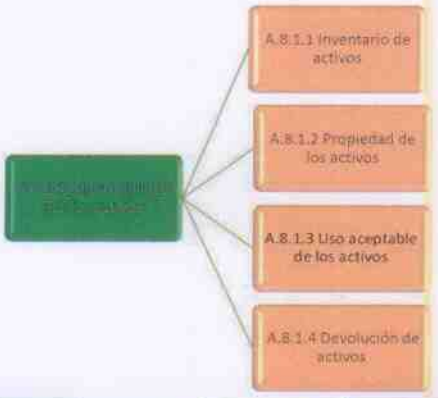
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.



BDO RESTREPO RAMAS... www.ro-sas.com

A.8 GESTIÓN DE ACTIVOS

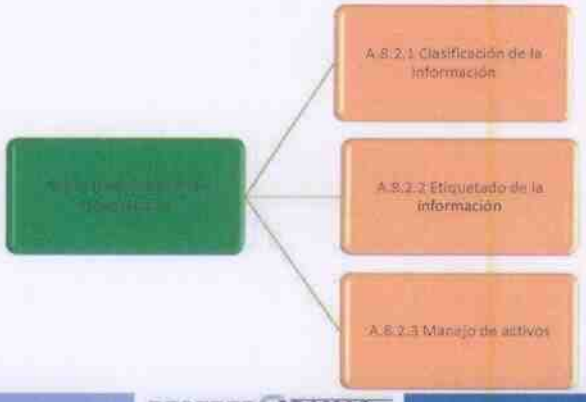
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.



BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.8 GESTIÓN DE ACTIVOS

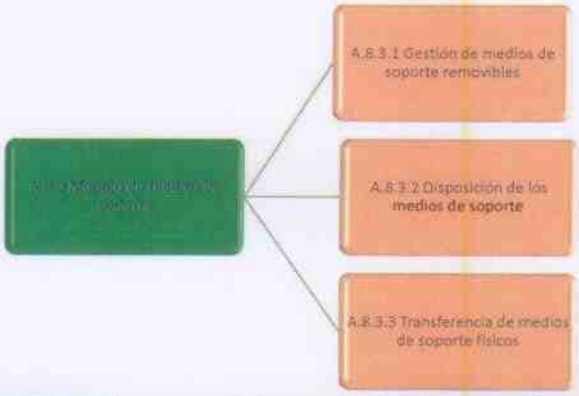
Objetivo: Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.



BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.8 GESTIÓN DE ACTIVOS

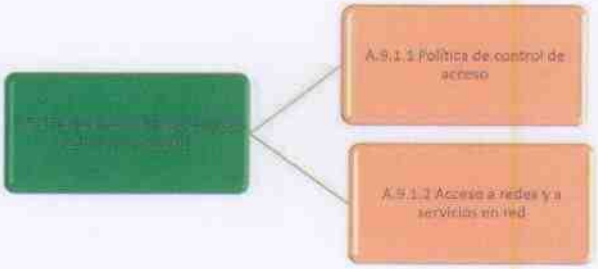
Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.



BDO RESTREPO RAMAS... www.ro-sas.com

A.9 CONTROL DE ACCESO

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.



BDO RESTREPO RAMAS... www.ro-sas.com

A.9 CONTROL DE ACCESO

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

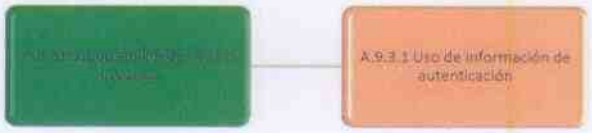
A.9 CONTROL DE ACCESO

Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.9 CONTROL DE ACCESO

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.



BDO RESTREPO RAMAS... www.ro-sas.com

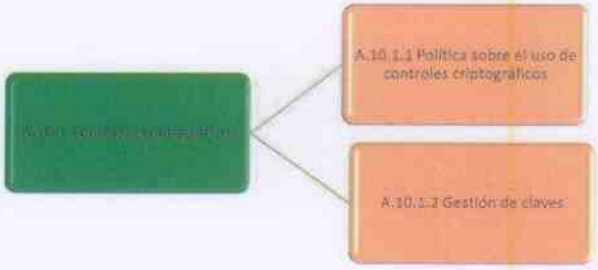
A.9 CONTROL DE ACCESO

Objetivo: Prevenir el uso no autorizado de sistemas y de aplicaciones.

