ESQUEMA DE CERTIFICACIÓN DE PERSONAS AUDITOR DE SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) ISO/IEC 27001:2022

EQ-DPE-007-2026
REVISIÓN 0
FECHA DE EMISIÓN: 16/09/2026

INSTITUTO DOMINICANO PARA LA CALIDAD (INDOCAL)
DIRECCIÓN EVALUACIÓN DE LA CONFORMIDAD

CONTENIDO

1. OBJETIVO

Establecer las competencias requeridas, y su correspondiente evaluación, para el esquema de certificación de personas para Auditor de Sistemas de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 del INDOCAL.

2. ALCANCE

Este esquema certifica a los auditores de Sistemas de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022, conforme a la norma ISO 19011:2026 "Directrices para la auditoría de los sistemas de gestión" en las siguientes categorías:

- Auditor ISO/IEC 27001:2022
- Auditor Líder ISO/IEC 27001:2022

3. DEFINICIONES

3.1. Alcance de la certificación: límites establecidos por el Esquema de Certificación para la emisión de las certificaciones, dentro de los cuales la persona certificada ha demostrado poseer un adecuado nivel de competencia técnica específica.

3.2. Candidato/a: solicitante que ha cumplido con los prerrequisitos especificados y ha sido admitido en el proceso de certificación.

3.3. Capacidades: habilidades o los talentos innatos. Dentro de las capacidades pueden estar incluidas la visión, la audición, la fuerza, la movilidad, entre otros.

3.4. Certificación: atestación de tercera parte relativa a un objeto de evaluación de la conformidad, con la excepción de la acreditación.

3.5. Certificado: documento emitido por un Organismo de Certificación, que indica que la persona mencionada ha cumplido los requisitos de certificación.

3.6. Competencia: capacidad para aplicar conocimientos y habilidades para lograr los resultados previstos.

3.7. Confiabilidad: indicador del grado de concordancia entre las calificaciones del examen correspondiente a diferentes momentos y lugares de examen, diferentes formas de examen y diferentes examinadores.

3.8. Esquema de certificación de personas: requisitos sobre competencia y otros, relacionados con categorías de ocupaciones específicas o habilidades de personas.

3.9. Evaluación: proceso mediante el cual se evalúa el cumplimiento de una persona con los requisitos del esquema de certificación.

3.10. Examen: mecanismo que es parte de la evaluación, que mide la competencia de un candidato por uno o varios medios tales como escritos, orales, prácticos y por observación, como se define en el esquema de certificación.

3.11. INDOCAL: El Instituto Dominicano para la Calidad es la Institución del Estado que implementará la aplicación de la Ley No. 166-12- Sistema Dominicano para la Calidad, como Instituto Nacional de Metrología (INM), así como los reglamentos relativos a los instrumentos de medida, a través del Departamento de Metrología Legal, y es la autoridad competente en el ámbito del control metrológico de los instrumentos de medida.

3.12. Inspección: evaluación de la conformidad por medio de observaciones y dictamen. Es acompañada, cuando sea apropiado, por mediciones, ensayos, pruebas o comparación con patrones, cuando se trate de metrología legal.

3.13. Otorgamiento: dictamen del Comité de Certificación autorizando la entrega del Certificado de Competencia Personal al (a los) candidato (s) que cumplieron con los requisitos y completaron satisfactoriamente el ciclo de evaluación establecido por el esquema de certificación correspondiente.

3.14. Parte interesada: individuo, grupo u organización afectada por el desempeño de una persona certificada o del INDOCAL.

3.15. Prerrequisitos: son las condiciones o los requerimientos de un esquema de certificación de personas, con los cuales el solicitante debe cumplir previo a ser certificado.

3.16. Propietario del esquema: organización responsable del desarrollo y mantenimiento de un esquema de certificación. Esta organización puede ser el INDOCAL, como organismo certificador, una autoridad oficial, ente regulador u otro con la competencia técnica aplicable.

