INSTITUTO ARGENTINO
DEL PETROLEO Y DEL GAS

PRÁCTICA
RECOMENDADA

PR IAPG-SC-47-2025-00

PRÁCTICA DE GESTIÓN DE SEGURIDAD DE PROCESOS

La presente PR fue aprobada en la reunión de Comisión Directiva el 3 de diciembre de 2025

"La gestión de seguridad de procesos es actualmente un pilar indispensable a nivel mundial para la sostenibilidad de las organizaciones en términos de la reducción del riesgo de accidentes mayores y una mayor eficiencia de procesos industriales. Las buenas prácticas y el manejo efectivo de los sistemas de gestión formales son práctica habitual en algunas compañías del país desde hace años, pero aún falta dar un paso para que estas sean una práctica generalizada en todas las industrias que operan en la Nación.

Durante los últimos 30 años, tanto en Europa, como en los Estados Unidos y, más recientemente, en algunos países latinoamericanos, se han desarrollado e implementado normativas regulatorias que establecen estándares formales para los sistemas de gestión de seguridad de procesos. En Argentina, si bien hay un avance sobre la necesidad de gestionar la seguridad de procesos, aún falta trabajar en un enfoque de gestión específicos para esta área.

Es por ello por lo que un grupo de empresas del O&G nos hemos reunido para discutir un Marco de Gestión de Seguridad de Procesos buscando poder transmitir la experiencia adquirida a lo largo de estos años y ponerlo a disposición para que sirva de ayuda a otras organizaciones a diseñar e implementar sus propios sistemas de gestión."

1 OBJETIVO

El propósito de esta práctica es establecer lineamientos y pautas para la implementación de un **Sistema de Gestión de Seguridad de Procesos**, con el fin de proteger la vida humana, el ambiente, y los activos.

2 ALCANCE

Esta práctica aplica a industrias con sistemas operativos y procesos en donde una pérdida de contención puede causar daño a personas, ambiente, comunidad, instalaciones, activos y/o sustentabilidad del negocio.

3 DEFINICIONES

Abandono: conclusión de actividades en un sitio y desmontaje o retiro de las instalaciones que se utilizaron, con el objetivo de devolver el área a su estado original o a un estado que sea ambientalmente adecuado. Este proceso puede ser total, cuando se finalizan todas las actividades y/o se retiran todas las instalaciones, o parcial, cuando solo se retiran algunos elementos o se realiza un desmantelamiento selectivo.

Accidente: evento no planeado y no deseado que provoca un daño, lesión u otra incidencia negativa sobre las personas, ambiente, instalaciones o activos, o comunidad.
Ambiente de trabajo: entorno en el que se desarrollan actividades laborales. Incluye aspectos físicos, psicológicos y organizacionales.

Análisis de riesgo: proceso para identificar, evaluar, priorizar y controlar las posibles amenazas que podrían afectar a un proceso o actividad industrial. Implica analizar las causas de las amenazas, las consecuencias que podrían generar y la probabilidad de que ocurran.

Análisis de riesgos cualitativo: los análisis cualitativos siguen siendo caracterizaciones analíticas del riesgo basadas en la evidencia, se utilizan tratamientos descriptivos o categóricos de la

información en lugar de estimaciones numéricas cuantitativas.

Análisis de riesgos semicuantitativo: combina elementos tanto cualitativos como cuantitativos para evaluar la probabilidad y el impacto de un riesgo. Se utiliza una escala numérica para representar la probabilidad y el impacto, pero también se considera la experiencia y el juicio de expertos para una evaluación más precisa.

Análisis de riesgos cuantitativo: es una metodología que cuantifica la probabilidad esperada de ciertos eventos, así como las consecuencias dañinas generadas por escenarios peligrosos sobre personas. Utilizan metodologías para simular consecuencias de eventos mediante modelos numéricos.

Auditoría: proceso sistemático, independiente y documentado para obtener evidencias objetivas y evaluarlas con el fin de determinar el grado en que se cumplen los criterios establecidos. Pueden ser de carácter interno o externo.

Barreras: medidas de protección que se implementan para evitar o mitigar los efectos de un incidente, accidente o fallo en un proceso. Estas barreras pueden ser físicas, procedimentales o de gestión, y su objetivo principal es proteger a los trabajadores, el entorno y el proceso mismo.

Cambio: cualquier agregado, eliminación, sustitución o modificación que afecte el diseño o el estado actual de equipos, instalaciones, modos operativos, productos u organizaciones.

Cambio permanente: cambios propuestos cuya implementación implican una alteración y/o transformación definitiva de las condiciones originales.

