ÁREA GOBERNANZA DE LAS NIS

Por: Mtro. Miguel Angel Díaz Pérez

Objetivo

Obtendrás una herramienta financiera que coadyuve a la administración de la entidad; así como mejores prácticas societarias; entre otras: Cómo debe integrarse un gobierno corporativo y el Código de Ética.

Temario

TEMA I. GOBIERNO CORPORATIVO

1. Consejo de Administración
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo
2. Mujeres en el Consejo de Administración
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo de implementación

Temario

3. Órgano de vigilancia independiente
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo de implementación

TEMA 2. GESTIÓN EMPRESARIAL SOSTENIBLE

1. Política de Administración de Riesgos
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo de implementación

Temario

2. Estrategia de sostenibilidad
    - Recomendaciones generales
    - Requerimientos de las NIS
    - Procesos y controles necesarios
    - Ejemplo de implementación

TEMA III. CONDUCTA EMPRESARIAL RESPONSABLE

1. Código de integridad y ética
    - Recomendaciones generales
    - Requerimientos de las NIS
    - Procesos y controles necesarios
    - Ejemplo de implementación

Temario

2. Seguridad en la información
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo de implementación
3. Protección y privacidad de datos de terceros
   - Recomendaciones generales
   - Requerimientos de las NIS
   - Procesos y controles necesarios
   - Ejemplo de implementación

Temario

TEMA 4. CONSIDERACIONES FINALES

- Recomendaciones y sugerencias para su implementación

ANTECEDENTE

Que integran

- El Consejo Mexicano de Normas de Información Financiera y de Sostenibilidad (CINIF), ha lanzado el Programa de Aceleración Sostenible NIS A-1 y NIS B-1, enfocado en preparar a empresas para la adopción de estos estándares a partir de 2025.

- La finalidad del CINIF es que las organizaciones empiecen a identificar los riesgos y amenazas que afecten negativamente a la entidad, con la finalidad de establecer políticas y procedimientos para mitigar esos impactos negativos

Estructura de las NIS

Sigue una estrategia de dos etapas:

1. Una primera etapa con el Marco Conceptual (NIS A-1) y Normas sobre **Métricas** de Desempeño Sostenible (NIS B-1), y

2. Una segunda etapa que desarrollará NIS temáticas más específicas, todo enfocado en temas ambientales, social y de gobernanza (ASG) para la revelación de información de sostenibilidad.

Quien deben aplicarlas

- Entidades de interés público (EIP): Aquellas que tienen la obligación de rendir cuentas al público.

- Las entidades que no son de interés público (ENIP): No obligadas, **pero deberán** incluir la información de sostenibilidad de manera parcial o total **cuando así lo requieran los usuarios de su información financiera o cuando la misma entidad lo considere relevante.** Este rubro incluye a las pymes, ya que las normas están pensadas para que, de manera sencilla, puedan adoptarlas. (Ver para creer)

Requerimientos de revelación (84.5.5)

Las NIF particulares identifican los siguientes requerimientos de revelación:

a) Revelaciones generales - obligatorias para todas las entidades (EIP y ENIP);

b) Revelaciones para ElP - obligatorias solo para ElP; no obstante, las ENIP deberán incluir estas revelaciones, ya sea de forma parcial o total, cuando así lo requieran los usuarios de su información financiera o bien, cuando la propia ENIP lo considere conveniente.

Trascendencia de la gestión de riesgos (ASG)

- Son criterios que enriquecen y engrandecen los niveles de responsabilidad de las empresas. (Sin duda en el curso lo conocerán; por la correlación en diferentes áreas del saber)

- Adicional a la obtención de beneficios económicos, generación de recursos financieros y de mejorar las economías de clientes y proveedores, también se agregan enfoques de **protección al ambiente**, mejoras en las **condiciones sociales** y el logro de las **mejores prácticas** en temas **de gobierno corporativo** y liderazgo.

- Guía de enfoque basado en riesgo (CNBV 2023 y COSO ERM)

Indicadores definidos y claros

- Es necesario que las entidades mantengan *registros robustos sobre la* ***implementación de políticas y procedimientos relativos a su gobernanza*** y aspectos de sostenibilidad que incluya: información fuente, hojas de cálculo, reportes internos requeridos por los IBSO* que soporten los cálculos y afirmaciones, controles internos, entre otros.

- Para esto, los preparadores de la información de sostenibilidad pueden consultar fuentes recomendadas por organismos especializados, las cuales pueden adecuarse a la complejidad de cada entidad y asegurar su implementación.

*Indicadores Básicos de Sostenibilidad

NIS B-1 (Indicadores Básicos de Sostenibilidad)

Introducción

- La NIS B-1 identifica y explica con detalle **30 Indicadores Básicos de Sostenibilidad** (IBSO) que deben ser implementados, monitoreados y gestionados para mejorar el desempeño sostenible; para el curso que nos ocupa tenemos los siguientes:

- **Indicadores cuantitativos**: Ambientales 16, Sociales 4 y **Gobernanza 1**

- **Indicadores cualitativos**: Ambientales NA, Sociales 2 y **Gobernanza 7**

- **Los 30 IBSO deben ser identificados, y posteriormente deben establecerse los procedimientos para mitigar los riesgos.**

Área Gobernanza, IBSO cuantitativos

Gobierno corporativo

- C.2 Mujeres en el consejo de administración

Área Gobernanza, IBSO cualitativos

Gobierno corporativo

- C.1 Consejo de administración
- C.3 Órgano de vigilancia independiente

Gestión empresarial sostenible

- C.4 Política de administración de riesgos
- C.5 Estrategia de sostenibilidad

Área Gobernanza, Indicadores cualitativos

Conducta empresarial responsable

- C.6 Código de integridad y ética
- C.7 Seguridad de la información
- C.8 Protección y privacidad de datos de terceros

TEMA I.

GOBIERNO CORPORATIVO

Introducción al tema
¿Qué es un gobierno corporativo?

- No existe una definición como tal y e la práctica profesional es muy común escuchar el anglicismo “COMPLIANCE”

- Podemos entender que es el **conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una empresa**.