3.17. Recertificación: evaluación realizada al finalizar la vigencia de la certificación establecida por el esquema de certificación.

3.18. Requisitos de certificación: conjunto de requisitos especificados, incluidos los requisitos del esquema, que se deben cumplir con el fin de obtener o mantener la certificación.

3.19. Solicitante: persona que ha presentado una solicitud para ser admitido en el proceso de certificación.

3.20. Supervisión/vigilancia: repetición sistemática de actividades de evaluación de la conformidad como base para mantener la validez de la declaración de conformidad.

Términos técnicos:

Serán aplicables las definiciones de los documentos citados en la sección de Referencias.

4. DESCRIPCIÓN DEL PROCESO

4.1. Descripción del trabajo y las tareas

Para optar por la certificación, los candidatos deberán evidenciar aptitud para realizar las siguientes actividades, atendiendo al alcance seleccionado:

Auditor ISO/IEC 27001:2022**:**

a) Aplicar los principios, procedimientos y técnicas de auditoría, basado en la norma ISO 19011:2026 "Directrices para la auditoría de los sistemas de gestión";
b) Apoyar la planificación y organización de la auditoría eficazmente;
c) Cumplir con el código de vestimenta establecido por la organización auditada;
d) Cumplir con las normas de seguridad establecidas por la organización auditada en el momento de la inducción;
e) Preparar los documentos de trabajo para la ejecución de la auditoría;
f) Dar cumplimiento al plan de auditoría y tiempos estipulados;
g) Recopilar información a través de entrevistas eficaces, escuchando, observando y revisando documentos, registros, datos y/o similares;
h) Verificar el cumplimiento de normas, requisitos legales y procedimientos y evaluar las desviaciones encontradas, según los criterios establecidos;
i) Evaluar la capacidad del Sistema de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 para asegurar el cumplimiento de los requisitos y para alcanzar los resultados previstos;
j) Identificar las áreas de mejora del sistema de gestión de la seguridad de la información;
k) Informar al auditor líder sobre cualquier situación durante el proceso de auditoría;
l) Redactar los hallazgos y aportar insumos para la elaboración del informe de auditoría.

Auditor Líder ISO/IEC 27001:2022**:**

a) Aplicar los principios, procedimientos y técnicas de auditoría, basado en la norma ISO 19011:2026 "Directrices para la auditoría de los sistemas de gestión";
b) Establecer los objetivos, el alcance y el programa de auditoría;
c) Dirigir la planificación y organización de la auditoría eficazmente;
d) Informar al auditado acerca del plan de auditoría;
e) Cumplir con el código de vestimenta establecido por la organización auditada;
f) Cumplir con las normas de seguridad establecidas por la organización auditada en el momento de la inducción;

g) Asegurar los recursos necesarios (infraestructura, humanos, competencia, tecnológicos, entre otros) para la realización de la auditoría;
h) Preparar los documentos de trabajo para la ejecución de la auditoría;
i) Asegurar el cumplimiento del plan de auditoría y tiempos estipulados;
j) Dirigir las reuniones de auditoría (apertura y cierre);
k) Recopilar información a través de entrevistas eficaces, escuchando, observando y revisando documentos, registros, datos y/o similares;
l) Verificar el cumplimiento de normas, requisitos legales y procedimientos y evaluar las desviaciones encontradas, según los criterios establecidos;
m) Liderar al equipo auditor;
n) Interceder entre el equipo auditor y el auditado ante la presencia de desacuerdos;
o) Evaluar la capacidad del Sistema de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 para asegurar el cumplimiento de los requisitos y para alcanzar los resultados previstos;
p) Identificar las áreas de mejora del sistema de gestión de la seguridad de la información;
q) Comunicar los hallazgos preliminares en la reunión de cierre de la auditoría;
r) Elaborar y distribuir el informe final de auditoría;
s) Verificar la eficacia de las acciones correctivas implementadas para tratar las no conformidades identificadas en auditorías previas
t) Identificar y comunicar los riesgos y oportunidades asociados al proceso de auditoría.