BDO RESTREPO RAMAS... www.ro-sas.com

A.10 CRIPTOGRAFÍA

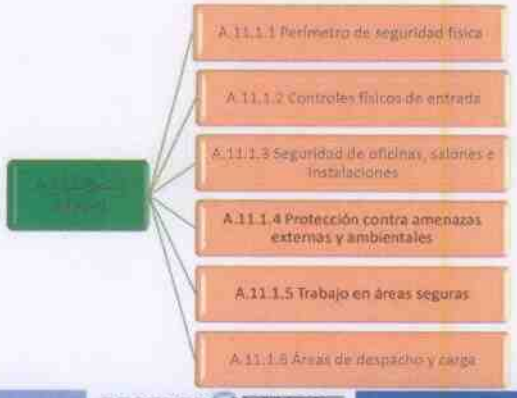
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de información.



BDO RESTREPO RAMAS... www.ro-sas.com

A.11 SEGURIDAD FÍSICA Y AMBIENTAL

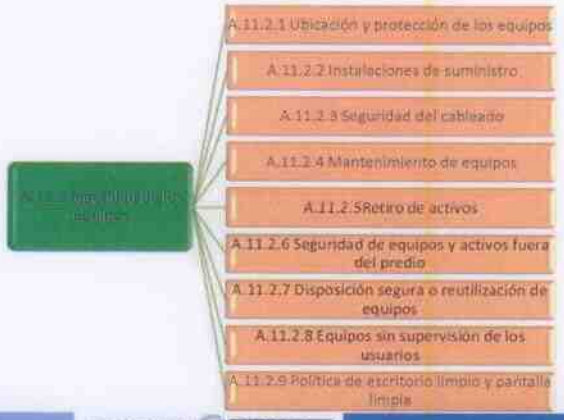
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.



BDO RESTREPO RAMAS... www.ro-sas.com

A.11 SEGURIDAD FÍSICA Y AMBIENTAL

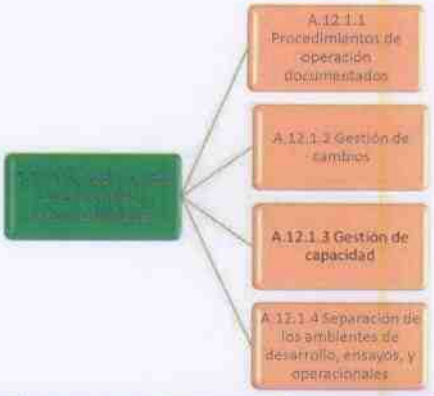
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.



BDO RESTREPO RAMAS www.ro-sas.com

A.12 SEGURIDAD EN LAS OPERACIONES

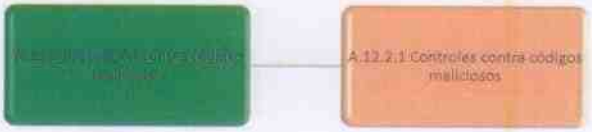
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.



BDO RESTREPO RAMAS www.ro-sas.com

A.12 SEGURIDAD EN LAS OPERACIONES

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.



A.12 SEGURIDAD EN LAS OPERACIONES

Objetivo: Proteger contra la pérdida de datos.

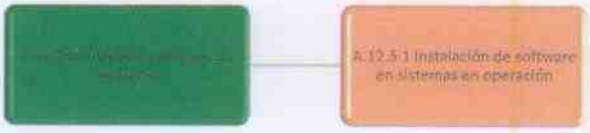
A.12 SEGURIDAD EN LAS OPERACIONES

Objetivo: Registrar eventos y generar evidencia.

BDO RESTREPO RAMAS... www.ro-sas.com

A.12 SEGURIDAD EN LAS OPERACIONES

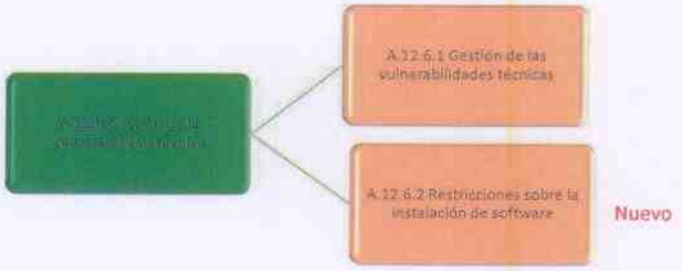
Objetivo: Asegurarse de la integridad de los sistemas operacionales.



BDO RESTREPO RAMAS... www.ro-sas.com

A.12 SEGURIDAD EN LAS OPERACIONES

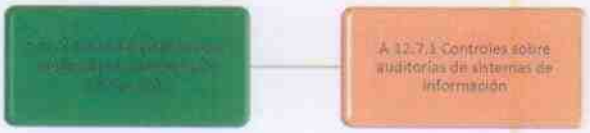
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.