Cambio temporal: cambio que tiene una duración limitada en el tiempo hecho con la intención de restablecer posteriormente la configuración original u otra configuración permanente.

Cambio de emergencia: cambio requerido ante situaciones que requieran acción inmediata con el objetivo de evitar daño a los equipos, peligros personales, daños ambientales o penalidades económicas severas.

Causa: factor o circunstancia que podría contribuir a la ocurrencia de un incidente o accidente. Este factor puede ser físicos, humanos, organizativos, o relacionados con el diseño o la gestión.

Certificaciones: proceso mediante el cual se verifica que un producto, servicio, persona o empresa cumple con requisitos específicos establecidos en normas o especificaciones técnicas. Es una forma de asegurar la conformidad con estándares establecidos, garantizando la calidad y el cumplimiento.

Ciclo de vida: secuencia de etapas sucesivas por la que pasa un activo industrial, desde su concepción como idea hasta su desmantelamiento y/o abandono.

Competencias: atributos personales y aptitud demostrados para aplicar conocimientos y habilidades.

Comunidad: individuos que viven o trabajan en proximidad de las instalaciones y que pueden ser impactados por pérdidas de contención o eventos de seguridad de procesos de las instalaciones industriales.

Consecuencia: impacto o efecto de un evento sobre personas, ambiente, activos o instalaciones, comunidad y/o reputación.

Criterio de tolerancia al riesgo: nivel máximo de desviación o incertidumbre que la organización está dispuesta a aceptar con respecto al riesgo. Típicamente se muestra en una Matriz de Riesgo, con niveles aceptables, ALARP (As low as reasonable posible), inaceptable.

Cultura de seguridad de procesos: maneras de pensar y de hacer, moldeadas por el contexto a lo largo del tiempo, adaptadas para afrontar los riesgos de seguridad más importantes, conectando las técnicas y procedimientos, con las competencias y saberes de las personas.

Desactivación: bloquear o aislar manualmente, inhibir, forzar, efectuar una derivación o deshabilitar un dispositivo, PLC o sistema de manera tal que éste no realice la función para la que fue diseñado, con el propósito de efectuar pruebas, mantenimiento y puesta en marcha o decomisionado.

Desvíos: Incumplimiento de un requisito. Falta de cumplimiento de las normas, estándares o requisitos especificados, tanto legales como internos, así afecten a parámetros técnicos o económicos, o a los elementos de los sistemas de gestión de Calidad, Medio Ambiente y/o Seguridad.

Documentación de seguridad de procesos: información relacionada con el proceso utilizada para ayudar al entendimiento de los peligros, incluyendo documentos y especificaciones técnica, planos y cálculos de ingeniería, especificación de diseño, fabricación e instalación de equipos de proceso, hojas de seguridad de materiales, limites de operación seguro, matriz causa efecto, plot plan y lay out, entre otros.

Documento puente: documento que facilita la comunicación y la coordinación entre diferentes partes involucradas en el proceso, asegurando que todos comprendan sus roles y responsabilidades, y que la información necesaria se comparta de manera efectiva.

Emergencia mayor: evento inesperado cuya magnitud podría causar daños significativos a personas, ambiente, instalaciones o procesos, requiriendo una acción inmediata para prevenir, mitigar o neutralizar las consecuencias.

Entrenamiento: proceso sistemático de actividades físicas o intelectuales diseñadas para mejorar las capacidades físicas, mentales o de destreza de una persona. Implica una serie de procedimientos y actividades.

Equipo de protección personal: cualquier equipo, ropa, pieza, dispositivo o accesorio utilizado para proteger a los trabajadores de riesgos que puedan amenazar su salud o seguridad durante su trabajo.

Equipo multidisciplinario: grupo de personas con diferentes especialidades y conocimientos que trabajan juntos para lograr un objetivo común.

Equipos críticos / elementos críticos de seguridad de procesos: cualquier dispositivo (mecánico, neumático, hidráulico, eléctrico o electrónico), sistema o subsistema que actúa como (o parte esencial de) una barrera para evitar o mitigar los efectos de uno de los siguientes escenarios:

- Una liberación no planificada de materiales inflamables o tóxicos / energía con impacto a las personas, instalación o ambiente de severidad nivel A o B (los más severos de una categoría).
- Un incidente relacionado con el proceso con posibilidad razonable de ocurrencia, que pudiese causar lesiones graves o muerte.
- Una liberación de materiales que podrían tener un impacto ambiental grave.
- Una violación del acceso de seguridad que tiene el potencial de sabotaje u otras consecuencias graves (por ejemplo: falla de los sistemas de control de acceso).