4.2. Competencias

4.2.1. Los conocimientos requeridos para garantizar el buen desempeño del Auditor de Sistemas de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 son:

a) Conocimiento de la Norma ISO 19011:2026 Directrices para la auditoría de los sistemas de gestión;
b) Conocimiento de la Norma ISO/IEC 27001:2022 sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) o su equivalente adoptado a nivel nacional;
c) Conocimiento de la Norma ISO 31000:2018 Gestión del riesgo — Directrices;
d) Conocimiento sobre métodos, herramientas de calidad y planificación;
e) Conocimientos de la Norma ISO/IEC 27005:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información;
f) Conocimientos de la Norma ISO/IEC 27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información.

4.2.2. Las Habilidades requeridas para garantizar el buen desempeño del Auditor de Sistemas de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 son:

- Pensamiento crítico;
- Capacidad de análisis;
- Manejo de conflictos;
- Comunicación efectiva;
- Liderazgo;
- Redacción de informes técnicos;
- Trabajo en equipo.
- Comprensión de terminología técnica básica en inglés, cuando aplique.

4.3. Prerrequisitos

Los siguientes prerrequisitos y capacidades deberán ser cumplidos por los postulantes al Esquema de Certificación para Auditor de Sistemas de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 del INDOCAL:

4.3.1. **Prerrequisitos:**

Auditor ISO/IEC **27001:2022:**

- Copia Cédula Identidad y Electoral o documento de identidad válido;
- Certificado de grado universitario o de nivel técnico superior;
- Certificado de capacitación en la Norma ISO 19011:2026;
- Certificado de capacitación en la Norma ISO/IEC 27001:2022 o su equivalente adoptado a nivel nacional;
- Certificación laboral de al menos un (1) año de experiencia en temas relacionados a la seguridad de la información; o constancia de experiencia de un mínimo de 24 horas en auditorías de sistemas de gestión de seguridad de la información bajo la supervisión de un auditor líder.

Auditor líder ISO/IEC **27001:2022:**

- Copia Cédula Identidad y Electoral o documento de identidad válido;
- Certificado de grado universitario;
- Certificado de capacitación en la Norma ISO 19011:2026
- Certificado de capacitación de auditor líder en la Norma ISO/IEC 27001:2022 o su equivalente adoptado a nivel nacional;
- Certificación laboral: de al menos tres (3) años de experiencia en temas relacionados a la seguridad de la información;
- Certificación de experiencia en auditorías: debe haber completado con éxito un mínimo de 48 horas como auditor líder de sistemas de gestión de seguridad de la información

4.4. Código de conducta

El código de conducta es una declaración del comportamiento esperado de la persona certificada; para estos fines el INDOCAL ha definido el Código de ***Conducta para la Certificación de Personas*** (OD-DPE-001). El/La solicitante deberá suscribirse a este código para poder optar por la certificación en sus dos alcances.

4.5. Criterios y métodos para la certificación inicial y la recertificación

4.5.1. **Criterios/Requisitos de la Certificación Inicial**

Para optar por la certificación de personas para Auditor Líder el solicitante deberá:

a) Completar el formulario Solicitud de Certificación de Personas (FO-DPE-002).
b) Suscribirse al Código de Conducta para la Certificación de Personas (OD-DPE-001).

c) Cumplir con los deberes desglosados en las Directrices y Lineamientos sobre el Servicio de Certificación de Personas del INDOCAL (OD-DEC-010).
d) Cumplir con los demás requisitos y criterios establecidos en el presente documento.
e) Cubrir los costos del proceso de certificación de personas de acuerdo con el tarifario vigente.

Los/as candidatos/as deberán pasar por una (1) evaluación constituida por un examen escrito. Condicionado por lo siguiente:

a) Para ser admitido/a como candidato/a, el/la solicitante deberá cumplir con todos los prerrequisitos y requisitos establecidos en el esquema.
b) El/La candidato/a deberá aprobar el examen escrito para pasar a la siguiente etapa.

