NORMA TÉCNICA DE COMPETENCIA LABORAL

I.- Datos Generales

Código: NUSPV006.01

Título: Consultoría en sistemas de gestión de la seguridad

Propósito de la Norma Técnica de Competencia Laboral:

Servir como referente para la evaluación y certificación de las personas que brindan consultoría en sistemas de gestión de la seguridad a través de la evaluación del riesgo, el diseño, la gestión para la implementación y la evaluación del desempeño, de un sistema de gestión de seguridad. Asimismo, puede ser referente para el desarrollo de programas de capacitación y de formación basados en NTCL.

Comité de Normalización de Competencia Laboral que la desarrolló:

Sector Seguridad Privada

Fecha de aprobación por el Comité Técnico del CONOCER:	Fecha de publicación en el D.O.F:
04/11/2008	05/02/2009

Nivel de competencia:

Cinco

Desempeña una amplia gama de actividades tanto programadas y poco rutinarias como impredecibles que implican la aplicación de un rango variado de principios fundamentales y técnicas complejas.
Emite lineamientos generales a sus subordinados.
Es el último responsable de la planeación y la programación de las actividades de la organización o grupo de trabajo.
Es el último responsable de los resultados finales del trabajo de todos los equipos y personas que de él dependen.

Ocupaciones relacionadas con esta NTCL de acuerdo con el Sistema de Información del Catálogo Nacional de Ocupaciones (SICNO):

Módulo Ocupacional	Clave del Módulo
Consultores en sistemas administrativos	0825-01

Ocupaciones:	Código:
Consultor de Análisis Organizacional	0825-01-02
Consultor de Sistemas Administrativos	0825-01-04

Clasificación según el Sistema de Clasificación Industrial de América del Norte (SCIAN):

Sector:

54 Servicios profesionales, científicos y técnicos

Subsector:

541 Servicios profesionales, científicos y técnicos

Rama:

5416 Servicios de consultoría administrativa, científica y técnica

Subrama:

54169 Otros servicios de consultoría científica y técnica

Clase:

541690 Otros servicios de consultoría científica y técnica

La presente Norma Técnica de Competencia Laboral, una vez publicada en el Diario Oficial de la Federación se integrará a la Base Nacional de Normas Técnicas de Competencia Laboral que opera el CONOCER a fin de facilitar su uso y consulta gratuita.

II.- Perfil de la NTCL

Unidad 1 de 1

Consultoría en sistemas de gestión de la seguridad

- **Elemento 1 de 4**
  Evaluar el riesgo de daño a los valores
- **Elemento 2 de 4**
  Diseñar el sistema para la gestión de requisitos de la seguridad
- **Elemento 3 de 4**
  Gestionar la implementación del sistema de gestión de la seguridad
- **Elemento 4 de 4**
  Evaluar el desempeño del sistema de gestión de la seguridad

III.-Estándares de la competencia laboral de la Unidad:

Código:	**Unidad:**
NUSPV006.01	Consultoría en sistemas de gestión de la seguridad

Elementos que conforman la Unidad:

Referencia	Código	Título
1 de 4	E0180	Evaluar el riesgo de daño a los valores

Criterios de Evaluación:

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El análisis del riesgo elaborado:

* Detalla el título de cada documento que lo integra, el folio, el nombre del consultor y de los participantes, y la fecha de actualización recomendada;
* Incluye el alcance recomendado del mismo;
* Contiene nominados los valores a proteger;
* Detalla las amenazas relacionadas con cada uno de los valores;
* Incluye las hipótesis de daño que indican la probabilidad de que las amenazas ocurran;
* Describe las prácticas de protección recomendadas para cada hipótesis de daño;
* Contiene la contribución a la protección de las prácticas de protección operantes con respecto a las prácticas de protección recomendadas;
* Especifica el indicador de vulnerabilidad relacionando las hipótesis de daño y las prácticas de protección operantes para cada uno de los valores;
* Detalla el indicador de la importancia crítica para cada uno de los valores;
* Contiene el grado de riesgo determinado para cada valor;
* Incluye las fuentes de información de los valores, las amenazas, las prácticas de protección e importancia crítica;
* Especifica la escala que aplica para cada variable, y;
* Contiene la fecha y el registro de aprobación de la alta dirección.