Escenario creíble: situación o evento realista que tiene una razonable probabilidad de ocurrencia considerando las sustancias involucradas, equipos, diseño, condiciones operativas, contexto, y otros factores.

Especificación de diseño: documento técnico clave que define los requisitos funcionales, operativos y de seguridad que debe cumplir un sistema, equipo o instalación para garantizar un funcionamiento seguro y confiable.

Estándares: documentos que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito.

Factores humanos: características, habilidades y limitaciones de las personas que influyen en su interacción con sistemas, equipos, procesos y otros individuos.

Falla: pérdida, deterioro, o desviación de la función de protección de un elemento o sistema crítico.

Gestión de riesgo: conjunto de actividades sistemáticas para identificar, evaluar, controlar y monitorear los peligros asociados a procesos industriales que involucran sustancias peligrosas.

Grupo de interés: toda persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad de la compañía.

Hallazgos: Conclusión alcanzada por el equipo de auditoria basada en los datos recolectados la cual indica una necesidad de mejora.

Hoja de Seguridad del Producto: Documento técnico que proporciona información detallada sobre los peligros de una sustancia química y las medidas necesarias para su manejo seguro.

Identificación de peligro: Reconocer y describir todas las fuentes potenciales de daño que pueden afectar a personas, ambiente y propiedad.

Incidentes: Evento no planificado que interrumpe o podría interrumpir el funcionamiento seguro de un proceso.

Indicadores: Herramientas claves para medir, monitorear y mejorar la eficacia del desempeño.

Indicadores reactivos: Indicadores que reflejan eventos ya ocurridos.

Indicadores proactivos: Indicadores que evalúan condiciones o acciones que pueden prevenir un incidente.

Inhibición: Acción, evento o configuración que interrumpe intencionalmente la función para la cual fue diseñado un sistema o equipo de seguridad.

Inspección: Actividad planificada y sistemática que tiene el objetivo de verificar que el estado físico, funcional y documental de equipos, instalaciones, procedimientos, con el fin de detectar hallazgos.

Instalación: Conjunto de equipos, recipientes y edificios donde se desarrolla un proceso.

Integridad mecánica: El proceso para verificar que un determinado equipo, sistema o instalación puedan funcionar de forma segura y confiable durante todo su ciclo de vida.

Investigación: Proceso estructurado y sistemático que busca identificar las causas de un evento con el objetivo de evitar su recurrencia.

Lecciones aprendidas: Conocimiento adquirido a partir de la experiencia con el propósito de evitar la repetición de eventos.

Limites operativos seguros: Rangos definidos para las variables críticas de un proceso (como presión, temperatura, nivel, caudal, concentración, etc.). Superar estos límites puede comprometer la integridad del proceso, activar barreras de seguridad o derivar en incidentes mayores.

Malos actores: Sistemas o equipos con performance de confiablidad inaceptables teniendo en cuenta la cantidad, costo de reparaciones y su disponibilidad.

Mantenimiento: Conjunto de actividades técnicas y organizativas destinadas a preservar o restaurar la funcionalidad y confiablidad de equipos e instalaciones.

Mantenimiento predictivo: Actividades de mantenimiento basado en información y/o monitoreo de condiciones para anticipar fallas.

Mantenimiento preventivo: Actividades de mantenimiento realizado de forma programada para evitar fallas.

Marco normativo: Marco compuesto de leyes, reglamentos, estándares y guías técnicas que establecen los requisitos mínimos para prevenir eventos.

Matriz de riesgo: Representación gráfica de los riesgos de un escenario basado en la probabilidad de ocurrencia y la severidad de la consecuencia del evento, que contiene los niveles aceptables e inaceptables de los riesgos para la compañía.

Mejora continua: Enfoque sistemático para identificar, evaluar, implementar y perfeccionar productos, servicios o procesos, con el objetivo de aumentar la eficiencia, la calidad y el valor entregado.

Nivel de investigación: Profundidad, rigurosidad y alcance metodológico requerido para analizar un evento.

Organización: Estructura, roles, responsabilidades, cultura y sistemas de gestión que conforman una empresa.

Operación: Ejecución segura, controlada y eficiente de las actividades productivas dentro de una instalación industrial. Existen diferentes modos de operación: normal, temporal, de puesta en marcha, parada programada, parada de emergencia, abandono, hibernación, otros.

Peligro: Cualquier situación, acto o fuente que tiene la capacidad de causar daño. Condición química, biológica o física que tiene el potencial de causar daño a personas, ambiente y activo.

Pérdida de Contención: Cualquier liberación no controlada ni planificada de materia o energía desde su sistema de confinamiento primario.