Los/as candidatos/as que no aprueben el examen tendrán una (1) oportunidad para repetirlo y contarán con un período de un ciclo (6 meses), durante el cual la solicitud se mantiene "válida" (cargos extras aplican, ver "Resolución de costos de servicios", asociados al esquema).

Contado a partir de haber reprobado el último intento, el solicitante deberá esperar seis (6) meses para volver a iniciar el proceso de certificación.

4.5.2. **Métodos de evaluación de la certificación inicial**

4.5.2.1. **Examen Teórico:**

El examen teórico o escrito de los candidatos incluye preguntas cerradas de diferentes tipos, basadas en los temas establecidos en este documento.

Para los fines de este esquema, se ha elaborado un banco de preguntas, del cual se seleccionarán de manera aleatoria las que conformarán el examen teórico, conforme a lo siguiente:

a) **Para el alcance de Auditor Líder ISO/IEC 27001:2022:** se seleccionarán ochenta (80) preguntas que conformarán el examen teórico, de acuerdo con las siguientes condiciones:

Temas	Cantidad preguntas/ examen
1. Norma ISO/IEC 27001:2022 sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) o su equivalente adoptado a nivel nacional	32
2. Conocimiento de la Norma ISO 19011:2026 Directrices para la auditoría de los sistemas de gestión	8
3. Norma ISO 31000:2018 Gestión del riesgo — Directrices	8
4. Métodos, herramientas de calidad y planificación	8
5. Norma ISO/IEC 27005:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información	12

6. Norma ISO/IEC 27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información	12
Total	**80**

b) Para el alcance de Auditor ISO/IEC 27001:2022: se seleccionarán sesenta (60) preguntas que conformarán el examen teórico, de acuerdo con las siguientes condiciones:

Temas	Cantidad preguntas/ examen
1. Norma ISO/IEC 27001:2022 sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) o su equivalente adoptado a nivel nacional	24
2. Conocimiento de la Norma ISO 19011:2026 Directrices para la auditoría de los sistemas de gestión	6
3. Norma ISO 31000:2018 Gestión del riesgo — Directrices	6
4. Métodos, herramientas de calidad y planificación	6
5. Norma ISO/IEC 27005:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información	9
6. Norma ISO/IEC 27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información	9
Total	**60**

El examen teórico para cada uno de los alcances tendrá un mínimo de aprobación de un **70**%, con un tiempo de duración de tres (**3**) horas para el alcance **de Auditor Líder ISO/IEC 27001:2022** y un tiempo de duración de dos (2) horas **para el alcance Auditor ISO/IEC 27001:2022**

Para fines del examen teórico o escrito se utilizará el ***Formulario Examen Teórico para Certificación de Personas*** (FO-DPE-008).

4.5.2.2. **Selección del Centro de Examen:**

La selección del centro de examen, tanto para evaluaciones teóricas como prácticas, se realizará conforme a los criterios establecidos en el ***Instructivo*** **Selección de Centro de Examen para las Evaluaciones Teóricas y/o Prácticas de Certificación Personas** ***(IN-DPE-004)***. La verificación de las condiciones del centro de examen se efectuará mediante la ***Lista de Verificación de Condiciones del Centro de Examen Teórico (FO-DPE-013)*** o la ***Lista de Verificación de Condiciones del Centro de Examen Práctico (FO-DPE-012)***, según corresponda, debiendo evidenciarse el cumplimiento de los requisitos aplicables antes de la realización de la evaluación.

- Examen de 60 preguntas:

Nivel	Cantidad de preguntas/examen	Valor	Puntaje
1	40	1.5 puntos	60
2	20	2 puntos	40
Total	**60**	**-**	**100**

➢ **Validez:**

Se deben validar todas las preguntas del banco de examen con una frecuencia anual si existen cambios en las mismas, o se hayan elaborado un total de al menos 10 preguntas, las cuales se mantendrán en una base de datos alterna hasta su validación, a través del método de validez de contenido.