Nuevo

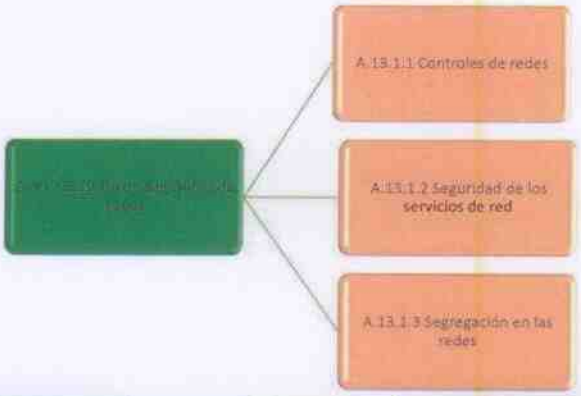
A.12 SEGURIDAD EN LAS OPERACIONES

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.



A.13 SEGURIDAD DE LAS COMUNICACIONES

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.



A.13 SEGURIDAD DE LAS COMUNICACIONES

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

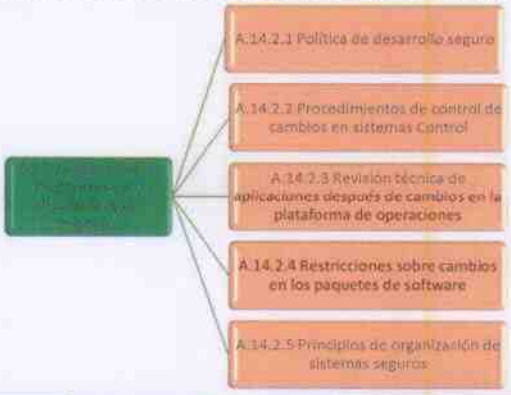
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: Garantizar* que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.



BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

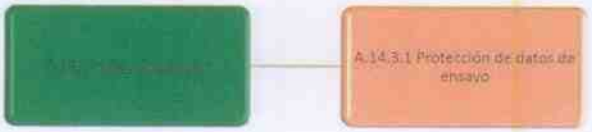
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivo: Asegurar la protección de los datos usados para ensayos.



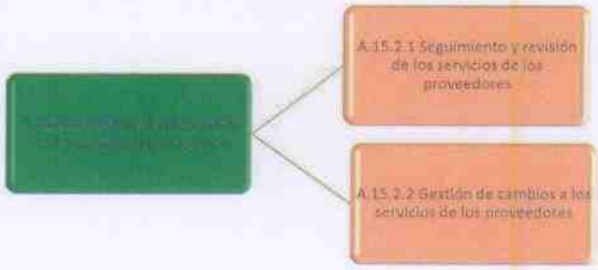
BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.15 RELACIÓN CON LOS PROVEEDORES

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

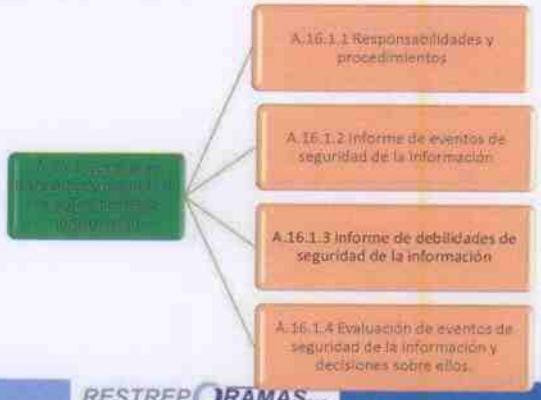
A.15 RELACIÓN CON LOS PROVEEDORES

Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.



A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

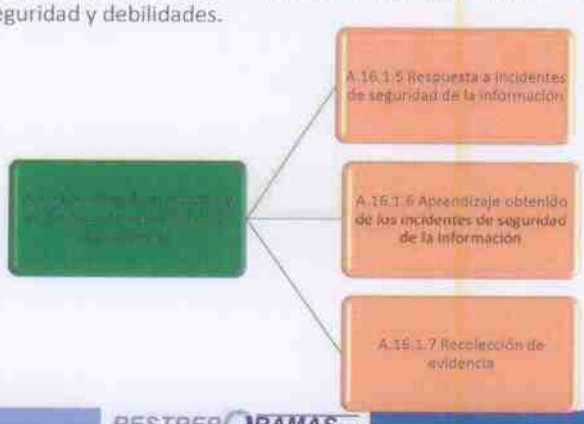
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.



BDO RESTREPO RAMAS... www.ro-sas.com

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.



