Centro de Especializaciones Noeder

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR ISO 27001 E ISO 22301

CICLO INTENSIVO

MÓDULO IV

IMPLEMENTACIÓN DE LA NORMA ISO 22301 – 2019

Ing. Johnattan Sifuentes Rojas

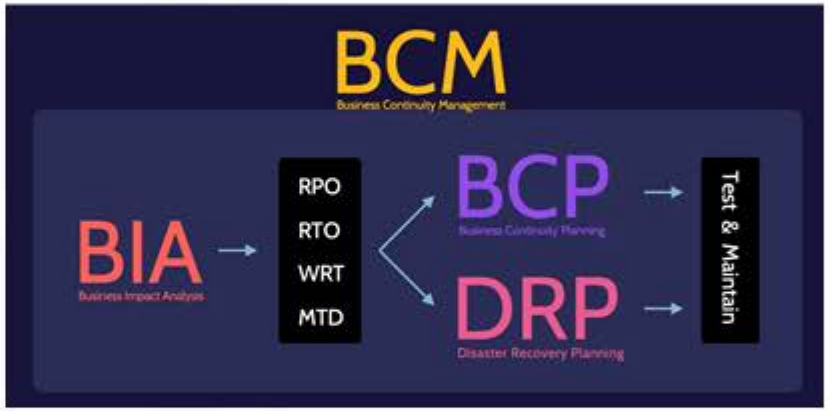
MODULO IV – IMPLEMENTACIÓN DE LA NORMA ISO 22301 - 2019

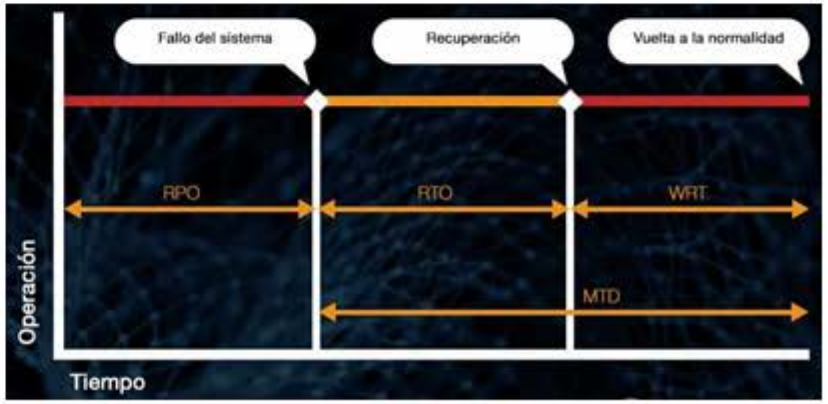
CONTENIDO MODULO IV

1. Gestión del contexto organizacional
2. Liderazgo y compromiso en el SGCN
3. Planificación del SGCN
4. Gestión de objetivos y planificación de cambios
5. Gestión de recursos
6. Gestión de la comunicación y documentación
7. Gestión de operaciones
8. Gestión del riesgo operacional
9. Evaluación de desempeño
10. Mejora continua