- **Validez de contenido**: a través del juicio de expertos.

  Se valorará la opinión de 3 jueces/expertos, los cuales deben validar el contenido y la claridad lingüística de cada pregunta.

  El proceso consiste en validar la pregunta si 2 o más jueces están de acuerdo y, por lo contrario, deben corregirse o eliminarse las preguntas en las que 2 o más jueces están en desacuerdo.

➢ **Confiabilidad:**

Cada año se debe aplicar un método de análisis por ítem con el fin de evaluar la calidad de las preguntas utilizadas en los exámenes, considerando la dificultad y capacidad de discriminación de cada una de ellas.

El análisis de Discriminación y Dificultad por Ítem permite identificar preguntas que no diferencian adecuadamente entre candidatos con alto y bajo desempeño, así como aquellas que resultan demasiado fáciles o difíciles.

Para este método se recopilan los resultados por pregunta de todos los exámenes aplicados, codificando las respuestas correctas con 1 y las incorrectas con 0. Los datos se agrupan por nivel de desempeño (alto y bajo) para el cálculo del índice de discriminación.

Se recomienda que las preguntas tengan un índice de discriminación de al menos 0.20 y una dificultad comprendida entre 0.30 y 0.70. Las preguntas que no cumplan con estos criterios deben ser revisadas o descartadas.

4.5.3. **Criterios y métodos de evaluación para la recertificación**

La certificación tendrá un período de vigencia de dos (**02**) años.

Durante ese período, la persona certificada deberá:

a) Demostrar, a partir de la fecha de obtención de la certificación, la actualización de sus conocimientos mediante el cumplimiento de uno de los siguientes requisitos: (40) horas de capacitación u otras actividades aplicables, realizadas en una institución educativa nacional o internacional cuya situación legal sea reconocida; o doce (12) meses de experiencia laboral comprobada, adquirida con posterioridad a la obtención de la certificación, en temas relacionados con este esquema de certificación.
b) No haber incurrido en ninguno de los criterios establecidos para la suspensión o retiro de la certificación.
c) Completar el formulario Solicitud de Certificación de Personas (FO-DPE-002).
d) Suscribirse al Código de Conducta para la Certificación de Personas (OD-DPE-001).

Si la persona certificada no cumple con estos requisitos, finalizada la vigencia de su certificado, deberá tomar nuevamente el examen teórico para la renovación de este, para lo cual serán aplicables los criterios establecidos en el numeral **4.5.1** y **4.5.2.1** del presente documento.

Nota: *En caso de que la norma de referencia de este esquema cambie o se actualice durante el periodo de certificación, la persona certificada, aún cumpla con lo establecido en los acápites (a) y (b), deberá tomar el examen teórico con los nuevos criterios incluidos en la norma cuando opte por la recertificación.*

La persona certificada podrá solicitar la recertificación desde 60 días antes del vencimiento de su certificado. Se otorgará un periodo de gracia de seis (6) meses para renovar la certificación, después del vencimiento de esta. En el caso de que la persona no agote el proceso de recertificación durante el periodo de gracia, deberá someterse al proceso establecido para la certificación inicial.

4.6. Métodos y criterios de vigilancia

El esquema de certificación de personas para Auditor de Sistema de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022 no conllevará actividades de vigilancia. Para esto, el Comité de Esquema ha tomado en consideración la corta duración del ciclo de recertificación.

4.7. Criterios para suspender y retirar certificación

Los criterios para suspender o retirar la certificación de personas para Auditor de Sistemas de Gestión de la Seguridad de la Información están establecidos en el documento definido por el INDOCAL para estos fines ***Directrices y Lineamientos sobre el Servicio de Certificación de Personas del INDOCAL*** (OD-DEC-010).