Permiso de trabajo: documento formal y obligatorio que autoriza la ejecución de tareas no rutinarias o con riesgos específicos, asegurando que se han identificado los peligros, evaluados los riesgos, y establecido las condiciones a cumplir para ejecutarlas.

Política: conjunto de principios, directrices y reglas establecidas por una organización para guiar la toma de decisiones y el comportamiento dentro de un área específica.

Procedimiento: conjunto de instrucciones escritas claras y precisas que describen los pasos para la realización de una tarea.

Riesgo: Una medida de impacto a personas, ambiente, activos o reputación, en función de la probabilidad de ocurrencia de un evento no deseado y la magnitud de sus consecuencias.

Seguridad de procesos: Marco disciplinado para la gestión de integridad de los procesos y sistemas operativos que manejan energía y/o sustancias peligrosas, mediante la aplicación de principios de buen diseño, ingeniería y prácticas de operación y mantenimiento.

Sistema de gestión: Conjunto de actividades formalmente establecidas y diseñadas para producir resultados específicos de manera consistente y sostenible.

Sistemas de seguridad: equipos y/o procedimientos diseñados para limitar o interrumpir una secuencia de incidente evitando así un evento de pérdida o mitigando sus consecuencias.

Situación insegura: cualquier aspecto de un entorno que puede poner en peligro la seguridad de las personas, instalaciones o medio ambiente, incluyendo condiciones físicas y materiales que pueden causar accidentes.

Tareas no rutinarias: se refiere a cualquier actividad que no es parte de las operaciones normales de una planta o proceso, y que no está cubierta por los procedimientos operativos estándar. Estas tareas pueden incluir trabajos de mantenimiento, reparaciones o cambios en el proceso que se realizan con poca frecuencia.

4 PROCESOS PRINCIPALES

El contenido de este documento se divide en 4 (cuatro) procesos principales con apertura de un total de 18 elementos, que podrán ser implementados total o parcialmente por las industrias que adopten esta práctica para la Gestión de la Seguridad de Procesos.

4.1. Proceso Principal I: Compromiso y Liderazgo
- Elemento 1: Cultura de seguridad de procesos, compromiso y responsabilidad de líderes
- Elemento 2: Participación del personal
- Elemento 3: Calificación, capacitación y desempeño del personal
- Elemento 4: Ambiente de trabajo y factores humanos
- Elemento 5: Gestión de contratistas
- Elemento 6: Cumplimiento del marco normativo, prácticas y estándares
- Elemento 7: Relaciones con grupos de interés

4.2. Proceso Principal II: Gestión de Riesgo de las Instalaciones
- Elemento 8: Información y documentación de Seguridad de Procesos
- Elemento 9: Identificación y análisis de riesgos
- Elemento 10: Integridad Mecánica y Elementos críticos de Seguridad de Procesos
- Elemento 11: Planificación y gestión de emergencias mayores

4.3. Proceso Principal III: Prácticas Operativas
- Elemento 12: Procedimientos operativos
- Elemento 13: Gestión del cambio
- Elemento 14: Revisión de Seguridad previa a la puesta en marcha (PSSR)
- Elemento 15: Prácticas de trabajo seguro

4.4. Proceso Principal IV: Aprendizaje y Mejora continua
- Elemento 16: Revisión y mejora continua
- Elemento 17: Investigación de incidentes y aprendizaje de la experiencia
- Elemento 18: Auditorías

PROCESO PRINCIPAL I
COMPROMISO y LIDERAZGO

1. ELEMENTO 1: CULTURA DE SEGURIDAD DE PROCESOS, COMPROMISO Y RESPONSABILIDAD DE LIDERES

Objetivo: Definir los valores y la política de seguridad de procesos, implementar una estructura organizacional con definición de responsabilidades y atribuciones del personal involucrado, crear medios de comunicación de los valores, las políticas y los objetivos, así como comprometerse a la disponibilidad de recursos para la implementación, la operación y la mejora continua del Sistema de Gestión de Seguridad de Procesos.

1.1. Valores y política de seguridad de procesos

La dirección de la organización asegurará que se establezcan, documenten, implementen y divulguen dentro de la política de la organización los valores de seguridad de procesos.

1.2. Estructura Organizacional y Responsabilidad de la Dirección

La dirección asegurará que se establezca y documente la estructura organizacional para la gestión de riesgos de las instalaciones, incluyendo en la descripción de Roles y Responsabilidades los aspectos de seguridad de procesos.

1.3. Compromiso

Los directivos y líderes deben mostrar activamente el compromiso con la seguridad de los procesos.