ALCANDE DEL SGCN

ISO 22301
Sistema de Gestión de Continuidad del Negocio - SGCN





GESTION DEL CONTEXTO DE LA ORGANIZACION

Contexto de la organización

Análisis Interno y externo

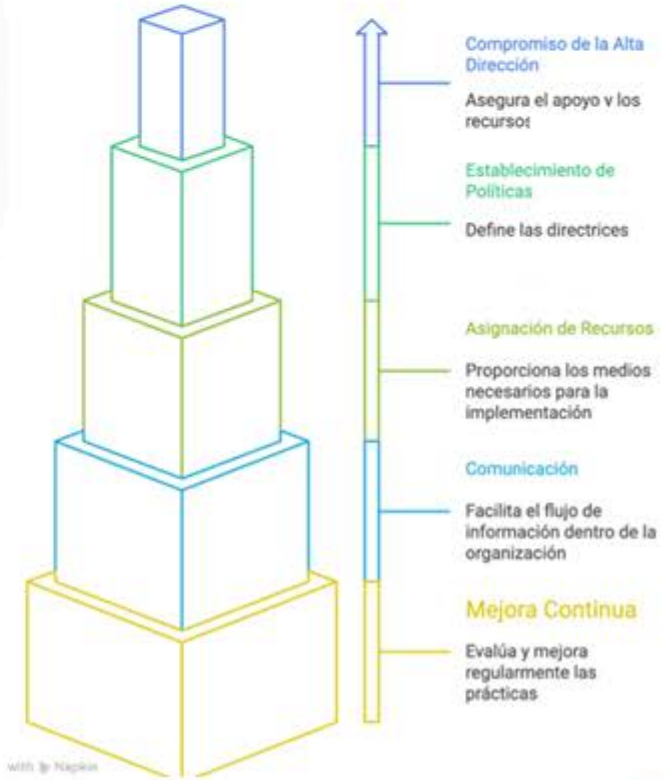
Partes Interesadas

Necesidades y expectativas

LIDERAZGO Y COMPROMISO

LIDERAZGO

- Liderazgo y compromiso
- Política SGCN
- Roles, responsabilidades y autoridades en la organización



PLANIFICACION

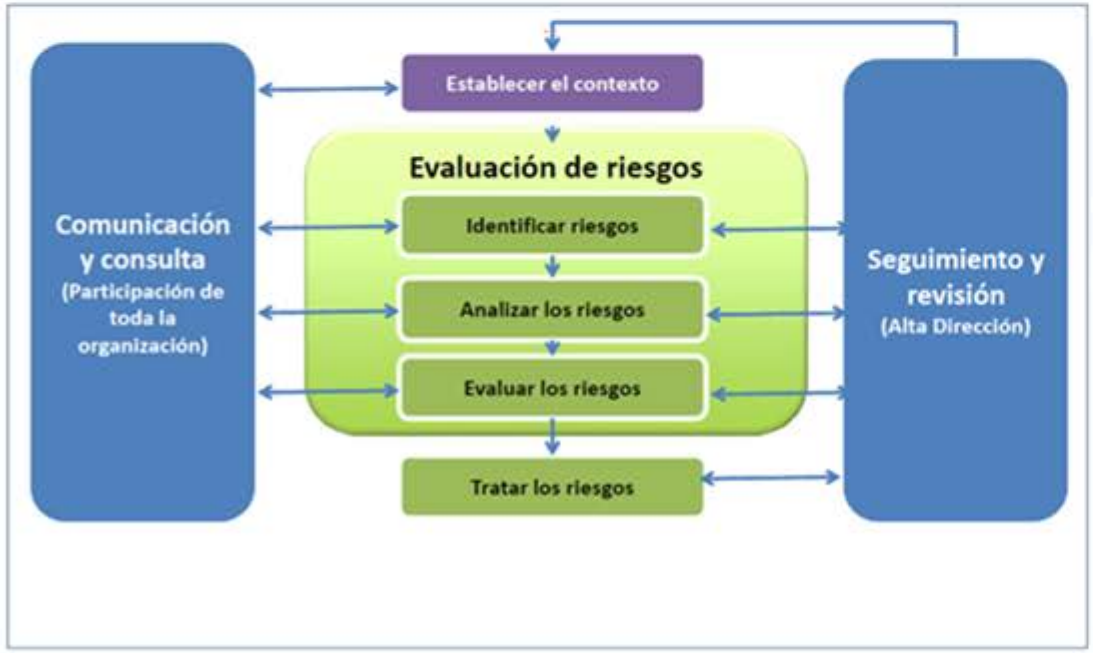
Planificación

Acciones para abordar riesgos y oportunidades

Determinación de riesgos y oportunidades

Abordar riesgos y oportunidades

Proceso de gestión del Riesgo según ISO 31000:2009



GESTIÓN DE OBJETIVOS Y PLANIFICACIÓN DE CAMBIOS

Planificación

Establecimiento y Determinación de los objetivos de continuidad del negocio

Los Objetivos y los Planes para Alcanzarlos

ISO 22301, Cláusula 6.2.1: Establecer los objetivos de la Continuidad de Negocio

- La organización debe establecer objetivos de continuidad del negocio en funciones y niveles relevantes.
- Los objetivos de Continuidad de Negocio deben:
  a) Ser coherentes con la política de continuidad del negocio.
  b) ser medibles (si es posible).
  c) Tomar en cuenta los requisitos aplicables (véase subcapitulos 4.1 y 4.2).
  d) Ser sujetos de seguimiento
  e) Ser comunicados.
  f) Estar actualizados según corresponda.
  - La organización debe retener información documentada sobre los objetivos de continuidad del negocio.