BDO RESTREPO RAMAS... www.ro-sas.com

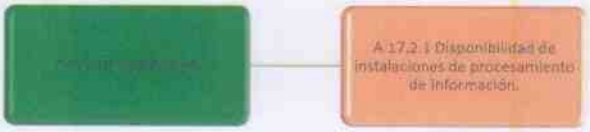
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN
EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

BDO RESTREPO RAMAS www.ro-sas.com

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN
EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.



BDO RESTREPO RAMAS www.ro-sas.com

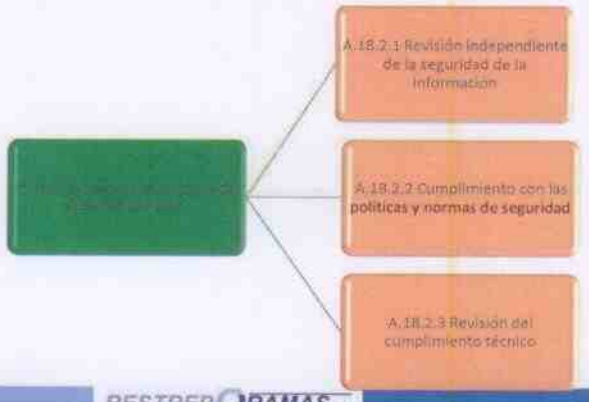
A.18 CUMPLIMIENTO

Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

A.18 CUMPLIMIENTO

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.



BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

Auditoria al Sistema de Gestión de Seguridad de la Información bajo la norma ISO 19011:2011

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Proporciona orientación sobre auditoria a los sistemas de gestión incluyendo Principios, gestión del programa, realización de auditorias; así como evaluación de la competencia de los participantes en el proceso de auditoria.

Capítulo 1: Objeto y campo de aplicación
Capítulo 2: Referencias normativas
Capítulo 3: Términos y definiciones
Capítulo 4: Principios de auditoria
Capítulo 5: Gestión de un programa de auditoria
Capítulo 6: Realización de una auditoria
Capítulo 7: Competencia y evaluación de los auditores

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

3: TÉRMINOS Y DEFINICIONES

Conclusiones de auditoria: Resultado de una auditoria que proporciona el equipo auditor, tras considerar los objetivos de la auditoria y todos los hallazgos.

Alcance de auditoria: Extensión y límites de una auditoria.

Plan de auditoria: Descripción de las actividades y los detalles acordados de una auditoria.

Competencia: Atributos personales y aptitud demostrada para aplicar conocimientos y habilidades.

CONTENIDO DE LA NORMA ISO 19011:2011

3. TÉRMINOS Y DEFINICIONES

Auditoria: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoria y evaluarlas de **manera objetiva** con el fin de determinar la extensión en que se cumplen los criterios de auditoria.

Criterios de auditoria: Conjunto de políticas, procedimientos o requisitos.

Evidencia de la auditoria: Registros, declaraciones de hechos, o cualquier otra información que son pertinentes para los criterios de auditoria y que son verificables

Hallazgos de auditoria: Resultado de la evaluación de la evidencia de auditoria recopilada, frente a los criterios de auditoria

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Soportan la realización de una auditoria eficaz y fiable permitiendo logra conclusiones de auditoria pertinentes y suficientes

"Alcanzar conclusiones similares en circunstancias similares"

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Integridad: Fundamento de la profesionalidad

- Honestidad diligencia y responsabilidad
- Cumplir requisitos legales
- Imparcialidad y ecuanimidad
- Alerta a influencias sobre su juicio profesional

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Presentación imparcial: Informar con veracidad y exactitud

Hallazgos, conclusiones e informes de auditoria
Informar **obstáculos significativos**
Diferencias de opinión
Comunicación exacta, clara, completa, oportuna

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Debido cuidado profesional: Aplicar diligencia y juicio al auditar
Confianza
Juicios razonados

Confidencialidad: Seguridad dela información

Buen uso y protección de la información del cliente

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Independencia: Imparcialidad de la auditoria y objetividad en conclusiones.

Independencia profesional
Conflicto de interés
Evidencias de Auditoria

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

4. PRINCIPIOS DE AUDITORIA

Enfoque basado en la evidencia: Método racional para alcanzar conclusiones de auditoria fiables y reproducibles en u proceso de auditoria sistemático.

Ser verificable
Muestreo sobre información disponible

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.1 Contribuye a determinar la eficacia del sistema de gestión del auditado incluyendo una o varias auditorias considerando una o más normas de sistemas de gestión.