4.8. Criterios para efectuar cambios de alcance.

Cuando se amerite, se podrá cambiar o modificar el alcance de este esquema de certificación de personas de acuerdo con los siguientes criterios:

1. Cambios en la normatividad legal vigente o en la norma de referencia utilizada en el presente esquema de certificación.
2. Creación de normas complementarias afines a este esquema de certificación.
3. Modificación en el perfil ocupacional o área del conocimiento específica del Auditor Sistema de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022.
4. Cambios tecnológicos aplicables a este esquema de certificación.
5. Identificación de nuevas necesidades del mercado/sector.

La modificación del presente esquema se comunicará por escrito a las personas afectadas, precisando, en caso necesario, el plazo que se concederá para aplicar las nuevas adecuaciones.

Cuando una persona certificada desee ampliar el alcance de su certificación, deberá solicitar dicha modificación, utilizar el formulario establecido para tales fines y cumplir con cada uno de los requisitos del alcance solicitado. También es posible, a solicitud de la persona, hacer coincidir la evaluación para la ampliación con una evaluación de supervisión o recertificación, siempre que ésta notifique la necesidad con, al menos, dos (2) meses de anticipación al INDOCAL para las previsiones de lugar.

Cuando una persona certificada desee reducir el alcance de su certificación deberá solicitarlo de forma escrita al INDOCAL, indicando las razones de tal decisión, y junto a esta solicitud devolver la documentación de certificación suministrada, como mínimo dos (2) meses antes de la próxima recertificación.

4.9. Criterios para el desarrollo y revisión del esquema.

El desarrollo y la revisión de este esquema de certificación de personas se realiza según los criterios establecidos en las ***Directrices y Lineamientos del Comité del Esquema del Departamento de Certificación de Personas del INDOCAL*** (OD-DEC-009) y en el ***Instructivo para el Desarrollo de Esquemas de Certificación de Personas basados en la Norma ISO/IEC 17024:2012*** (IN-DPE-002).

En ese sentido, durante el desarrollo de este esquema se tomaron en consideración los siguientes criterios:

a) La participación de los/as expertos/as durante el desarrollo del esquema;
b) Representación equitativa de los intereses de cada una de las partes interesadas;
c) Identificación de los prerrequisitos y su vinculación con los requisitos de la competencia;
d) La identificación y alineación de los mecanismos de evaluación con los requisitos de competencia.

Para fines de revisión de este esquema, el Comité del Esquema se reunirá al menos una (1) vez al año, tomando como referencia la fecha de aprobación del mismo.

En caso de que exista un cambio que amerite la modificación del alcance *(tecnológico, del conocimiento específico, de un requisito legal, etc.)* o si la norma ISO/IEC 17024:2012 se actualiza y establece nuevos requisitos para un esquema de certificación de personas, el Comité de Esquema podrá reunirse de manera extraordinaria.

El cumplimiento de estos criterios quedará evidenciado en las ***Actas Sesión Comité del Esquema*** (FO-DPE-004), ***Formulario Control de Asistencia*** (FO-DEC-004) y en el documento del esquema.

5. REFERENCIAS

a) NORDOM ISO/IEC 17024:2012, Evaluación de la conformidad: Requisitos generales para los organismos que realizan la certificación de personas;
b) ISO/IEC 17000 Evaluación de la conformidad. Vocabulario y principios generales;
c) ISO/IEC TS 17027:2014 Evaluación de la Conformidad – Vocabulario relacionado con la competencia de las personas que son usados para la certificación de personas;
d) Norma ISO/IEC 27001:2022 sobre Sistemas de Gestión de la Seguridad de la Información (SGSI) o su equivalente adoptado a nivel nacional;
e) Norma ISO 19011:2026 Directrices para la auditoría de los sistemas de gestión;
f) Norma ISO 31000:2018 Gestión del riesgo — Directrices;
g) Norma ISO/IEC 27005:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información;
h) Norma ISO/IEC 27002:2022 sobre Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información;
i) Directrices y Lineamientos del Comité del Esquema del Departamento de Certificación de Personas del INDOCAL (OD-DEC-009);
j) Directrices y Lineamientos sobre Servicios de Certificación de Personas (OD-DEC-010);
k) Procedimiento Descripción del Proceso de Certificación de Personas (PR-DPE-001);
l) Instructivo para el Desarrollo de Esquemas de Certificación de Personas (IN-DPE-002).