- En concreto, establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de partes interesadas, y estipula las reglas por las que se rige el proceso de toma de decisiones sobre la compañía para la generación de valor. (Cuidado en materia fiscal, “Control efectivo de la entidad”, inciso c) del último párrafo de la fracción X del Artículo 26 del CFF)

¿Cómo se integra?

No hay regla escrita; empero, con órganos intermedios de control, entre otros:

1. Comité de administración de riesgos
2. Comité de vigilancia
3. Comité de auditoría interna
4. Comité de practicas societarias

Trascendencia de los estatutos

- En el sector financiero es muy común encontrar la estructura de un gobierno corporativo dentro de los estatutos.

- Cuando una entidad quiere implementar un Gobierno Corporativo, es de suma trascendencia hacer un diagnóstico de los estatutos sociales y proceder a realizar las modificaciones que procedan.

- **En empresas administradas por el Administrador Único; sin duda, deberán proceder a cambiarlo a un Consejo de Administración, motivado por los IBSO en estudio.** Ya que de no hacerlo deberán ser revelado en las notas a los Estados Financieros.

- Cuidar la fracción VI, del Apartado B del artículo 27 del Código Fiscal de la Federación.

1. Consejo de Administración (IBSO C.1)

Recomendaciones generales

- De acuerdo con el inicio de vigencia de las NIS, la información de sostenibilidad **deberá presentarse en las notas a los estados financieros** correspondientes a 2025, informe que se emitirá en 2026. Sin embargo, se recomienda que, a partir de enero de 2025, las entidades tomen en cuenta las medidas y acciones sugeridas y detalladas en este documento.

- De suma trascendencia conocer la estructura orgánica de toda entidad y resiliencia para enfrentar las nuevas NIS en materia.

- Cuidar libro de actas de asamblea y libro de sesiones del Consejo de Administración.

Recomendaciones generales

- Tener estructuras que contengan elementos clave como **políticas** claras, **procedimientos** documentados e implementados, operación y composición del consejo de administración, gestión de su estrategia, riesgos y ética empresarial.

- **Un compliance o cumplimiento normativo** es un sistema integral de políticas y procedimientos que una organización implementa para asegurar la adhesión a las leyes, regulaciones, estándares éticos y políticas internas aplicables a su actividad. Su objetivo es prevenir y sancionar incumplimientos legales y éticos, mitigando riesgos de multas, daños a la reputación y pérdidas de negocio, y promoviendo una cultura de transparencia y responsabilidad corporativa.

- Sin duda, un gran momento para iniciar la aventura del cambio en muchas empresas, ¿no creen?

Recomendaciones generales

- Mantener un registro actualizado de los integrantes del Consejo de Administración que cuente con la siguiente información: nombre completo, género, cargo dentro del consejo, participación en comités estratégicos. (SIC)

- Clasificar a los miembros del consejo por género y rol dentro del consejo. (SIC)

- De suma Trascendencia el Libro de actas de sesiones del Consejo de Administración (Artículo 143 de la Ley General de Sociedades Mercantiles, en correlación con el artículo 36 y 41 del Código de Comercio)

Requerimientos de las NIS

- Dentro del documento denominado “Guías para su implementación”, la CINIF solo establece el tener un Consejo de Administración. (NO reconoce al Administrador único)

- Órganos análogos, Consejo de Gerentes en una S de RL de CV, Asamblea de socios en una Sociedad Civil.

- Sin embargo, sugiero que vaya adoptando estructuras corporativas en materia; ya que, 7 (siete) IBSO son cualitativos y sólo uno es cuantitativo.

Procesos y controles necesarios conforme al IBSO C.1

- Revisar el acta constitutiva de la entidad y sus modificaciones para identificar si la administración de la entidad está a cargo de un administrador único o de un consejo de administración u órgano análogo.

- En caso de que sí exista un consejo de administración, identificar el número de consejeros independientes y desglosarse por hombres y mujeres.

Ejemplo

- Tipo de indicador Cualitativo

- Revelación: **SI** o NO

Objetivo: El indicador permite conocer si la entidad cuenta con un Consejo de administración (u órgano de gobierno equivalente) que defina su rumbo estratégico, vigile su operación y apruebe su gestión

Ejemplo

CONTEXTO

La entidad “X” se constituyó como sociedad anónima de capital variable (S.A. de C.V.) cuyo objetivo es la comercialización de pinturas, solventes, y otros artículos para pintar. Dentro de su acta constitutiva se designó como **administrador único al socio mayoritario**, quién se encarga de establecer las estrategias de la entidad y tiene gran interés en incluir aspectos ambientales y sociales en su plan de acción para este año. En dicha acta también se nombre a un comisario.

Considerando que la NIS B-1 establece puntualmente que, para efectos de este indicador, el administrador único no debe considerarse como órgano de gobierno equivalente al conejo de administración, la entidad deberá revelar que NO cuenta con un consejo de administración.

El gran final del IBSO C.1

Revelación en la notas a los estados financieros

> "Con base a la información y documentación que obra en la administración de la entidad y el Indicador Básico de Sostenibilidad C.1 obtenido, la entidad **NO** cuenta con un Consejo de Administración implementado y vigente que cumpla con todos los requisitos de la NIS B-1"

Conclusión

En este indicador, creo que no vamos a tener problema.

2. Mujeres en el Consejo de Administración (IBSO C.2)

Antecedente

- La reforma Constitucional que entró en vigor en 2019, conocida como Paridad en Todo (Paridad de Género), busca asegurar que la mitad de los cargos de decisión sean para las mujeres en los tres poderes del Estado.

- El tema nodal es que a pesar de los avances de las mujeres en el terreno de los derechos formales y en diversos ámbitos como la educación y el laboral, entre otros, han seguido excluidas de los núcleos donde se toman las decisiones.