- Alta Administración aprueba los objetivos del programa
- Asignación de recursos
- Definir un alcance con base en tamaño, naturaleza
- Grado de madurez del sistema de gestión
- Auditoria basada en riesgos

BDO RESTREPO RAMAS... www.ro-sas.com

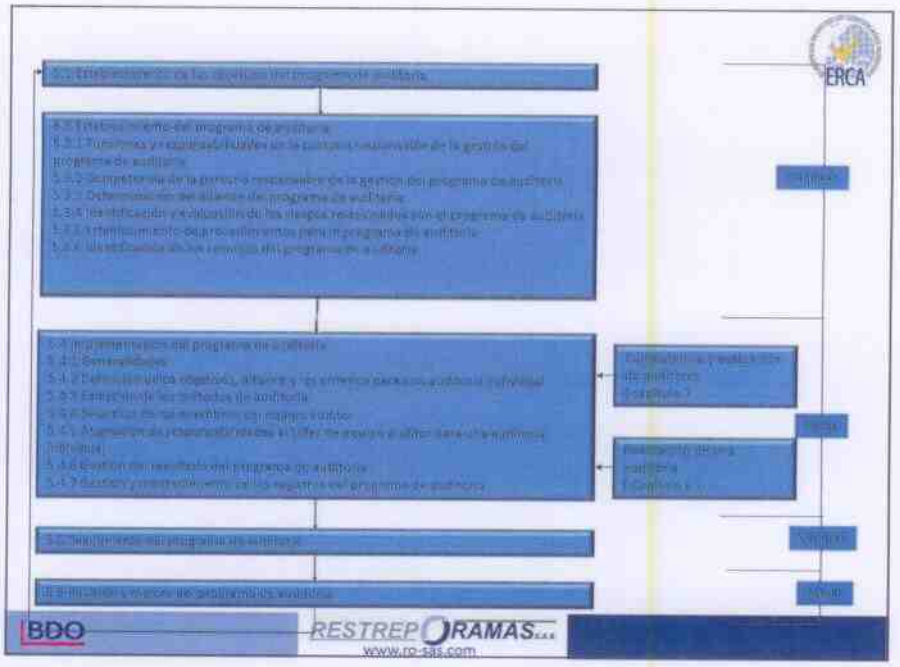
CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

Contenido del programa de auditoria

- Objetivo
- Alcance/ número/ tipo/ duración / ubicaciones
- Procedimientos, criterios, métodos
- Equipo auditor
- Recursos necesarios
- Protección de confidencialidad
- Revisión y seguimiento

BDO RESTREPO RAMAS... www.ro-sas.com



CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.2 Establecimiento de los objetivos del programa de auditoria

Prioridades de la Dirección
Características productos / servicios / Proyectos
Requisitos legales / contractuales
Evaluación de proveedores
Nivel de madurez del sistema auditado
Nivel de desempeño del auditado

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.3 Establecimiento del programa de auditoria

El responsable del programa debería

- Establecer el alcance
- Identificar y evaluar riesgos
- Establecer responsabilidades
- Determinar recursos
- Gestionar y mantener los registros de auditoria

El responsable del programa debería contar con la competencia para gestionar el programa y sus riesgos; además de demostrar conocimiento en principios, procedimientos, métodos de auditoria.

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.3.3 Determinación del alcance del programa de auditoria

- Determinado por el responsable del programa
- Depende del tamaño y naturaleza del auditado
- Complejidad funcionalidad y madurez del sistema de gestión.
- Incluye objetivo, alcance, duración de cada auditoria
- Seguimientos de auditorias anteriores
- Cambios significativos del auditado

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.3.4 Identificación y evaluación de riesgos relacionados con el programa de auditoria

Eventos que afecten logro de los objetivos

A nivel de

- Planificación
- Asignación de recursos
- Selección equipo auditor
- Comunicación ineficaz
- Registros y sus controles

BDO RESTREPORAMAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.3.6 Identificación de recursos del programa de auditoria

- Financieros
- Métodos de auditoria
- Auditores y experto técnicos
- Transporte, alojamiento
- Tecnologías de información

BDO RESTREPORAMAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.4 Implementación del programa de auditoria

Definición de objetivos, alcance y criterios
Selección de métodos de auditoria
Selección del equipo auditor
Asignación de responsabilidad al líder del equipo auditor
Gestión del resultado del programa de auditoria
Gestión y mantenimiento de los registros del programa de auditoria

BDO RESTREPOGRAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.5 Seguimiento del programa de auditoria

Evaluar conformidad objetivos, calendarios
Desempeño equipo auditor
Retroalimentación partes interesadas
Cambios en el programa de auditoria

BDO RESTREPOGRAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

5. GESTIÓN DE UN PROGRAMA DE AUDITORIA

5.6 Revisión y mejora del programa de auditoria

Lecciones aprendidas
Mejora continua
Informar los resultados de la revisión
Efectividad tratamiento riesgos del programa