Planificando los cambios en el SGCN

Consideraciones de cambios en el SGCN

ISO 22301, Cláusula 6.3

- Cuando la organización determina la necesidad de cambios en el SGCN, incluidos los identificados en la cláusula 10, los cambios se llevarán a cabo de manera planificada.
- La organización deberá considerar:
  a) El propósito de los cambios y sus posibles consecuencias.
  b) La integridad del BCMS.
  c) La disponibilidad de recursos.
  d) La asignación o reasignación de responsabilidades y autoridades.

Ejemplo

Una organización evidencia su cumplimiento con la presentación del análisis de cierre de brechas que puede existir en el SGCN y el cumplimiento de los objetivos.

GESTION DE RECURSOS

Soporte

- Recursos
- Competencia
- Toma de Conciencia
- Comunicación
- Información Documentada

Capacitación	Concienciación	Comunicación
Adquisición de habilidades	Cambios de hábitos	Estar informado
Dirigido al intelecto	Dirigida principalmente a las emociones y el comportamiento	Dirigida al intelecto
¿Qué habilidades tiene que adquirir?	¿Qué comportamiento queremos reforzar o cambiar?	¿Qué mensajes enviamos?

GESTION DE OPERACIONES

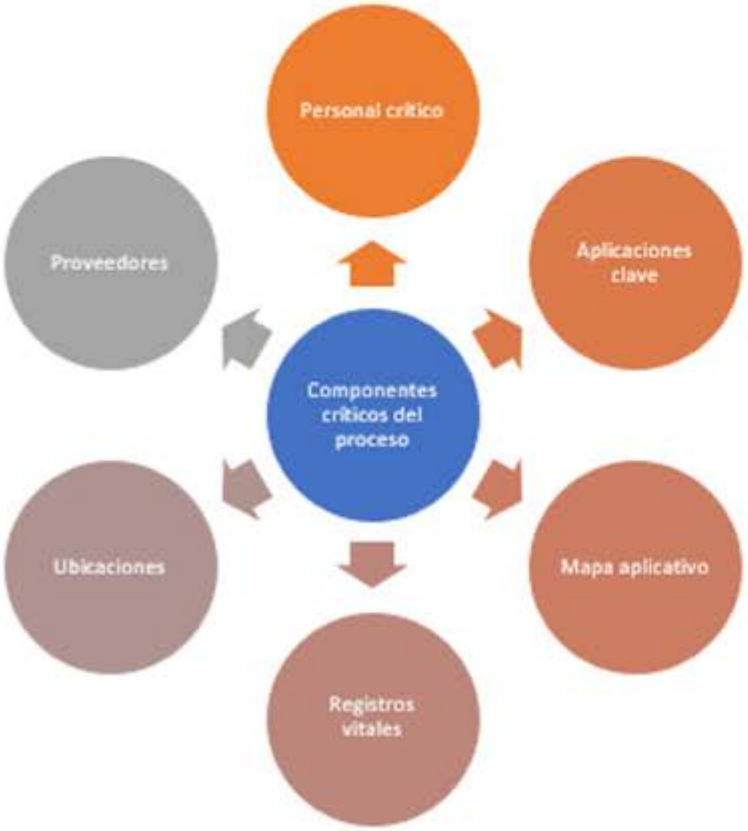
Operación

Planificación y control operacional

GESTION DE OPERACIONES

Operación

Análisis de Impacto en el negocio (AIN) y evaluación de riesgos



TIPOS DE IMPACTOS Y CRITERIOS RELEVANTES

Nivel de Impacto	Impacto Monetario	Efecto en la imagen	Impacto normativo	Impacto operacional	Masividad
1 Insignificante	0 a 1.000.000	No afecta la imagen de la compañía.	No afecta la reputación del Banco.	No afecta la operación de la organización	<100 transacciones mensuales
2 Menor	1.000.000 a 10.000.000	La situación afecta a un grupo reducido de clientes sin trascender de ellos.	La situación no provoca impacto normativo de ningún tipo.	Interrumpe la operación de un proceso de control para la gestión interna de la organización.	Entre 100 y 500 transacciones **mensuales**
3 Moderado	10.000.000 a 100.000.000	La situación trasciende y se divulga en medios de comunicación no masivos.	La situación puede provocar sanciones u observaciones de auditoría de los organismos reguladores.	Interrumpe la operación de un proceso interno de la organización (ejemplo: Pago de sueldos)	100 transacciones **diarias**
4 Mayor	100.000.000 a 1.000.000.000	La situación trasciende a medios específicos de denuncia y se divulga en redes sociales.	La situación puede provocar multas de los organismos reguladores pero que no traen consecuencias a nivel de restricciones en la	Interrumpe la operación de un proceso crítico ya identenficado, el cual tiene un alto impacto en el cliente.	1000 transacciones **diarias**
5 Catastrófico	mas de 1.000.000.000	La situación trasciende y se divulga en medios de comunicación masivos y redes sociales.	La situación casi con seguridad obligaría al pronunciamiento público de los organismos reguladores, otras entidades del mercado o stakeholders de la industria. Podría traer como consecuencia restricciones en la	Impacta directamente el tiempo de respuesta comprometido con el cliente para entregarle un producto o servicio.	> 1000 transacciones **diarias**

GESTION DE OPERACIONES

Operación

Estrategias y soluciones de continuidad del negocio

RPO
Determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación

RTO
Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

MTDP
Define el tiempo máximo tolerable de la indisponibilidad debido a una interrupción (por lo general desde la perspectiva del negocio o del equipo estratégico). Esto es en el caso que un servicio o producto no se pueda reanudar.

GESTION DE OPERACIONES

Operación

Planes y procedimientos de continuidad del negocio

Programas de ejercicios

01
Planificación del ejercicio

Definir plan de trabajo detallado que permita tener un hilo conductor del ejercicio, y que contenga los lineamientos organizacionales.

02
Establecer objetivos

Definir las razones por las cuales se está ejecutando el ejercicio, permitiendo establecer objetivos y alcance.

03
Planificación del ejercicio

Definir el escenario del ejercicio, los inyectores y la narrativa teniendo en cuenta los objetivos y alcance, identificar indicadores asociados a los objetivos, equipos de trabajo y roles.

04
Preparación ejercicio

Establecer riesgos y planes para controlarlos, medios a utilizar durante el ejercicio, documentación, capacitación de personal y logística.

05
Conducir ejercicio

Presentar alcance, objetivos, equipos, escenario, inyectores, minutograma, ejecutar actividades e identificar lecciones aprendidas.

06
Contrastar objetivos

Verificar indicadores, determinar el logro de los objetivos, analizar oportunidades de mejora del proceso de planificación y ejecución del ejercicio.

GESTIÓN DE LOS RIESGOS OPERACIONALES

EVALUAR EL DESEMPEÑO

Monitoreo

Determinar el estado de un sistema, un proceso o actividad

Medida

Proceso para determinar un valor

Evaluación del Rendimiento

Proceso de determinar resultados mensurables

Monitoreo

1. El monitoreo en que se cumplen la continuidad del negocio, política, objetivos y metas de la organización.

2. Los procesos, procedimientos y funciones que protegen sus actividades prioritarias.

3. El cumplimiento de las exigencias legales y normativas, las mejores prácticas del sector y de la conformidad con su propia gestión de la política y objetivos de la continuidad del negocio.

4. Evidencia histórica de los resultados deficientes del SGCN, por ejemplo, no conformidad, conatos, falsas alarmas, fracasos, incidentes.

5. Los datos y los resultados del monitoreo y medición suficientes para facilitar el posterior análisis de las acciones correctivas y preventivas.

Evaluación del Rendimiento

Incidentes	Capacitación	Ejercicios	No Conformidad
▪ % de falsas alarmas con detección de eventos ▪ Costo promedio de un incidente	▪ % del personal que ha recibido capacitación y calificación de CN ▪ Número de horas de capacitación de los empleados	▪ % de planes probados ▪ Número de ejercicios realizados en el último año	▪ % de no conformidades no cerradas en la demora fijada ▪ Número de días en promedio para cerrar una no conformidad

MEJORA CONTINUA

Mantenimiento y Mejora del SGCN

- El **SGCN** debe ser mantenido y actualizado periódicamente.
- Las mejoras acordadas en el proceso y las acciones necesarias para mejorar el procesos deberian ser notificadas a los directores más apropiados para asegurar que ningún riesgo o elemento de riesgo es pasado por alto ni subestimado antes de la aplicación de los cambios.

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón

CENTRO DE ESPECIALIZACIONES NOEDER | R.U.C. 20604924236 | Todos los derechos reservados © 2025