1.4. Sistema de comunicación

La dirección asegurará que se defina un sistema de comunicación para:

a. Informar la política, los valores, las metas y los planes para lograr el desempeño establecido de seguridad de procesos.

b. Lograr la comunicación continua y recíproca entre los diferentes niveles de la organización incluyendo situaciones inseguras, incidentes ocurridos, resultados de investigaciones de incidentes, auditorías realizadas y desempeño de seguridad de procesos.

1.5. Disponibilidad de recursos y planificación

La dirección asegurará la planificación y la disponibilidad de los recursos necesarios para la implementación y ejecución del Sistema de Gestión de Seguridad de Procesos, así como el cumplimiento de los demás requisitos establecidos en esta práctica recomendada.

2. ELEMENTO 2: PARTICIPACIÓN DEL PERSONAL

Objetivo: Realizar prácticas de gestión para promover el involucramiento, la conciencia y la participación de todo el personal en el diseño, desarrollo, implementación y mejora de la Seguridad de Procesos.

2.1 Disponibilidad de los canales de participación:

La dirección deberá asegurar que existan canales e instancias de participación del personal y que sean accesibles a todos los empleados y contratistas. Dicho sistema deberá asegurar la protección de la información e identidad de los participantes, así como el resguardo de las propuestas ingresadas, cuando sea requerido. Deberá ser un sistema abierto de modo que se pueda conocer el estado de aquellos que requieran seguimiento.

Ejemplos de dichos canales son: foros, actividades de sensibilización e información, reportes de incidentes, situaciones inseguras, accidentes, identificación de peligros, investigación de accidentes, otras.

2.2 Evaluación de las propuestas

La dirección deberá definir los procesos, roles y responsabilidades asociados a la evaluación de cada sugerencia, la implementación de acciones surgidas de dicho análisis y el seguimiento de estas.

2.3 Comunicación
La dirección deberá garantizar que se comunique a los involucrados el resultado del análisis de las sugerencias y propuestas.

3. ELEMENTO 3: CALIFICACIÓN, CAPACITACION Y DESEMPEÑO DEL PERSONAL
Objetivo Contar con los procesos que garanticen las competencias de los empleados y de todos los involucrados en tareas o actividades de la compañía, para que realicen las mismas de manera segura, de acuerdo con la estructura organizacional y las responsabilidades.

3.1. Estructura organizacional
Se deberá contar con una estructura que establezca roles y responsabilidades de cada puesto.
La organización identificará los niveles específicos de capacitación, competencia, habilidad y conocimiento que le permitan a los trabajadores realizar las tareas relacionadas con el puesto que ocupa en forma segura, en particular las relacionadas con la seguridad de procesos.

3.2. Capacitación y Entrenamiento
La organización es responsable de:

a. Establecer los requisitos de capacitación para que sus empleados puedan realizar tareas relacionadas con el puesto desempeñado y / o la actividad realizada.
b. Diseñar el programa de competencias y capacitación de acuerdo con el tipo de trabajo y las tareas relacionadas con el puesto desempeñado y / o la actividad realizada.
c. Asegurar que los contratistas establezcan requisitos de capacitación y verificación de competencias, desarrollen sus programas y los cumplan, como se establece en los dos puntos anteriores.
d. Establecer la calificación y capacitación requeridas para realizar las actividades previstas en los procedimientos operativos.
e. Desarrollar los siguientes programas de entrenamiento:
- Entrenamiento Inicial: inducción de la seguridad y el riesgo asociados con las instalaciones, aplicable a todos los empleados al momento del ingreso incluyendo a los visitantes.
- Entrenamiento de desarrollo: Capacitación a los empleados para la ejecución segura de las actividades en las áreas de operación, mantenimiento, inspección y otras. Se incluye los reentrenamientos periódicos cuando fuera necesario.

3.3. Registro de capacitación y verificación:
La organización deberá mantener un registro de capacitación para el desempeño de sus roles y responsabilidades, deberá proporcionar medios para verificar periódicamente el cumplimiento de este requisito, y la trazabilidad de la capacitación, y contar con registros de la efectividad de la capacitación, el entrenamiento, y la verificación de las competencias en función al puesto.

4. ELEMENTO 4: AMBIENTE DE TRABAJO Y FACTORES HUMANOS
Objetivo: Promover un ambiente de trabajo apropiado que considere los factores humanos.

4.1. Ambiente de trabajo y factores humanos.
La dirección deberá asegurar que se consideren los aspectos relacionados al ambiente de trabajo incluyendo los factores humanos en la instalación, sistemas, estructuras y equipos.
Ejemplos de aspectos a considerar son:

a. Competencia y formación
b. Estructura organizacional
c. Cambios organizacionales
d. Comunicaciones críticas de seguridad (cambios de turno, permisos de trabajo)
e. Diseño, interfaces hombres-máquina, gestión de alarmas.
f. Condiciones ambientales
g. Gestión de fatiga
h. Mantenimiento.