BDO RESTREPO RAMAS... www.ro-sas.com

6.2 Inicio de la auditoría
6.2.1 Generalidades
6.2.2 Establecimiento contacto inicial con el auditado
6.2.3 Determinación de la viabilidad dela auditoria

6.3 Preparación de las actividades de la auditoria
6.3.1 Revisión dela documentación
6.3.2 Preparación del plan de auditoria
6.3.3 Asignación de tareas al equipo auditor
6.3.4 Preparación de papeles de trabajo

6.4 Realización de las actividades de la auditoría
6.4.1. Generalidades
6.4.2 Reunión de apertura
6.4.3 Revisión de documentación durante auditoria
6.4.4 Comunicación durante auditoria
6.4.5 Asignación de funciones a guías y observadores
6.4.6 Recopilación y verificación de información
6.4.7 Generación de hallazgos
6.4.8 Preparación de conclusiones
6.4.9 Realizar reunión de cierre

6.5 Preparación y distribución del informe de auditoría
6.5.1 Preparación del informe de auditoria
6.5.2 Distribución del informe

6.6 Finalización de la auditoria

6.7 Realización de actividades de seguimiento de una auditoría
Si se especifica en el Plan de auditoria

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.2 INICIO DE LA AUDITORIA

6.2.2 Establecimiento contacto inicial con el auditado

Contacto con representantes del auditado
Informa objetivos, alcance, métodos y equipo auditor
Acceso a documentos y registros
Confidencialidad
Acceso, seguridad y salud
Escuchar al auditado

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.2 INICIO DE LA AUDITORIA

6.2.3 Determinación de la viabilidad de la auditoria

Información suficiente y apropiada
Cooperación adecuada
Tiempo y recursos adecuados
Buscar alternativas para dar viabilidad.

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.3 PREPARACIÓN DE LAS ACTIVIDAES DE L A AUDITORIA

6.3.1 Revisión de la documentación

Acorde al tamaño y naturaleza de la organización
Coherente con el objetivo y alcance de auditoria
Reunir información para preparar actividades
Diseño de papeles de trabajo
Detección de posibles debilidades

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.3 PREPARACIÓN DE LAS ACTIVIDAES DE L A AUDITORIA

6.3.1 Preparación del Plan de Auditoria

Programa de auditoria y documentación del auditado
Considerar efecto en procesos del auditado
Acuerdo entre cliente auditor y auditado
Estimación del tiempo de acuerdo a las actividades

Tener en cuenta

Técnicas de muestreo apropiadas
Competencia equipo auditoria
Riesgos para la organización

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.3 PREPARACIÓN DE LAS ACTIVIDAES DE L A AUDITORIA

6.3.1 Preparación del Plan de Auditoria

El Plan de Auditoria debería incluir:

- Objetivo de la auditoria
- Alcance (Procesos, ubicación, procesos)
- Criterios de auditoria
- Fechas, horarios y duración
- Métodos de muestreo a utilizar
- Funciones y responsabilidades equipo auditor
- Asignación de recursos apropiados

El Plan de auditoria debería ser revisado y aprobado por el cliente y conocido por el auditado.

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.3 PREPARACIÓN DE LAS ACTIVIDAES DE L A AUDITORIA

6.3.3 Asignación de tareas al equipo auditor

- Asignado por el Líder del equipo auditor
- Procesos, actividades, funciones o lugares
- Tener en cuenta independencia y competencia
- Posibilidad de realizar cambios en programación

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.3 PREPARACIÓN DE LAS ACTIVIDADES DE L A AUDITORIA

6.3.4 Preparación de los papeles de trabajo

Listas de verificación
Planes de muestreo de auditoria
Formularios para registrar información
Custodia y retención de papeles de trabajo
Protección información confidencial

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.2 Reunión de apertura

Confirmar el acuerdo entre las partes sobre el Plan auditoria
Presentar al equipo auditor
Asegurar que se puede realizar la auditoria planificada
Responder preguntas de los asistentes
Posible registro de asistencia
Líder del equipo de auditoria preside
Canales de comunicación formal

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.3 Revisión de la documentación

Determinar la conformidad del sistema
Reunir información como apoyo a la auditoria
Puede continuar a lo largo de la auditoria
Entrega de documentos dentro del tiempo establecido

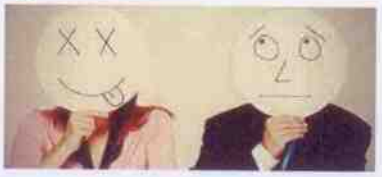
BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.4 Comunicación durante la auditoria