Recomendaciones generales

- Los Indicadores Básicos de Sostenibilidad (NIS B-1) requiere la revelación de los treinta indicadores, ya que se considera que este set de indicadores es, en lo individual y en su conjunto, información relevante; **por lo tanto, no se requiere llevar a cabo un análisis de materialidad adicional.**

Esto se explica como sigue:

1. Los IBSO pueden tener dos posibles lecturas:

a) Por una parte, representan el impacto de sus prácticas de gobernanza; y

Recomendaciones generales

b) Por otro lado, pueden ayudar a entender los riesgos que representan para una entidad los relacionados con la sostenibilidad

El Marco Conceptual (MC) de las NIS, en su párrafo 42.1.18 establece que la información de sostenibilidad de una entidad relacionada con su impacto con sus principales prácticas en materia de gobernanza, es importante para monitorear la contribución de dicha entidad a la sostenibilidad del entorno global.

Requerimientos de las NIS

- De acuerdo al IBSO C.2 en estudio, el único requerimiento es determinar el número de mujeres que participan en el Consejo de Administración.

- Sugiero que se detalle el cargo y función que desempeña; así como, describir que tipo de poderes tiene en la entidad.

Procesos y controles necesarios

- Revisar el acta constitutiva de la entidad y sus modificaciones para conocer la conformación del Consejo de Administración y determinar el número de mujeres que integran en el Consejo de Administración. (SIC)

- Además, cuidar la obligación prevista en la fracción VI del Apartado B del artículo 27 del Código Fiscal de la Federación. (Avisos al RFC)

- Es menester comentar los integrantes del Consejo de Administración pueden ser catalogados Beneficiarios Controladores de la Entidad, conforme lo establece el último párrafo del la Regla Miscelánea 2.8.1.20, la cual establece los siguiente

Procesos y controles necesarios

"Cuando no se identifique a persona física alguna bajo los criterios establecidos en esta regla, en relación con el artículo 32-B Quáter del CFF, se considerará como beneficiario controlador a la persona física que ocupe el cargo de administrador único de la persona moral o equivalente. **En caso de que la persona moral cuente con un consejo de administración u órgano equivalente, cada miembro de dicho consejo se considerará como beneficiario controlador de la persona moral**."

Ejemplo de implementación

- Ejemplo de la NIS B-1, del IBSO C-2, elaborado por la CINIF.
- Tipo de indicador : Cuantitativo
- Objetivo: El indicador mujeres en el consejo de administración permite identificar si la entidad cuenta con una composición diversa en su gobierno corporativo.
- Procedimientos:

Procedimientos

Valor Absoluto: Sumatoria de todas las mujeres que integran el Consejo de Administración al cierre del informe de la entidad (Vgr. Asamblea General Ordinaria de Accionistas)

Valor Relativo:

Mujeres en el Consejo de Administración

Entre:

Total de integrantes del Consejo de Administración

Igual:

Valor Relativo

Ejemplo

- La entidad ‘X’ S.A. de C.V. ofrece servicios de turismo. Cuenta con un consejo de administración conformado por 15 personas, de los cuales 13 son hombres y 2 son mujeres. Todos los consejeros cuentan con perfiles profesionales distintos que aportan a la firma solidez en sus decisiones. Tres de los integrantes son independientes.

- VALOR ABSOLUTO: 2 mujeres
- VALOR RELATIVO: (2/15) x 100 = 13.33% Mujeres en el Consejo de Administración
- REVELACIÓN: SI

El gran final del IBSO C.2
Mujeres en el Consejo de Administración

Revelación en la notas a los estados financieros

> "Con base a la información y documentación que obra en la administración de la entidad y el Indicador Básico de Sostenibilidad obtenido, la entidad **SI** cuenta con la determinación de número de mujeres que integran el Consejo de Administración, implementada y vigente que cumple con todos los requisitos de la NIS B-1"

Conclusión

Considero que este IBSO, no será complicado determinarlo, solo basta cuidar lo asentado en el libro de sesiones del Consejo de Administración.

3. Órgano de vigilancia independiente (IBSO C.3)

Antecedente

- Por historia, Comisario en una SA de CV
- Por naturaleza jurídica: Consejo de Vigilancia (S de RL de CV)
- En la actualidad:
  a) Comité de vigilancia
  b) Comité de Auditoría Interna

Recomendaciones generales

- La información relacionada con su impacto con sus principales prácticas en materia de gobernanza debe ser revelada, en cualquier caso; por ejemplo: Informe del Comisario. (Artículo 166 de la LGSM)

- Por lo anterior, tomando en cuenta el Marco Conceptual (MC) NIS A-1 y considerando que los IBSO permiten identificar y medir los impactos sobre la gobernanza de toda entidad, además de ayudar a la identificación de riesgos, deben ser revelados en su totalidad.

- Por el ejemplo citado en el primer punto de la presente diapositiva, Trasciende el Acta de Asamblea General Ordinaria de Accionistas.

Requerimientos de las NIS

- Identificar si existe órgano independiente y activo que vigile la actuación de los administradores de la entidad. (SIC)

Procesos y controles necesarios

- Revisar el contrato social constitutivo de la entidad y sus modificaciones para conocer si está prevista la existencia de un órgano de vigilancia independiente.

- Cabe mencionar que la Ley General de Sociedades Mercantiles requiere que exista un Comisario y la Ley del Mercado de Valores requiere, para ciertos casos, que exista un Comité de Auditoría.

- En caso de no tener establecida la figura de un órgano de vigilancia y se quiere subsanar esta falta, la entidad puede establecer el órgano de vigilancia mediante la figura de un comité de vigilancia, seleccionando para ello, gente que tenga capacidad técnica y experiencia suficiente para llevar a cabo actividades de verificación de que la administración está trabajando para cumplir los objetivos de sus accionistas y con apego a la ley y las normas que le son aplicables a la entidad. (Estructura de gobierno corporativo)

Procesos y controles necesarios

Si la entidad no cuenta con un órgano de vigilancia independiente y activo responderá “No” a este indicador; no obstante, si tiene la intención de implementarlo, en adición a las acciones sugeridas en la sección de procesos y controles necesarios para la implementación de las NIS, para una mejor implementación puede llevar a cabo los siguientes procesos y controles, los cuales toman en cuenta las mejores prácticas; no obstante, no deben interpretarse como requisitos ni como criterios de verificación de la NIS B-1:

- Establecer los criterios de selección y designación de los miembros del órgano de vigilancia.