5. ELEMENTO 5: GESTION DE CONTRATISTAS

Objetivo: Establecer e implementar criterios de gestión de contratistas, considerando los aspectos de seguridad de procesos durante la selección, el otorgamiento de contratos y la gestión de todas las fases de estos.

5.1. Selección de contratistas

La Organización contemplará la gestión de Seguridad de Procesos en la selección de contratistas, teniendo en cuenta la naturaleza, el tamaño del trabajo y el riesgo que implica. Se considerarán la estructura, los valores, la cultura y la experiencia en Seguridad de Procesos de los potenciales oferentes.

5.2. Otorgamiento del contrato

Durante esta fase se definirán los aspectos y requerimientos de Seguridad de Procesos tales como controles, barreras, permisos, habilitaciones, certificaciones, y competencias, entre otros. Se establecerán las interfases y los documentos "puentes" entre la organización y el contratista para coordinar la aplicación de los requerimientos mencionados. Se emitirán recomendaciones para la adjudicación del contrato en base a la selección de contratistas realizada.

5.3. Ejecución del contrato

La Organización es responsable de asegurar que los aspectos y requerimientos de Seguridad de Procesos identificados en el contrato sean comunicados, comprendidos, implementados y gestionados por todas las partes involucradas durante la ejecución.

Como parte de la gestión la organización deberá:

a. Verificar las competencias requeridas en Seguridad de Procesos
b. Asegurar la formación de contratistas en los riesgos asociados a la operación
c. Realizar evaluaciones periódicas de desempeño del contratista
d. Asegurar que el trabajo se realiza de acuerdo con lo establecido en el plan del contrato

6. ELEMENTO 6: CUMPLIMIENTO DEL MARCO NORMATIVO, PRÁCTICAS Y ESTÁNDARES

Objetivo: Establecer un proceso que permita la correcta y oportuna identificación y comprensión de los requerimientos legales aplicables y normativa técnica con el fin de garantizar que la organización las aplica en sus activos y operaciones.

6.1. Requerimientos Legales

La organización es responsable del cumplimiento de los requerimientos legales vigentes aplicables. Para ello establecerá un mecanismo que permita:

a. Identificar, documentar y actualizar periódicamente los requerimientos legales vigentes y aplicables a las operaciones de la organización
b. Mantener debidamente actualizado el marco legal ante los cambios en la dinámica operativa y organizacional
c. Incorporar los mismos en las políticas, estándares y procedimientos de la organización
d. Mantener debidamente informados a todos aquellos alcanzados por estos requerimientos legales dentro de la organización
e. Verificar el entendimiento y cumplimiento de los requerimientos legales.

6.2. Normativa Técnica

Un sistema de seguimiento de estándares y normativas técnicas proporciona un mecanismo de aseguramiento de la calidad y la seguridad durante las etapas del ciclo de vida de las instalaciones, permitiendo a la organización:

a. Identificar las normativas técnicas de incumbencia
b. Seleccionar y adoptar el conjunto de prácticas o normas a aplicar
c. Mantener debidamente actualizado el conjunto de prácticas y normas adoptadas ante los cambios en la dinámica operativa y organizacional
d. Incorporar los mismos en las políticas, estándares y procedimientos de la organización
e. Mantener debidamente informados a todos aquellos alcanzados por estas prácticas dentro de la organización
f. Verificar su entendimiento y cumplimiento
g. Incluir un proceso de gestión de desvíos definiendo niveles de aprobación.

7. ELEMENTO 7: RELACIONES CON LOS GRUPOS DE INTERES

Objetivo: Contar con un proceso de comunicación y relación de la Compañía con los grupos de interés del entorno donde posea sus activos y opere.

7.1. Identificación de grupos de interés

La Compañía deberá identificar los grupos de interés afectados e involucrados con las actividades que desarrolle la misma en la comunidad. Una efectiva construcción de relaciones no puede suceder a menos que las partes claves interesadas sean identificadas.

7.2. Acciones para la comunicación y relación con grupos de interés

La comunicación con los grupos de interés buscará el desarrollo de las siguientes acciones:

a. Entendimiento del nivel de riesgo de las operaciones de la Compañía.
b. Identificación de las necesidades de las comunidades, para implementar acciones en conjunto.
c. Articular planes de respuesta ante contingencias y acciones de colaboración (Compañía – Grupos de Interés).
d. Entender el ambito de la comunidad para desarrollo de potenciales proveedores en el área.
e. Identificar los tipos de información y mensajes que deben comunicarse para cada grupo de las partes interesadas.
f. Documentar los encuentros, comunicación y acciones desarrolladas.
g. Cumplir con las acciones y compromisos asumidos con los grupos de interés.