2. El alcance recomendado del análisis de riesgo:

* Detalla el espacio, tiempo y materia que conforman el escenario de riesgo, e;

* Incluye los compromisos de confidencialidad de la información aprobados por las partes interesadas.

3. Las prácticas de protección recomendadas:

* Incluyen referencias a la gestión de la mejora de la seguridad y las relacionadas con la materia especificada en el alcance, y;

* Especifican los criterios de evaluación de la contribución a la protección de los valores.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Relación entre los términos fundamentales para la evaluación de riesgo: *Alta dirección *Amenaza *Criticidad de imagen pública *Importancia crítica *Interrupción operativa *Protección *Riesgo *Seguridad *Vulnerabilidad	Comprensión

GLOSARIO

1. Alta dirección:	Persona o grupo de personas que representan el nivel jerárquico más alto dentro de una organización, la cual dirigen y controlan.
2. Amenazas:	Se refiere al conjunto de factores cuyos efectos al incidir en los valores logran una disminución o pérdida de su importancia. La guía general de evaluación de ASIS (The American Society and Industrial Security) la define como evento de perdida.
3. Análisis de riesgo:	Se refiere al proceso que se realiza para estimar la magnitud del riesgo. Se conoce también como mapa de riesgo, evaluación de riesgo, matriz de riesgo o estudio de vulnerabilidad.
4. Criterios de evaluación:	Refiere a los parámetros para evaluar el grado de cumplimiento de las prácticas de protección.

5.	Daño:	Se refiere a la disminución o pérdida de valor.
6.	Gestión de la mejora de la seguridad:	Forma parte de la gestión de la seguridad, orientada a reducir el riesgo de manera recurrente.
7.	Hipótesis de daño:	Probabilidad de que una amenaza cause daño sobre un valor determinado.
8.	Importancia crítica:	Ponderación del daño probable. Se expresa en términos de impacto financiero, discontinuidad operativa y/o pérdida de la confianza pública inherentes a un valor o conjunto de valores.
9.	Materia:	Delimitador temático del alcance del escenario al que se referirá el análisis de riesgo, ejemplos: protección civil, seguridad industrial, atención de emergencias, etc.
10.	Partes interesadas:	Es la persona o grupo de personas que están involucradas en la seguridad.
11.	Prácticas de protección operantes:	Son las acciones que se mantienen operando para reducir el riesgo.
12.	Prácticas de protección recomendadas:	Son las acciones que de acuerdo con la experiencia y conocimiento del consultor, reducen el riesgo.
13.	Prevención:	Acciones que pretenden evitar daños.
14.	Protección:	Se refiere al conjunto de funciones que reducen el impacto de los factores de las amenazas.
15.	Riesgo:	Es la relación probabilística entre la vulnerabilidad y la importancia crítica.
16.	Valores:	Se refiere a todo aquello que tiene importancia para quien contrata el servicio de consultoría.
17.	Vulnerabilidad:	Relación entre la cuantificación de las hipótesis de daño y las prácticas de protección operantes.

Referencia	Código	Título
2 de 4	E0181	Diseñar el sistema para la gestión de requisitos de la seguridad

Criterios de Evaluación:

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El manual del sistema de gestión de la seguridad diseñado:

* Detalla el título de cada documento que lo integra, el folio, el nombre del consultor y de los participantes, y la fecha de actualización recomendada;
* Especifica las referencias a otros documentos normativos relacionados con la gestión de la seguridad y con la materia especificada en el alcance del sistema de gestión;
* Contiene la descripción del sistema de gestión de la seguridad;
* Enuncia la política del sistema de gestión de la seguridad;
* Incluye los procedimientos que satisfacen los requisitos de protección del sistema de gestión de la seguridad, y;
* Contiene la fecha y el registro de aprobación de la alta dirección.

2. La descripción del sistema de gestión de la seguridad diseñado:

* Enuncia el alcance determinado del mismo;
* Especifica las mejores prácticas de protección aprobadas por la alta dirección que satisfacen los requisitos de las partes interesadas;
* Contiene los procedimientos de acción correctiva y acción preventiva;
* Incluye los indicadores para la evaluación del sistema, y;
* Enuncia los requisitos de conformidad legal aplicables.

