Centro de Especializaciones Noeder

Florida Global University

Diplomado de Especialización

IMPLEMENTADOR Y AUDITOR INTERNO DE CONTINUIDAD DEL NEGOCIO ISO 22301

CICLO REGULAR

MÓDULO VI

CLASE 03

FORMACIÓN DE AUDITOR INTERNO EN CONTINUIDAD DEL NEGOCIO – ISO 22301

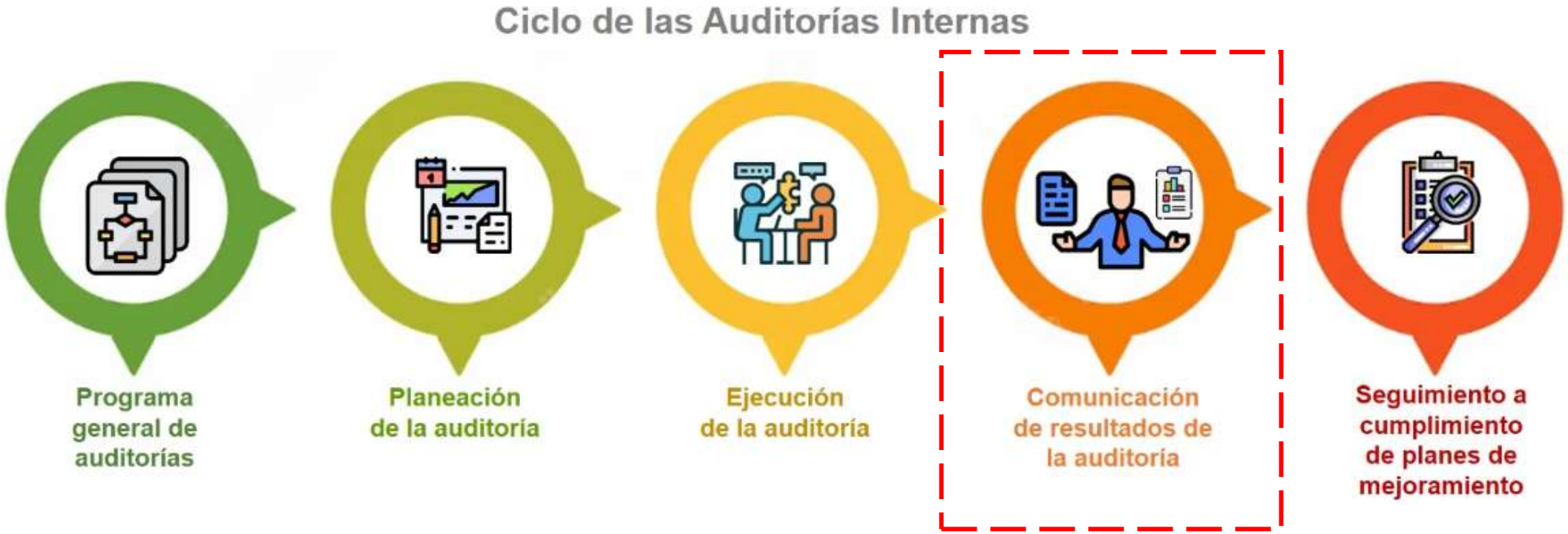
Ing. Johnattan Sifuentes Rojas

MODULO VI – FORMACIÓN DE AUDITORES INTERNOS ISO 22301

CONTENIDO MODULO VI – SESION 03

1. Comunicación de los resultados de auditoria
2. Seguimiento a cumplimiento de planes de mejoramiento

COMUNICACION DE RESULTADOS DE LA AUDITORIA



COMUNICACION DE RESULTADOS DE LA AUDITORIA

CARACTERISICAS

- ✓ Conciso y sin “Novedades / sorpresas”
- ✓ Distribuido a la Gerencia / Coordinación y Representante de la Dirección.

CONTENIDO DEL INFORME

- ✓ Alcance y objetivo
- ✓ Itinerario
- ✓ Documentación de referencia
- ✓ Referencia a las listas de verificación
- ✓ Integrantes del equipo auditor
- ✓ Personal Contactado
- ✓ Resumen de hallazgos
- ✓ Descripción de No conformidades