Dentro del equipo de auditoria y con el auditado
Reuniones internas del equipo de auditoria
Comunicación periódica con el cliente y auditado
Comunicar sin demora riesgos significativos
Comunicación organismos externos



BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.5 Asignación de responsabilidad a los guías y observadores

- Acompañantes del equipo auditor
- No deberían interferir ni influir en la auditoria
- Guías son designados por el auditado
  - El guía puede actuar como testigo
  - El guía puede proporcionar aclaraciones

BDO RESTREPO RAMAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

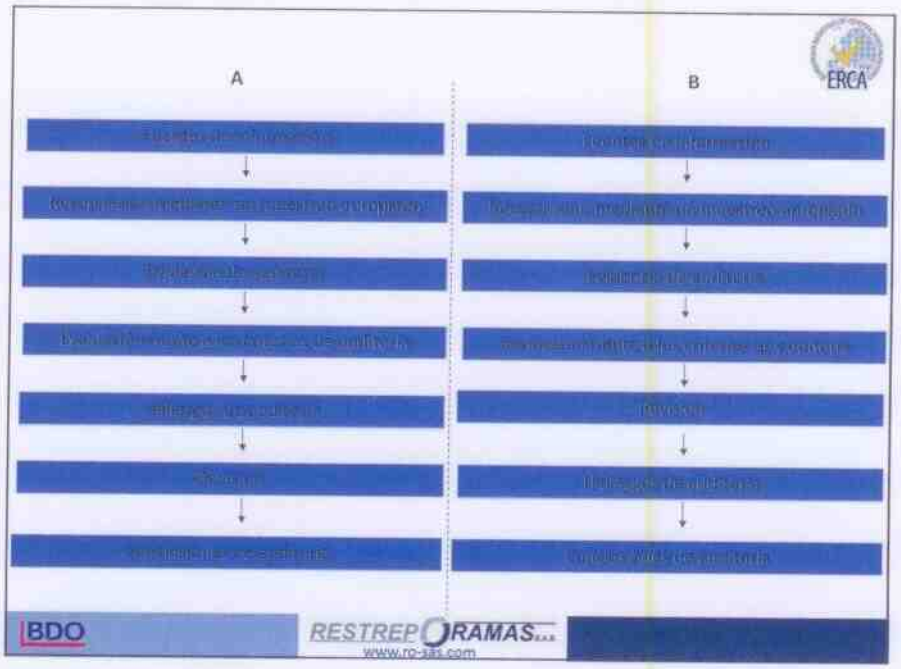
6.4.6 Recopilación y verificación de información

Recopilar información mediante un muestreo apropiado y verificarse la información pertinente a los objetivos, alcance y criterios de la misma.

Solo información que es verificable debería aceptarse como evidencia

Debería registrarse la evidencia que origina hallazgos de auditoria

BDO RESTREPO RAMAS www.ro-sas.com


A
B
ERCA
BDO
RESTREPO RAMAS S.A.S.
www.ro-sas.com


CONTENIDO DE LA NORMA ISO 19011:2011
ERCA
BDO
RESTREPO RAMAS S.A.S.
www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Los métodos para recopilar información incluyen

- *Entrevistas*
- *Observaciones*
- *Revisión de documentos incluyendo registros*

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.6 Recopilación y verificación de información

Entrevistas con empleados y otras personas
Observación de actividades y condiciones circundantes
Revisión documental (política, manuales, procedimientos, normas)
Registros (actas, informes auditoria, desempeño de indicadores)
Bases de datos de conocimiento (sector, Internet)

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.7 Generación de hallazgos de auditoria

La evidencia frente a los criterios de auditoria
Solo información verificable constituye evidencia
Conformidad o No conformidad
Si es acordado se generan recomendaciones
No conformidades soportadas por evidencias
Revisar No conformidades con el auditado
Manejo de opiniones divergentes

BDO RESTREPO RAMAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.8 Preparación de las conclusiones de auditoria

Reunión del equipo auditor
Revisión de hallazgos e información pertinente
Acordar conclusiones (incertidumbre)
Preparar recomendaciones
Seguimiento a la auditoria

CONCLUSION

BDO RESTREPO RAMAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.8 Preparación de las conclusiones de auditoria

Las conclusiones deberían tratar aspectos como:

- Grado de conformidad
- Fortalezas del sistema
- Proceso de revisión por la Dirección
- Cumplimiento de los objetivos de auditoria
- Causa raíz de los hallazgos (si aplica)
- Hallazgos similares en distintas áreas (tendencias)