3. El alcance del sistema de gestión de la seguridad determinado:

* Delimita los procesos, áreas funcionales y espacios físicos aprobados, y;
* Especifica la vigencia del sistema.

4. La política del sistema de gestión de la seguridad redactada:

* Determina los principios del sistema de gestión de la seguridad, y;
* Contiene la autorización de la alta dirección.

5. Los principios del sistema de gestión de la seguridad determinados:

* Enuncian los compromisos de la alta dirección con la satisfacción de los requisitos de las partes interesadas, con la mejora continua, con la toma de decisiones soportada en la evaluación de riesgos y con la promoción de la participación de todo el personal.

6. Los indicadores de evaluación determinados:

* Especifican para cada requisito de protección su contribución a la protección y los criterios de conformidad y desempeño del sistema de gestión.

7. Los procedimientos del sistema de gestión de la seguridad desarrollados:

* Contienen un propósito, su alcance, y el control de los cambios;

* Describen las actividades, la responsabilidad y la autoridad de los involucrados, e;

* Incluyen las instrucciones de trabajo y los formularios para el registro de los datos de conformidad.

8. Las instrucciones de trabajo desarrolladas:

* Incluyen el identificador único, referencias a los procedimientos relacionados, y la descripción de actividades de una función/puesto involucrado en particular.

9. Los formularios diseñados:

* Incluyen el identificador único y la referencia a los procedimientos relacionados, y;

* Contienen los espacios necesarios para el registro de los datos de conformidad con los requisitos del sistema de gestión de la seguridad.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Relación entre los términos que se manejan para el diseño del manual del sistema de gestión de la seguridad *Acción correctiva *Acción preventiva *Control de cambios *Documento *Instrucción de trabajo *Política *Principios del sistema de gestión de la seguridad *Procedimiento *Proceso *Sistema de gestión de la seguridad	Comprensión

GLOSARIO

1. Acción correctiva:	Se refiere a las acciones plasmadas en un procedimiento para eliminar la causa de una no conformidad detectada u otra situación indeseable.
2. Acción preventiva:	Se refiere a las acciones plasmadas en un procedimiento para prevenir la causa de una no conformidad potencial u otra situación potencialmente indeseable.

3.	Áreas funcionales:	Llamado así al subconjunto de áreas de una organización con funciones, autoridad y responsabilidad determinadas.
4.	Conformidad:	Se determina cuando se da cumplimiento a un requisito de seguridad.
5.	Control de los cambios:	Es el registro explicativo de los cambios que han afectado a un documento, contiene la fecha, el cambio propuesto, la identidad del proponente y la justificación del cambio.
6.	Criterios de conformidad:	Refiere a los parámetros para determinar el grado de conformidad de la evidencia.
7.	Criterios de desempeño:	Se llama así a los parámetros para determinar el grado de desempeño de la evidencia.
8.	Identificador único:	También se le conoce como la nomenclatura para diferenciar cada instrucción de trabajo o de formularios.
9.	Indicadores de evaluación:	Evidencias que servirán para evaluar conformidad o desempeño respecto de criterios especificados.
10.	Instrucciones de trabajo:	Son las disposiciones técnicas que explican el desempeño de tareas específicas de un proceso.
11.	Mejora continua:	Actividad recurrente para aumentar la capacidad para cumplir los requisitos de seguridad.
12.	Mejores prácticas de protección:	Acciones de protección que han probado su eficacia en otros proyectos de consultoría.
13.	No conformidad:	Se refiere al incumplimiento de un requisito de seguridad.
14.	Organización:	Es el conjunto de personas o instalaciones con una disposición de autoridades, responsabilidades y relaciones.
15.	Política:	Es la expresión que da respuesta al compromiso para cumplir con los requisitos y mejorar continuamente la eficacia del sistema de gestión de la seguridad.
16.	Principios del sistema de gestión de la seguridad:	Son aquellos que rigen el desempeño del sistema de gestión de la seguridad, y se refieren a lo siguiente: a. Enfoque al cliente b. Liderazgo c. Participación del personal d. Enfoque en procesos e. Gestión sistémica f. Mejora continua g. Toma de decisiones fáctica h. Proveedores interdependientes

17.	Procedimientos:	Se refieren a las actividades especificadas en un documento para llevar a cabo un proceso.
18.	Procesos:	Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
19.	Requisitos de conformidad legal:	Necesidad o expectativa establecida en leyes y reglamentos.
20.	Requisitos de protección:	Necesidad o expectativa de protección establecida, generalmente implícita u obligatoria.
21.	Sistema:	Conjunto de procesos mutuamente relacionados o que interactúan.
22.	Sistema de gestión de la seguridad:	Es el que se desarrolla para dirigir y controlar los requisitos con respecto a la seguridad.