LO QUE NO DEBE INCLUIR

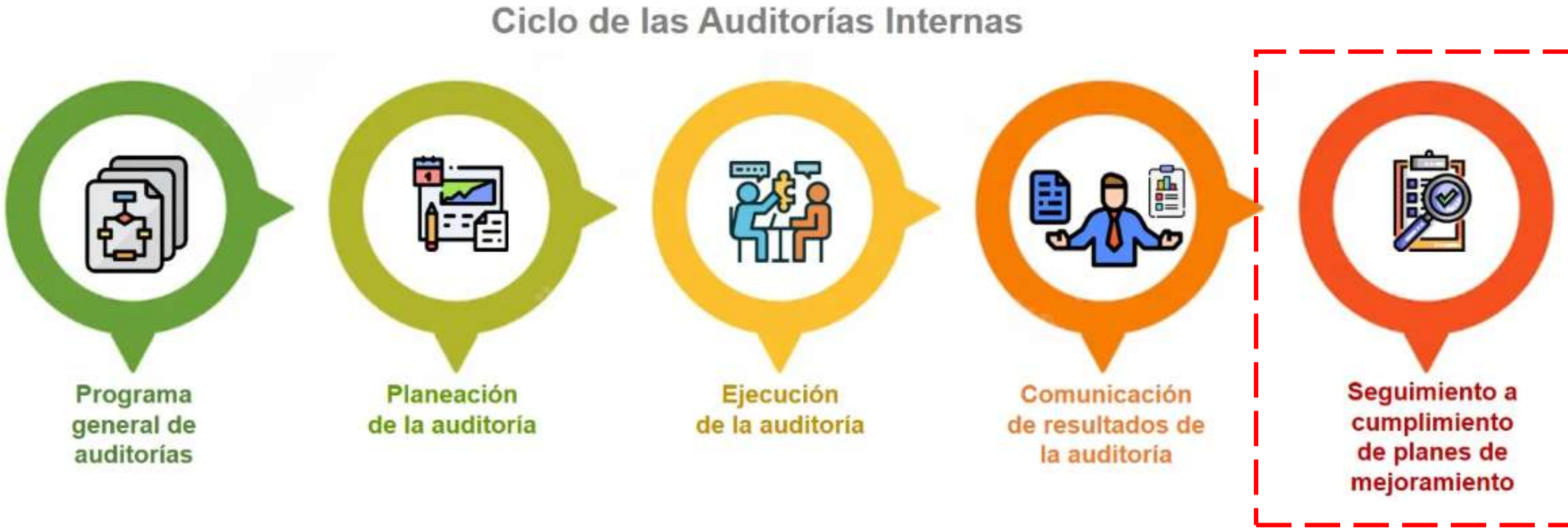
- ✓ Opiniones subjetivas, información confidencial, critica hacia las personas, declaraciones ambiguas, detalles triviales y hallazgos no mencionados en la reunión de cierre.

COMUNICACION DE RESULTADOS DE LA AUDITORIA

CUIDADOS EN LA REDACCIÓN

- ✓ Lenguaje claro, no retorico
- ✓ Emplear el titulo del párrafo de la Norma para presentar una No conformidad
- ✓ Emplear frases de la norma.
- ✓ No utilizar las palabras “Defecto” o “Deficiencia” sino “No Conformidad”
- ✓ No hablar en general: Informe detalladamente
- ✓ No proponer soluciones, es la empresa quien debe hacerlo (Auditoria de 2da y 3ra)
- ✓ No emplear frases “Me parece que…”, “En mi opinión…” que expresan ideas subjetivas

COMUNICACION DE RESULTADOS DE LA AUDITORIA



SEGUIMIENTO A CUMPLIMIENTO DE PLANES

LA GERENCIA RESPONSABLE DEL AREA AUDITADA DEBE:

- ✓ Investigar causas
- ✓ Determinar acciones correctivas
- ✓ Implementar las acciones correctivas

LA ACCION CORRECTIVA DEBE:

- ✓ Corregir el problema.
- ✓ Determinar magnitud del problema
- ✓ Prevenir la repetición de la NC
- ✓ Obtener respuesta del auditado
- ✓ Evaluar la acción correctiva propuesta
- ✓ Confirmar la implementación de la acción correctiva

CLASIFICACION Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

2. * Determinación de las competencias del auditor

1. Generalidades

Al decidir los conocimientos y habilidades apropiados requeridos al auditor, debería considerarse lo siguiente:

- el tamaño, naturaleza y complejidad de la organización que se va a auditar;
- las disciplinas del sistema de gestión que se va a auditar;
- los objetivos y amplitud del programa de auditoría;
- otros requisitos, tales como los impuestos por organismos externos, cuando sea apropiado;
- la función del proceso de auditoría en el sistema de gestión del auditado;
- la complejidad del sistema de gestión que se va a auditar;
- la incertidumbre en el logro de los objetivos de la auditoría.