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.4 REALIZACIÓN DE LAS ACTIVIDADES DE AUDITORIA

6.4.9 Reunión de cierre

- Presentar hallazgos y conclusiones
- Prevenir al auditado de situaciones encontradas
- Acordar planes de acción (si aplica)
- Aclarar que conclusiones se basan sobre muestreo
- Proceso de tratamiento de hallazgos y posibles consecuencias
- Actividades posteriores a la auditoria (quejas, apelación)
- Manejo de opiniones divergentes

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.5 PREPARACIÓN Y DISTRIBUCIÓN DEL INFORME

6.5.1 Preparación del informe de auditoria

Elaborado por el Líder del equipo de auditoria
Registro completo, preciso, claro conciso
Incluir objetivo, alcance, criterio de auditoria
Conclusiones
Declaración del grado de conformidad
Opiniones divergentes sin resolver
Buenas prácticas identificadas

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.5 PREPARACIÓN Y DISTRIBUCIÓN DEL INFORME

6.5.2 Distribución del informe

Entregarse dentro del tiempo acordado
Estar fechado, revisado y aprobado
Distribuirse a los receptores autorizados

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Finaliza cuando se realicen todas las actividades de auditoria
Conservación o destrucción de documentos
La información es del cliente (pedir autorización)
Informar al cliente de una revelación de su información
Recopilar lecciones aprendidas

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.6 FINALIZAR LA AUDITORIA

Terminación de todas las actividades del Plan de auditoria
Informe de auditoria aprobado fue distribuido
Conservación de documentos (destrucción de común acuerdo)
Acuerdo de no revelación del contenido de los documentos
Para divulgación debe haber aprobación del cliente / auditado

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

6.7 REALIZAR ACTIVIDADES DE SEGUIMIENTO

Correcciones, acciones correctivas o de mejora
Acordar tiempos
Auditado informa sobre avance
Auditor verifica finalización de acciones
Auditor verifica efectividad de acciones

BDO RESTREPO RAMAS SAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Clasificación de las No Conformidades

Menor: Falta simple contra los requisitos, se resuelve en corto tiempo
Mayor: Falta de impacto contra un requisito, toma tiempo resolverla
Crítica: da como resultado que la auditoria se interrumpa temporalmente
Observación: Posible futura no conformidad, condición que amerita una mejora en el sistema.

BDO RESTREPO RAMAS SAS www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Fiabilidad y confianza en el proceso de auditoria
Cualidades personales / Aptitud para aplicar conocimiento
Educación, experiencia laboral, formación como auditor, experiencia en auditorias.
Habilidades generales y particulares
Continuo desarrollo profesional y práctica en auditoria
Proceso evaluación de los auditores

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Atributos personales

Actuar de acuerdo con los principios de auditoria
Ético, imparcial, sincero, honesto y discreto
Mentalidad abierta, diplomático y observador
Decidido y seguro de si mismo
Tenaz, persistente orientado al logro de objetivos

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Conocimientos y habilidades

- Principios, procedimientos y técnicas de auditoria
- Planificador y organizador
- Establecer prioridades y centrarse en lo importante
- Recolección, análisis y reporte de información
- Uso apropiado de técnicas de muestreo
- Verificar exactitud de información
- Preparar informes de auditoria
- Comunicación efectiva, habilidades lingüísticas
- Mantener la confidencialidad y seguridad en la información

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Conocimientos y habilidades

- Conocimiento del sistema de gestión y de referencia
- Aplicación de documentos de referencia a diferentes situaciones
- Sistemas de distribución, control de datos y registros
- Entender el contexto de las operaciones de la organización.
- Costumbres sociales y culturales
- Leyes, reglamentos aplicables a la disciplina

Cultura

BDO RESTREPO RAMAS S.A.S. www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Conocimientos y habilidades líderes de equipo

- Planificar y **usar eficazmente los recursos**
- Comunicación efectiva con el cliente y su equipo
- Organizar y **dirigir a su equipo**
- Formar a su equipo
- Conducir al equipo para **llegar a las conclusiones**
- Prevenir y **resolver conflictos**
- Preparar, completar y presentar el informe de auditoria

BDO RESTREPO RAMAS... www.ro-sas.com

CONTENIDO DE LA NORMA ISO 19011:2011

Capítulo 7: Competencia y evaluación de los auditores

Evaluación del auditor

- Actividad planificada, implementada y con registros
- **Resultado objetivo, coherente, justo y fiable**
- Selección / Constitución de equipo / desempeño
- Identificación de necesidades del programa de auditoria
- **Establecer los criterios de evaluación**
- Seleccionar el método de evaluación adecuado
  - Revisión de registros
  - Entrevista
  - Observación
  - Examen
  - Revisión después de auditoria

BDO RESTREPO RAMAS... www.ro-sas.com