PROCESO PRINCIPAL II
GESTIÓN DE RIESGO DE LAS INSTALACIONES

8. ELEMENTO 8: INFORMACIÓN Y DOCUMENTACIÓN DE SEGURIDAD DE PROCESOS

Objetivo: Contar con un sistema de manejo de documentos fundamentales para la gestión de seguridad de procesos.

8.1. Responsabilidades en la gestión de la información

La dirección deberá garantizar que se desarrolle e implemente un sistema de gestión de documentos de Seguridad de Procesos que refleje la condición actual de las instalaciones. Este sistema debe asegurar el adecuado acceso, guarda y actualización de dichos documentos. Los documentos deben describir la tecnología del proceso incluyendo, pero sin restringirse: diagramas de ingeniería, procedimientos operativos, listados de equipos críticos, hojas de datos de equipos.

8.2. Acceso a la información:

La dirección debe garantizar que todo el personal tenga acceso adecuado a la información para la gestión de las distintas actividades, considerando permisos de accesos y protección de la información.

9. ELEMENTO 9: IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Objetivo: Establecer los procesos que garanticen la identificación de peligros, mediante el uso de herramientas reconocidas y bien documentadas para su análisis y evaluación de los riesgos resultantes.

9.1. Identificación de Peligros y Tolerabilidad de Riesgos

El término “Identificación de Peligros y Análisis de Riesgos”, abarca a todas las actividades involucradas en la identificación de peligros y la evaluación de riesgos en las instalaciones a lo largo de su ciclo de vida, para asegurar que el riesgo a las personas, al ambiente, a los activos y a la reputación, sea controlado consistentemente dentro de los criterios de tolerancia al riesgo de la organización.

Dicha tolerancia al riesgo deberá ser definida, normalmente en forma de una “Matriz de Riesgos”, donde se establecen los diferentes niveles de Severidad de los impactos y las Frecuencias de ocurrencia de los eventos, definiéndose las combinaciones aceptables, tolerables e inaceptables para la organización.

Los resultados de los análisis de riesgos deberán ser comunicados y aprobados según procedimientos de la organización, considerando la potencial continuidad del negocio con diferentes niveles de riesgo.

9.2. Metodologías para la Identificación de Peligros

Existen diferentes metodologías para la identificación de Peligros asociados a los procesos productivos e instalaciones. La organización definirá cuál es la metodología apropiada para sus procesos e instalaciones, teniendo en cuenta como mínimo los siguientes lineamientos:

a. Definición del alcance
b. Utilización de documentos de referencia actualizados
c. Consideración de otros análisis de riesgo en la instalación (revisiones anteriores o derivados de la gestión de cambio) o de instalaciones similares
d. Consideración de análisis históricos de incidentes ocurridos en la instalación u otra instalación similar
e. Consideración del diseño, los factores humanos, los ecosistemas, las causas externas y las instalaciones / vecindarios, según corresponda
f. Consideración de un programa de revisión/revalidación de estos con una frecuencia definida.

9.3. Tipos de Análisis y Evaluación de Riesgo

La organización establece los criterios para el análisis y evaluación de riesgos, los cuales pueden ser Cualitativos, Semicuantitativos o Cuantitativos, para una parte o la totalidad de la instalación

o proceso a analizar. Como parte del estudio se deberán definir las acciones a implementar para mitigar, controlar y prevenir los riesgos evaluados dentro de los valores aceptables definidos por la organización.

La identificación y el análisis de riesgos deben ser realizados por un equipo multidisciplinario. El número de personas involucradas y las características de la experiencia de estas personas deben determinarse por el tamaño, la complejidad de la actividad, instalación, operación, empresa y entorno a analizar.

9.4. Documentación: Informe y Resultados

La organización es responsable de mantener durante el ciclo de vida de la instalación la documentación vigente referente a los procesos de identificación, análisis y evaluación de riesgos disponible para su revisión y uso por parte de la operación, partes interesadas o autoridades que así lo requieran.

El equipo de identificación y análisis de riesgos debe preparar un informe completo sobre los estudios que contemple como mínimo los siguientes apartados:

a. Fecha y duración
b. Objetivo y alcance del estudio
c. Identificación de todas las personas que componen el equipo detallando su área de conocimiento y experiencia
d. Descripción de la instalación, parte de la instalación, unidad, sistema o equipo que estará sujeto a estudio
e. Descripción de la metodología utilizada y justificación de su elección
f. Enumeración de toda la documentación utilizada en el estudio
g. Clasificación de riesgos acorde a la matriz de riesgo de la organización
h. Listado de Recomendaciones y conclusiones.