- **Definir normas de operación, roles y responsabilidades del órgano de vigilancia.**

Procesos y controles necesarios

- Implementar una estrategia de monitoreo de la información financiera y riesgos operativos.
- Implementar mecanismos para detectar y prevenir prácticas desleales.
- **Verificar que la empresa cumpla con regulaciones fiscales, laborales y comerciales.**
- Garantizar la comunicación clara y efectiva de las actividades del órgano de vigilancia.
- Desarrollar programas de formación en ética, gobernanza y prevención de riesgos.

Ejemplo de implementación

- Ejemplo del IBSO de la C.3
- Tipo de indicador : Cualitativo
- Objetivo: El indicador permite conocer si se cuenta con un órgano encargado de la vigilancia de la gestión de una entidad, el cual puede establecerse, según las leyes vigentes, en la figura de uno o varios comisarios o de un comité de apoyo al consejo de administración, como podría ser un comité de auditoría.
- Procedimientos: NA, es indicador cualitativo

Contexto

- La entidad ‘X’ se dedica a la comercialización de productos para el hogar. Cuenta con 25 socios, y en su contrato social se establece el nombramiento de un consejo de vigilancia.

- El consejo de vigilancia se reúne una vez al mes y se encargan, entre otras cosas, de gestionar los riesgos inherentes a la operación de la
- sociedad para lo que realizan auditorías administrativas y financieras.

- El comité incluye miembros independientes

Revelación: SI

El gran final del IBSO C.3
Órgano de Vigilancia Independiente

Revelación en la notas a los estados financieros

SI "Con base a la información y documentación que obra en la administración de la entidad y el Indicador Básico de Sostenibilidad obtenido C.3, la entidad cuenta con un Órgano de vigilancia independiente, implementado y vigente que cumple con todos los requisitos de la NIS B-1"

TEMA II.

GESTIÓN EMPRESARIAL SOSTENIBLE

¿Qué es?

- La gestión empresarial sostenible es un **modelo de negocio que integra las consideraciones económicas, sociales y ambientales** en la toma de decisiones y operaciones para generar valor a largo plazo, sin comprometer los recursos ni el bienestar de las futuras generaciones.

- Implica un enfoque sistémico que va más allá del beneficio financiero, buscando un equilibrio entre la rentabilidad, el cuidado del planeta y el bienestar de la sociedad a través de los pilares de la triple cuenta de resultados (planeta, personas y beneficios).

- Cualquier similitud con las NIS, es pura coincidencia, de aquí, su trascendencia

1. Política de Administración de Riesgos (IBSO C.4)

Introducción

- Trascendental el control interno de la entidad (Sugerencia, COSO ERM)
- Nos podemos apoyar de la Guía de un enfoque basado en riesgos, emitida por la CNBV en el 2023.
- De suma importancia identificar el riesgo, para mitigar cualquier contingencia futura.
- De moda por la reforma en materia en prevención de lavado de dinero

Recomendaciones generales

- Tener un Comité de Administración de Riesgo (Parte fundamental de un Gobierno Corporativo)

- Implementar un adecuado control interno

- Objetivo del Control Interno:

a) Implementar un sistema de normas, acciones, políticas y procedimientos para controlar la gestión administrativa y operativa de una empresa.

b) Prevenir y detectar errores, fraudes e irregularidades.

c) Asegurar la eficiencia de los procesos y la consecución de los **objetivos estratégicos** de la organización.

Recomendaciones para su implementación

- Si la entidad **no cuenta con la política** mencionada responderá “No” a este indicador; no obstante, si tiene la intención de implementarla, en adición a las acciones sugeridas en la sección de procesos y controles necesarios para la implementación de las NIS, para una mejor implementación puede llevar a cabo los siguientes procesos y controles, los cuales toman en cuenta las mejores prácticas; **no obstante, no deben interpretarse como requisitos ni como criterios de verificación de la NIS B-1. (SIC)**

- Una adecuada política tiene como mínimo los siguientes puntos relevantes: objetivo, alcance, principios rectores, controles internos, indicadores de desempeño, designación de responsabilidades, sanciones y medidas correctivas, así como fecha de vigencia; además de establecer en todos los casos ya sea el comité, el área o persona que será responsable de llevar a cabo las acciones definidas.

Recomendaciones para su implementación

Para un mejor funcionamiento de la política, se sugiere:

1. Implementar un proceso de identificación y clasificación de riesgos.
2. Mantener un registro de riesgos y su evolución (mapa de riesgos).
3. Establecer planes de acción específicos para reducir o mitigar los riesgos más críticos.
4. Implementar una metodología de monitoreo continuo de riesgos.
5. Implementar mecanismos de prevención y detección de fraudes internos y externos.
6. **Diseñar un Plan de Continuidad del Negocio (PCN) para situaciones de crisis**.
7. Fomentar una cultura organizacional de prevención de riesgos.
8. Revisar anualmente la efectividad de la política de gestión de riesgos.

Requerimientos de las NIS

- Identificar si la entidad tiene establecida una política de administración de riesgos, implementada y vigente que cumpla con todos los requisitos establecidos en la NIS B-1. (SIC)

- Entorno a PLD/FT no dudo que exista; empero, para cualquier entidad, dudo que exista. (Escucho comentarios por parte de ustedes)

- Cada vez es más común tener una valuación con un enfoque basado a riesgo

Procesos y controles necesarios

En caso de que la entidad tenga la intención de implementarla como parte de su evolución hacia un desempeño sostenible, puede considerar las siguientes acciones:

1. Designar a una persona, área o comité como responsable de la gestión de riesgos en la entidad.

2. Diseñar y establecer la política de administración de riesgos que cumpla con todos los requisitos establecidos en la NIS B-1. Por ejemplo, parte de esta política podría establecer que se contraten pólizas de seguros para los activos más importantes de la entidad.