Los tipos, niveles de riesgos, y oportunidades abordados por el sistema de gestión;
otros requisitos, tales como aquellos impuestos por entes externos, cuando sea apropiado;

CLASIFICACION Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

7.2.2 Comportamiento personal

Los auditores deberían poseer las cualidades necesarias que les permitan actuar de acuerdo con los principios de la auditoría. Los auditores deberían demostrar un comportamiento profesional durante el desempeño de las actividades de auditoría, incluyendo ser:

- Ético, es decir, imparcial, sincero, honesto y discreto;
- De mentalidad abierta, es decir, dispuesto a considerar ideas o puntos de vista alternativos;
- Diplomático, es decir, con tacto en las relaciones con las personas;
- Observador, es decir, activamente consciente del entorno físico y las actividades;
- Perceptivo, es decir, consciente y capaz de entender las situaciones;
- Versátil, es decir, capaz de adaptarse fácilmente a diferentes situaciones;
- Tenaz, es decir, persistente y orientado hacia el logro de los objetivos;

CLASIFICACION Y REGISTRO DE AUDITORES

COMPETENCIA Y EVALUACION DE AUDITORES

7.2.3.2 Conocimientos y habilidades genéricos de los auditores de sistemas de gestión

Los auditores deberían tener conocimientos y habilidades de las áreas señaladas a continuación.

a) Principios, procedimientos y métodos de auditoría

b) Sistema de gestión y documentos de referencia

c) Contexto de la organización

d) Requisitos legales y contractuales aplicables y otros requisitos que aplican al auditado

Entender los tipos de riesgo y oportunidades asociados a la auditoría, así como los principios del enfoque basado en el riesgo para la auditoría.

7.2.3.3 Debe contar también con conocimientos y habilidades especificas de la disciplina o sector que se va a auditar.

CLASIFICACION Y REGISTRO DE AUDITORES

Observaciones	Apdo. Norma 9001	Apdo. Norma 22301	Apdo. Norma 20000-1	Apdo. Norma 27001
Se observó debilidad en la determinación de los roles en el ámbito del SGCN: - Se han declarado 02 roles: Comité de crisis y Equipo de respuesta a incidentes, Falta el líder de continuidad, del gestor del SGCN. - No es clara la determinación de los roles en el antes – durante – después de un incidente disruptivo.	--	5.3	--	--
Se observaron discrepancias en la determinación de los RTO, RPO y MTDP en el BIA con el BCP.	--	8.2.2	--	--
Una vez valorado su último análisis de riesgos disruptivos, actualizado Se requiere ampliar/revisar el enfoque a riesgos/incidentes de desastre/disruptivos con afectación a la continuidad del negocio/servicio o actividades prioritarias, como: "La falla en los enlaces dedicados con sus clientes"	--	8.2.3 a)	--	--

CLASIFICACION Y REGISTRO DE AUDITORES

Observaciones	Apdo. Norma 9001	Apdo. Norma 22301	Apdo. Norma 20000-1	Apdo. Norma 27001
Con relación a las estrategias de continuidad del negocio, se observó la eficacia con el que se determinaron las estrategias que soportan a los escenarios declarados. No queda clara la determinación y selección de estrategias. Se requiere dar oportunidad de valorar diversas estrategias y documentar la selección.	--	8.3	--	--
Con relación a los ejercicios/ pruebas de recuperación: Para la recuperación del PRTG, se declaró en el informe la recuperación desde un Bk, pero no indican el punto de recuperación (la fecha/hora del respaldo) que garantice el cumplimiento del RPO.	--	8.5	--	--

CLASIFICACION Y REGISTRO DE AUDITORES

Observaciones	Apdo. Norma 9001	Apdo. Norma 22301	Apdo. Norma 20000-1	Apdo. Norma 27001
BIA Una vez valorado el análisis de impacto al negocio, INS-CNG-AIN-001 (BIA) se observó: - En el ítem de procesos críticos: no se logró sostener el impacto real en la línea del tiempo en concordancia con los criterios establecidos, por ejemplo, para el criterio "impacto Financiero" se declaró "nivel alto" cuando la perdida es mayor a 1000 usd, pero no se consideró en el tiempo. Por ejemplo MTPD para los 4 servicios indican 24 horas, no esta claramente relacionados los criterios. - De la misma forma, los tiempos de recuperación (RTO) no cuentan con sustento de los tiempos definidos.	--	--	8.2.2	--
Estrategias y soluciones En atención a la NC-04 declarado en revisión previa, se han declarado estrategias y establecido procedimiento. Sin embargo, están limitados a una parte o algún componente sobre el escenario declarado y no con un enfoque hacia acortar los tiempos de recuperación, protejan las actividades prioritarias, recudir los impactos. Ante la materialización de un incidente disruptivo. Por ejemplo: para el escenario de indisponibilidad de infraestructura TI, se declaró estrategia: "recuperar backup-PRTG". Por lo tanto, no fue posible sostener la elección y/o priorización de las soluciones/ estrategias que den respuesta al riesgo/incidente disruptivo con el objetivo de no afectar a los requisitos de continuidad.	--	--	8.3.2 /8.3.3	--

¡Gracias!

Centro de
Especializaciones
Noeder

Conéctate con nuestra comunidad