Referencia	Código	Título
3 de 4	E0182	Gestionar la implementación del sistema de gestión de la seguridad

Criterios de Evaluación:

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El plan de implementación del sistema de gestión de la seguridad elaborado:

* Detalla, en cada documento que lo integra, el título, la fecha de elaboración, la fecha de liberación prevista, el nombre del consultor y de los participantes;
* Contiene el pronóstico, el programa y el presupuesto para la implementación del sistema de gestión, y;
* Contiene la fecha y el registro de aprobación de la alta dirección.

2. El pronóstico de implementación elaborado:

* Describe los requisitos de protección cuyo desempeño evidencie no conformidad u oportunidad de mejora;
* Describe cada no conformidad y oportunidad de mejora detectada;
* Establece un objetivo de mejora para cada no conformidad y oportunidad de mejora descrita, y;
* Contiene la valoración del efecto de los objetivos de mejora sobre el riesgo.

3. El programa de implementación desarrollado para agregar al pronóstico:

* Contiene el nombre del responsable de alcanzar el objetivo de mejora, y;

* Especifica la fecha esperada para el cumplimiento de cada objetivo de mejora.

4. El presupuesto de implementación desarrollado para agregar al programa:

* Detalla el costo de implementación de las acciones requeridas para el cumplimiento de cada objetivo de mejora.

La persona es competente cuando posee los siguientes:

CONOCIMIENTOS	NIVEL
1. Relación entre los términos para la implementación del sistema de gestión de seguridad *Eficacia *Eficiencia *Implementación *Mejora continua *No conformidad	Comprensión

GLOSARIO

1.	Fecha de liberación:	Es aquella que se establece para concluir la implementación de lo incluido en el plan de implementación.
2.	Implementación:	Proceso requerido para alcanzar un objetivo de mejora.
3.	Objetivo de mejora:	Resultado de conformidad pretendido.

Referencia	Código	Título
4 de 4	E0183	Evaluar el desempeño del sistema de gestión de la seguridad

Criterios de Evaluación:

La persona es competente cuando obtiene los siguientes:

PRODUCTOS

1. El comparativo de indicadores elaborado:

* Detalla la fecha para cada periodo que se compara;

* Incluye el resultado de la comparación entre la evaluación de riesgos previa y la evaluación de riesgos actualizada, e;

* Incluye el resultado de la comparación entre el riesgo evaluado y el pronosticado.

2. El juicio de desempeño determinado:

* Contiene el resultado del sistema de gestión de la seguridad expresado en tiempo, costo y protección, e;

* Incluye indicadores de eficacia y eficiencia del plan de implementación.

3. El reporte gerencial de evaluación desarrollado:

* Detalla el título, la fecha de elaboración y el nombre del consultor y de los participantes;

* Contiene los resultados de los indicadores del desempeño del sistema de gestión de la seguridad, e;

* Incluye la explicación de los cambios detectados.

GLOSARIO

1. Evaluación de riesgos actualizada:	Es aquella que fue realizada en la fecha más próxima.
2. Evaluación de riesgos previa:	Es aquella que se realizó anterior a la evaluación de riesgos actualizada.
3. Juicio de desempeño:	Dictamen respecto de la eficacia y eficiencia de los resultados del plan de implementación.

Conocer
Normalización · Certificación
Competencias Laborales

NORMA TÉCNICA DE COMPETENCIA LABORAL

Anexo 1: EC0062

Fecha límite para revisar y/o actualizar el Estándar de Competencia	Vigencia de la Certificación en el Estándar de Competencia
5 de febrero de 2011	**Sin vigencia**

La revisión realizada establece como fecha límite para revisar y/o actualizar el Estándar de Competencia	La revisión realizada establece la vigencia de la Certificación en el Estándar de Competencia
31 de Enero de 2015	**Sin vigencia**