3. Establecer esquemas de monitoreo para asegurar que la política está implementada y es ejecutada en la operación de la entidad. (Sugerencia IA denominada CLICK UP, para gestión de proyectos y automatización de tareas)

Ejemplo de implementación

- C.4: Política de administración de riesgo

- Tipo de indicador: Cualitativo

- **Objetivo**: Este indicador permite conocer si la entidad cuenta con procesos para identificar, cuantificar, priorizar y monitorear los posibles riesgos.

- REVELACIÓN: SI o NO

1. **SI**: la entidad cuenta con una política implementada de administración de riesgos establecida que cumpla **TODAS** las características establecidas en el párrafo 45.3.1.3 de la NIS B-1
2. **NO**: la entidad no cuenta con una política implementada que reúna las características establecidas por la NIS B-1

Contexto

ALCANCE

Esta política abarca:

1. Todas las áreas operativas, administrativas y logísticas de la empresa.

2. Actividades de producción, mantenimiento, transporte, almacenamiento y manejo de materiales peligrosos.

3. Aplicación a todos los empleados, contratistas, proveedores y visitantes que acceden a las instalaciones de la empresa.

OBJETIVOS

1. Identificar y evaluar riesgos que puedan impactar la seguridad, salud, medio ambiente, activos o la reputación de la empresa.

2. Establecer medidas preventivas y correctivas para mitigar riesgos de manera eficiente.

Contexto

3. Promover una cultura organizacional orientada a la seguridad y prevención.

4. Garantizar el cumplimiento de regulaciones y estándares aplicables, tales como:
   a) ISO 45001 (Seguridad y Salud Ocupacional).
   b) Normas de seguridad industrial locales e internacionales.
   c) Regulaciones ambientales aplicables

Contexto

PRINCIPIOS RECTORES

1. Prevención primero: Priorizar las acciones preventivas sobre las correctivas.

2. Cumplimiento normativo: Garantizar el respeto y adopción de las leyes y normativas aplicables.

3. Cultura de seguridad: Fomentar el compromiso de todos los niveles jerárquicos hacia la gestión de riesgos.

4. Mejora continua: Revisar y actualizar continuamente los procesos y controles

Contexto

COMPONENTES DE LA POLÍTICA

1. Identificación de Riesgos

Realizar análisis iniciales y periódicos de peligros (ej., Análisis de Riesgo de Trabajo - y Análisis de Riesgo por Procesos).

Categorizar los riesgos en:

- Físicos: Ruido, vibración, calor.
- Químicos: Contacto o manejo de sustancias peligrosas.
- Mecánicos: Riesgos asociados con máquinas y equipos.
- Humanos: Fatiga, errores de procedimiento o capacitación insuficiente.

Contexto

2. Evaluación y Priorización

- Asignar niveles de severidad (bajo, medio, alto) y probabilidad de ocurrencia.
- Determinar cuáles riesgos requieren medidas inmediatas y cuáles pueden ser gestionados a mediano o largo plazo.

3. Controles y Mitigación

Controles técnicos:

- Instalación de barreras físicas y sistemas de protección (guardas en máquinas).
- Implementación de sistemas de alarma y detección automática.
- Revisión y mantenimiento programado de equipos.

Controles organizacionales:

- Capacitación continua del personal en protocolos de seguridad y uso de equipos.
- Protocolos de autorización y permisos de trabajo en áreas críticas.

Contexto

Controles administrativos:

- Uso obligatorio de Equipos de Protección Personal (EPP) en áreas definidas.
- Gestión documental para el cumplimiento de las normativas de seguridad.

Plan de emergencias:

- Desarrollo de procedimientos para actuar ante incendios, derrames, explosiones o fallos de equipos críticos.
- Simulacros de emergencia al menos dos veces al año

El gran final del IBSO C.4
Política de administración de riesgo

La Entidad “X” analiza su política de administración de riesgos para verificar si cumple todos los puntos señalados en el párrafo 45.3.1.3 de la NIS B-1. Si bien la entidad cubre la mayoría de los requerimientos establecidos en la NIS sobre la política de administración de riesgos, no cuenta con un plan de continuidad del negocio en caso de la materialización de riesgos establecido; y, por lo tanto, la Entidad “X” revela en su información de sostenibilidad que **NO** cumple con este indicador.

SIN DUDA SERÁ UNO DE LOS MÁS COMPLICADOS A IMPLEMENTAR Y DAR CABAL CUMPLIMIENTO.

Además falto que la empresa cumpliera con lo siguiente

- Supervisión y monitoreo
- Responsabilidades (Alta dirección, Trabajadores y equipo de seguridad e higiene)
- Implementación (Capacitación inicial y publicación de la política)
- Plazo de evaluación y revisión

2. ESTRATEGIA DE SOSTENIBILIDAD (IBSO C.5)

¿En que consiste?

- Es un plan integral a largo plazo que una organización o individuo implementa **para equilibrar los aspectos ambientales, sociales y económicos de su operación**, con el objetivo de prosperar sin dañar el medio ambiente ni comprometer los recursos de futuras generaciones.

- Implica integrar la sostenibilidad en el propósito, la cultura y las operaciones diarias para reducir el impacto negativo, aumentar la competitividad y generar valor a largo plazo

Recomendaciones generales

Cabe señalar que las acciones listadas se han elaborado con base en mejores prácticas; no obstante, no deben interpretarse como requisitos ni como criterios de verificación de la NIS B-1:

- Implementar un proceso de identificación y clasificación de riesgos relacionados con cuestiones ambientales, sociales y de gobierno corporativo (ASG).
- Mantener un registro de riesgos ASG y su evolución (mapa de riesgos).
- Establecer planes de acción específicos para reducir o mitigar los riesgos ASG más críticos.
- Implementar una metodología de monitoreo continuo de riesgos ASG.
- **Diseñar un Plan de Continuidad del Negocio (PCN) para situaciones de crisis**.
- Fomentar una cultura organizacional de prevención de riesgos ASG.
- Revisar anualmente la efectividad de la política de gestión de riesgos ASG.

Requerimientos de las NIS

- Identificar si la entidad tiene establecida una estrategia de sostenibilidad que cumpla con todos los requisitos de la NIS B-1

- Sugerencia para desarrollar una estrategia de sostenibilidad.