6. REGISTROS

Documento	Registro No.	Responsable	Tiempo de Retención
Registro Expediente Comité de Esquema	RG-DPE-002	Encargado Departamento de Certificación de Personas	10 años

7. NOTIFICACIÓN DE CAMBIOS

Revisión No.	Descripción del/de los Cambio(s)	Razón(es) del/de los cambio(s)
No. 0	Versión original	N/A

8. ANEXOS

Seguridad, Equidad, Validez y Confiabilidad
Para mantener la seguridad, equidad, validez y confiabilidad en los exámenes del Esquema de Auditor de Sistemas de Gestión de la Seguridad de la Información (SGSI) ISO/IEC 27001:2022, se tomarán las siguientes medidas:

- **Seguridad:**

  - El banco de preguntas debe ser igual o mayor a 2 veces la cantidad de preguntas que contiene cada examen.
  - El banco de preguntas deberá ser protegido con contraseña.
  - Se deberá reducir al mínimo las fechas en que se ofrecen exámenes escritos.

- **Equidad:**

Se mantendrá en cada examen la misma igualdad de oportunidades para cada participante, para lo cual:

- **Examen Escrito**: se impartirán exámenes con igual cantidad de preguntas de cada nivel de dificultad (2 niveles):

  Las preguntas de nivel 1 tienen un valor de: 1 punto.
  Las preguntas de nivel 2 tienen un valor de: 2 puntos.

  El valor total de la puntuación asignada a cada tema dependerá de la cantidad de preguntas y del nivel de dificultad de las preguntas que lo integren. El examen deberá estar compuesto de acuerdo con la cantidad de preguntas establecida en el numeral 4.5.2 y con la distribución de niveles indicada en la siguiente tabla:

  - Examen de 80 preguntas:

Nivel	Cantidad de preguntas/examen	Valor	Puntaje
1	60	1 punto	60
2	20	2 puntos	40
Total	**80**	**-**	**100**

9. APROBACIÓN DEL ESQUEMA

Elaborado por:	Revisado por:	Aprobado por:
9.9.2026	Mayke Lerebours — Firmado digitalmente por Mayke Lerebours Fecha: 2026.09.09 09:46:02 -04'00'	9/9/2026
Encargado/a Departamento Certificación de Personas	Analista Departamento de Gestión Técnica	Director/a Evaluación de la Conformidad
		Director General INDOCAL

Miembros del Comité de Esquema:

Organizaciones gubernamentales del sector:

José Raúl Madera — Crismeylin Pérez
Instituto Dominicano de Telecomunicaciones (INDOTEL)

Jenny De Jesús
Centro Nacional de Ciberseguridad (CNCS)

Organizaciones no gubernamentales del sector:

Niurka Hernández — Deiby Lozada
IQTEK Solutions

Raúl Mejía
Claro Dominicana

Experto técnico/consultor privado:

Daniel Batista
Julio Ureña
Red Team RD

Carlos Henríquez
Precisión IT

Institutos de formación y universidades:

Alfonsina Martínez
Betsy Campsteyn
Instituto Tecnológico de Santo Domingo (INTEC)

Nelk Valerio
Daniel Méndez
Instituto Nacional de Formación Técnico Profesional (INFOTEP)

Representante derechos del consumidor:

Antonio Reyes
Instituto Nacional de Protección de los Derechos del Consumidor (Pro-Consumidor)

Representante del organismo de certificación:

Yasser Fajardo
Dirección de Evaluación de la Conformidad – INDOCAL

Marelin Peña
Dirección de Evaluación de la Conformidad – INDOCAL