1. Análisis y Diagnóstico
2. Definición de Objetivos y Metas
3. Compromiso y Cultura
4. **Plan de acción e implementación**; por ejemplo: Transición a energías renovables, economía circular (RRR), gestión de recursos, etcétera.
5. Monitoreo y mejora continua

Procesos y controles necesarios

En caso de que la entidad tenga la intención de implementarla como parte de su evolución hacia un desempeño sostenible, puede considerar las siguientes acciones:

- Determinar los IBSO y analizar los riesgos importantes que de esta revisión se deriven.

- Establecer un plan de acción de mitigación de los riesgos importantes identificados; este plan de acción es, **en sí mismo, la estrategia de sostenibilidad**.

Ejemplo

- Tipo de indicador : Cualitativo

- **Objetivo**: Este indicador permite conocer si la entidad cuenta con una estrategia de sostenibilidad aprobada y supervisada por el consejo de administración o en su caso por el administrador único

REVELACIÓN: SI o NO

- **SI:** la entidad cuenta con una estrategia de sostenibilidad establecida que contemple TODAS las características establecidas en el párrafo 45.3.2.4 de la NIS B-1
- **NO**: la entidad no cuenta con una política implementada que reúna las características establecidas por la NIS B-1.

Ejemplo 1

La entidad ‘X’ ha establecido como parte de su misión y visión ser una de las entidades líderes en el ramo de la producción de materiales para la construcción, utilizando tecnologías que contribuyen a la baja emisión de gases de efecto invernadero. El administrador único, apoyado de un experto en la materia, se encargó de la revisión de ambos enunciados, y aunque cumplen con lo que se considera una buena estructura, **no permearon al plan de acción de la entidad**.

REVELACIÓN: NO

Ejemplo 2

La entidad “X” se dedica a la elaboración de productos alimenticios de harina de trigo. Cuenta con un consejo de administración, el cual se encarga de supervisar que se cumpla el **plan estratégico** establecido, mismo que incluye aspectos ambientales y sociales. La entidad aún no cuenta con un reporte de sostenibilidad, pero cuenta con evidencia de identificar riesgos relacionados con sus trabajadores, la comunidad, consumo de agua y energía, así como manejo de desechos. También ha establecido acciones para mitigar esos riesgos y ha establecido metas al respecto. Por ejemplo, reducir el consumo de energía eléctrica en un 10% para el siguiente año. Además, ha relacionado sus acciones con los objetivos del desarrollo sostenible (ODS).

REVELACIÓN: **SI**

TEMA III.

CONDUCTA EMPRESARIAL RESPONSABLE

Antecedente

- Es el compromiso de las empresas de **operar de manera ética y sostenible**, gestionando los impactos de sus actividades sobre el medio ambiente, la sociedad y los derechos humanos, y alineando sus acciones con el desarrollo sostenible.

- Implica identificar y abordar los efectos negativos de sus operaciones y cadenas de suministro, buscando no solo evitar daños, sino también contribuir activamente al bienestar social y a la protección del planeta para las generaciones presentes y futuras.

Antecedente

Aspectos clave de la Conducta Empresarial Responsable (CER)

1. Consideración de los impactos: Las empresas deben evaluar y gestionar los impactos negativos de sus negocios en las personas, el medio ambiente y la sociedad.

2. Cadenas de suministro: El compromiso se extiende a los impactos generados por sus proveedores y otras empresas con las que tienen vínculos comerciales.

3. Compromiso con el desarrollo sostenible: Las empresas responsables contribuyen al desarrollo sostenible en las comunidades donde operan.

4. Estándares internacionales: Las Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable son un marco internacional importante que guía estas prácticas.

1. CÓDIGO DE INTEGRIDAD Y ÉTICA (C.6)

Introducción

- Es un documento que establece los valores, principios y pautas de conducta que rigen el desempeño de los miembros de una organización para asegurar un comportamiento ético, responsable y honesto en el ejercicio de sus funciones.

- Estos códigos buscan fortalecer la cultura de integridad, **prevenir la corrupción** y la discriminación; así como, mantener la confianza de clientes, proveedores e inversionistas en las instituciones.

Recomendaciones generales

- Toda entidad deberá reportar este indicador a partir del 2025

- Es importante aclarar que los IBSO reportados deben de corresponder a la misma entidad económica que presenta los estados financieros, tal y como se establece en el párrafo 42.2 de la NIS B-1.

- De acuerdo con el Marco Conceptual (NIS A-1), las entidades deben realizar la mejor estimación posible **utilizando información razonable, respaldada y verificable** disponible en la fecha de emisión de la información de sostenibilidad.

Requerimientos de las NIS

- Identificar si la entidad tiene un Código de Ética

- En la práctica profesional es común saber o encontrar que en las entidades ya tienen este Código; empero, hay que revisarlo y saber si cumple con todo lo dispuesto en la NIS B-1

Procesos y controles necesarios de acuerdo a lo descrito en la C.6

En caso de que la entidad tenga la intención de implementarla como parte de su evolución hacia un desempeño sostenible, puede considerar las siguientes acciones:

1. Diseñar y establecer un código de ética que cumpla con todos los requisitos establecidos en la NIS B-1.

2. Designar a una persona, área o comité como responsable de la ética empresarial y que será quien recibirá las denuncias de faltas al código de ética, investigará los casos denunciados y establecerá sanciones a los responsables de las faltas.

Procesos y controles necesarios de acuerdo a lo descrito en la C.6

3. Implementar una línea de denuncias de faltas al código de ética, por ejemplo: un correo electrónico, una línea telefónica, un buzón físico o una página web, garantizando el anonimato del denunciante. Existen empresas que prestan estos servicios.

4. Establecer una matriz de sanciones a quienes cometieron faltas al código.

5. Hacer del conocimiento de todos los colaboradores de la entidad, así como de clientes y proveedore y, la existencia del código de ética, de un canal de denuncias de faltas a este código y de la existencia de una matriz de sanciones.

6. Establecer esquemas de monitoreo para asegurar que el código de ética se está cumpliendo

Ejemplo de implementación

- Tipo de indicador: Cualitativo

- El IBSO código de integridad y ética permite conocer si la entidad cuenta con un código de integridad y ética implementado y conocido por todos los trabajadores y partes interesadas, mediante el cual se establezcan en la organización principios, valores y reglas de conducta para que todos sus colaboradores se conduzcan dentro de un marco de excelencia en el ejercicio de su empleo, cargo o comisión.

- **Objetivo**: Establecer una cultura de integridad, de comportamiento ético y responsable. El código de integridad y ética debe prohibir expresamente la promoción, realización o cualquier actividad tendiente a cometer actos de corrupción, situaciones de acoso, o de comportamiento antiético entre otros por parte de sus colaboradores.

REVELACIÓN: SI O NO

- SI: la entidad si cuenta con cuenta con un código de integridad y ética implementado que contemple todos los elementos establecidos en el párrafo 45.4.1.6 de la NIS B-1

Contexto

- La entidad “X” es una firma que presta servicios de consultoría financiera cuenta con un código de integridad y ética que contiene políticas para el correcto actuar de todas las personas que colaboran en la organización.

- Ha establecido controles internos que les ayudan a cumplir con la legislación aplicable para prevenir e identificar Operaciones con Recursos de Procedencia Ilícita y a prevenir y mitigar incidentes de corrupción y faltas de integridad.

- Adicionalmente, dentro del mismo código se mencionan los medios para presentar denuncias anónimas, los cuales consisten en un correo electrónico y un número de teléfono gestionado por un tercero que apoya en el tratamiento de las denuncias y reporta lo conducente al comité de honor y justicia de la organización.

Contexto

- El código contempla sanciones a imponer a quién no cumple con el código que van desde la separación temporal hasta definitiva dependiendo de la severidad de la infracción.

- También dan a conocer el código a través de pláticas, correos, carteles, entre otros.

- REVELACIÓN: SI ¿Cómo redactarían la nota a los estados financieros?

2. SEGURIDAD EN LA INFORMACIÓN (IBSO C.7)

Antecedente

- Es el conjunto de procedimientos, herramientas y políticas para **proteger la confidencialidad, integridad y disponibilidad de los datos** y los sistemas que los procesan, tanto físicos como digitales, frente al acceso no autorizado, la alteración o la destrucción. Su objetivo es prevenir, detectar y corregir amenazas para garantizar que la información crítica esté accesible y funcional solo para usuarios autorizados.

- La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México, recientemente actualizada en 2025, **protege la confidencialidad, integridad y disponibilidad de los datos personales** de los ciudadanos, obligando a las empresas a obtener consentimiento para su uso, informar sobre el manejo de la información y garantizar los derechos ARCO (acceso, rectificación, cancelación y oposición) de los titulares, así como a implementar medidas de seguridad para su protección.

Recomendaciones generales

- Aviso de Privacidad: Deben informar a los usuarios sobre cómo se usarán sus datos personales. (Clientes, Proveedores y Trabajadores)

- Consentimiento: Es necesario obtener el consentimiento del titular de la información antes de tratar sus datos.

- Derechos ARCO: Los titulares tienen derecho a **acceder** a sus datos, **rectificarlo**s, **cancelarlos** y **oponerse** a su tratamiento.

- Medidas de Seguridad: Deben **implementar medidas técnicas** y organizativas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Recomendaciones para su implementación

- Restringir el acceso a la información y solo permitir a personal autorizado.
- Proteger información confidencial mediante cifrado.
- Prevenir ataques de phishing, malware y suplantación de identidad.
- Asegurar la recuperación de información en caso de pérdida o ataque.
- Regular el uso de computadoras, móviles de acceso fuera de las instalaciones de la entidad.
- Identificar y responder a incidentes de seguridad de forma rápida.
- Capacitar a los trabajadores en buenas prácticas de seguridad digital.

Requerimientos de las NIS

- Identificar si la entidad tiene una política para salvaguardar la información, que esté implementada y vigente que cumpla con todos los requisitos establecidos en la NIS B-1.

- Por los tiempos que vivimos, no dudo que muchas entidades ya tengan una política en materia y más por el alto riesgo que existe en medios electrónicos y digitales.

Procesos y controles necesarios

En caso de que la entidad tenga la intención de implementar la política como parte de su evolución hacia un desempeño sostenible, puede considerar las siguientes acciones:

- Designar a una persona, área o comité como responsable de la política de seguridad de la información.
- Diseñar y establecer la política de seguridad de la información que cumpla con todos los requisitos establecidos en la NIS B-1.
- Establecer esquemas de monitoreo para asegurar que la política está implementada y es ejecutada en la operación de la entidad

Procesos y controles necesarios

- Revisar y en su caso actualizar el aviso de privacidad, para que sea acorde a la NIF B-1.

- La actualización a la Ley de la materia incluye la obligación de adoptar prácticas de privacidad desde el diseño (Privacy by Design) y el uso de técnicas de anónimos y pseudónimos para proteger la privacidad.

Ejemplo

- Tipo de IBSO: Cualitativo

- **Objetivo:** El indicador seguridad de la información permite conocer si una entidad cuenta con una política implementada para proteger los activos de información, así como la información bajo su custodia, de posibles amenazas o vulnerabilidades que pongan en riesgo la integridad, confidencialidad o disponibilidad de la información.

REVELACIÓN: SI O NO

- **SI**: la entidad cuenta con una política implementada de seguridad de la información para salvaguardar la confidencialidad, integridad y disponibilidad de esta, que contemple todas las características establecidas en el párrafo 45.4.2.6 de la NIS B-1.

- **NO**: la entidad no cuenta con una política implementada que reúna las características establecidas por la NIS B-1.

Contexto

Una firma que presta servicios de defensa fiscal, ubicada en una zona de alta exposición a temblores, cuenta con un servidor para respaldar su información en la nube y tiene su aviso de privacidad y manejo de datos. Identifica toda la información que se considera sensible para el negocio. También tienen un control para el manejo de los expedientes físicos y hay una persona que lleva el control de entrada y salida dichos expedientes. Los colaboradores saben que nadie puede sacar información de la oficina, ya que reciben.

REVELACIÓN: **SI**

NO dudo que muchas empresas ya lo tienen y no será problema revelar lo que proceda en la nota correspondiente

3. PROTECCIÓN Y PRIVACIDAD DE DATOS DE TERCEROS (IBSO C.8)

Antecedente

- La protección y privacidad de datos de terceros se refieren al **derecho de las personas a controlar cómo se usa, comparte y almacena su información personal**, garantizando que las organizaciones la manejen de forma ética y segura, y protegiéndolas de daños como la suplantación de identidad.

- En México, este derecho está consagrado en el Artículo 16 de la Constitución y se regula con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y sus reglamentos, así como a través de los principios de consentimiento, transparencia y derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

¿Qué implica?

- Control sobre la información: Los individuos tienen derecho a decidir quién tiene acceso a sus datos y cómo se utilizarán.

- Seguridad: Se trata de proteger la información de accesos no autorizados y de sufrir consecuencias negativas, como el fraude o el ciberacoso.

- Consentimiento informado: Las organizaciones deben solicitar y obtener el consentimiento de las personas antes de recopilar y usar sus datos, informándoles sobre el propósito y los riesgos.

- Tratamiento legítimo: Los datos deben utilizarse solo para los fines para los que fueron recopilados y no más allá del tiempo necesario.

Recomendaciones generales

- Tener cuidado con lo que se comparte: No proporcionar datos personales en sitios no confiables, ser cauteloso con correos electrónicos sospechosos y no dar información sensible a desconocidos.

- Leer avisos de privacidad: Conocer qué datos se recogen y a quién se comparten las empresas o servicios.

- Activar la autenticación de dos factores: Agregar una capa de seguridad adicional a las cuentas.

- Utilizar software antivirus y redes seguras: Proteger los dispositivos contra malware y accesos no autorizados.

Recomendaciones para su implementación

- Restringir el acceso a la información y solo permitir a personal autorizado.
- Proteger información confidencial mediante cifrado.
- Prevenir ataques de phishing, malware y suplantación de identidad.
- Asegurar la recuperación de información en caso de pérdida o ataque.
- Regular el uso de computadoras, móviles de acceso fuera de las instalaciones de la entidad.
- Identificar y responder a incidentes de seguridad de forma rápida.
- Capacitar a los trabajadores en buenas prácticas de seguridad digital.

Requerimientos de las NIS

- Identificar si la entidad tiene una política para salvaguardar la información, que esté implementada y vigente que cumpla con todos los requisitos establecidos en la NIS B-1.

- Por los tiempos que vivimos, no dudo que muchas entidades ya tengan una política en materia y más por el alto riesgo que existe en medios electrónicos y digitales.

Procesos y controles necesarios

- Recopilar y tratar datos de forma transparente: Informar a los individuos sobre qué datos se recogen y cómo se utilizarán.

- Garantizar la seguridad de los datos: Implementar medidas para proteger la información contra accesos indebidos y vulneraciones.

- Cumplir con la normativa: Adherirse a la Ley Federal de Protección de Datos Personales y sus regulaciones.

Ejemplo

- Tipo de indicador: Cualitativo

- Objetivo: El indicador protección y privacidad de datos de terceros permite identificar si una entidad cuenta con una política implementada para fomentar la protección y privacidad de datos personales, tanto en la recopilación y almacenamiento, como en el uso o destrucción de estos.

REVELACIÓN: SI O NO

- **SI**: la entidad cuenta con una política implementada de protección y privacidad de datos personales de terceros que contemple todas las características establecidas en el párrafo 45.4.3.4 de la NIS B-1
- **NO**: la entidad no cuenta con una política implementada que reúna las características establecidas por la NIS B-1

Contexto

- Una tienda departamental ofrece productos en su página web, donde guarda datos personales de sus clientes como su nombre, domicilio, datos de contacto y datos de pago, los cuales incluyen tarjetas de crédito y débito.

- Durante el proceso de compra, el cliente puede leer el aviso de protección y privacidad de datos de la entidad y debe seleccionar el recuadro que indica que ha leído la política y está de acuerdo con la manera de proceder. Si el cliente tiene dudas sobre su pedido, se comunica a los números que proporciona la entidad y el colaborador que atiende al cliente, le pide algunos datos como, por ejemplo, el número de pedido y algunos datos adicionales como tipo de productos comprados o relacionados con su domicilio y teléfono.

- Todo el personal es capacitado sobre el uso de los datos personales de los clientes.

- REVELACION: **SI**

TEMA IV.

CONSIDERACIONES FINALES

Recomendaciones y sugerencias para su implementación

- Los IBSO en el área Gobernanza, conllevan el cumplimiento de varias disposiciones legales; por lo que, sugiero que iniciemos con un diagnóstico para saber que tiene la entidad implementado y que hay que realizar.

- Hoy en día el enfoque basado en riesgo es trascendental en cualquier entidad; por lo que, sugiero en estudio y en su caso, la implementación del modelo de control interno denominado COSO-ERM y en entidades de interés publico (EIP) conocer la Guía con enfoque basado a Riesgo publicada en 2023 por la CNBV.

- Por último, no olvidar que esta obligación de Información de Sostenibilidad entró en vigor a partir de enero de 2025; para los indicadores que procedan.

Citas citables

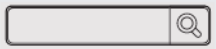
- Las buenas prácticas en gobierno corporativo aportan seguridad económica y jurídica, fomentando el crecimiento sostenible de las empresas.*

*fuente: https://www.deloitte.com/es/es/services/risk-advisory/perspectives/que-es-el-gobierno-corporativo.html

¿QUÉ OPINAN?

POR SU ATENCIÓN ¡GRACIAS!

CONTÁCTANOS



PÁGINA WEB

www.cofide.mx

TELÉFONO

01 (55) 46 30 46 46

DIRECCIÓN

Av. Río Churubusco 594 Int. 203,
Col. Del Carmen Coyoacán, 04100
CDMX

SIGUE NUESTRAS REDES SOCIALES

COFIDE

Cofide SC

Cofide SC

@cofide.mx