La persona designada por la organización para aprobar el informe de Identificación y análisis de riesgos será el responsable último de que las acciones preventivas y correctivas derivadas de estos estudios, sean monitoreadas y se documente su implementación. Modificar la implementación de estas acciones o rechazarlas debe estar técnicamente justificado.

Toda la información resultante del estudio, como el informe, el listado de recomendaciones y su plan de implementación y seguimiento debe ser considerado como parte de la información y documentación de seguridad de procesos de la instalación y tratado como se indica en el elemento 8 de la presenta Practica Recomendada.

9.5. Revisión de la Identificación y Análisis de Riesgos

La identificación y el análisis de riesgos deben revisarse cuando la instalación sufre modificaciones físicas u operativas y según la frecuencia definida en el punto 9.2. En situaciones en las que no se identifica la necesidad de una revisión del análisis de riesgos, debe haber registros que técnicamente justifiquen no realizar la misma.

10. ELEMENTO 10: INTEGRIDAD MECÁNICA Y ELEMENTOS CRITICOS DE SEGURIDAD DE PROCESOS

Objetivo: Establecer un proceso de gestión de la integridad de las instalaciones que asegure la disponibilidad de los equipos críticos de seguridad de procesos incluyendo la definición de las ventanas de integridad y operación, la definición e identificación de los equipos críticos, sus planes de mantenimiento y el aseguramiento de calidad a lo largo de todo su ciclo de vida.

10.1. Definición de ventanas de integridad y operación

La organización implementará un proceso para conocer, identificar o definir los limites operativos seguros de los equipos, procesos e instalaciones y determinar los controles necesarios para que estos no se excedan.

10.2. Definición e Identificación de elementos críticos de seguridad de procesos

La organización debe establecer criterios para definir e identificar los elementos críticos de seguridad de procesos de las instalaciones de acuerdo con la definición de elemento crítico de este documento.

10.3. Planificación, inspección, prueba y mantenimiento preventivo

La organización deberá:

a. Establecer e implementar planes de inspección, prueba y mantenimiento preventivo, para lograr la integridad mecánica de los "elementos críticos de seguridad de procesos", deberá estar en línea con las recomendaciones de diseño y operación, estándares, y buenas prácticas de ingeniería de los fabricantes y licenciatarios de tecnología.

b. Definir y desplegar procedimientos escritos de inspección, prueba y mantenimiento que contengan instrucciones claras para la realización segura de actividades, por parte de personal entrenado o certificado.

c. Definir y planificar la periodicidad para realizar actividades de inspección, prueba y mantenimiento preventivo y/o predictivo de acuerdo criterios de riesgos.

10.4. Gestión de calidad del proceso de integridad

La organización deberá:

a. Implementar un procedimiento para gestionar la desactivación, inhibición, falla o extensión del período de mantenimiento de los elementos críticos. Incluir como mínimo un análisis de riesgo con niveles de aprobación para cada situación.

b. Instrumentar un proceso de gestión que garantice que los materiales, equipos e instrumentos cumplan con la especificación de diseño y sean comprados, almacenados e instalados de acuerdo con las especificaciones y buenas prácticas.

c. Documentar todas las actividades relacionadas con la integridad mecánica realizadas en la instalación incluyendo manuales, hojas de diseño o cualquier otro documento relacionado con la instalación, sus sistemas, estructuras y equipos como información de seguridad de procesos según lo establecido en el Elemento 8 "Información y documentación de Seguridad de Procesos".

10.5. Monitoreo y Evaluación de Resultados.

La organización deberá instrumentar los medios para:

a. Monitorear el cumplimiento y los resultados de los planes de inspección y pruebas

b. Identificar los "malos actores" y la necesidad de cambio de frecuencia de mantenimiento, diseño o tecnología

11. ELEMENTO 11: PLANIFICACIÓN Y GESTIÓN DE EMERGENCIAS MAYORES

Objetivo: Asegurar la planificación adecuada para el manejo de emergencias que puedan ocurrir durante la operación de la instalación. Desarrollar los recursos necesarios para la gestión y respuesta a situaciones de emergencia.

11.1. Planificación de posibles situaciones de emergencia

La dirección de la organización asegurará que se elaboren y documenten planes de respuesta a emergencias mayores, incluyendo todos los posibles escenarios creíbles, haciendo foco en que dichos planes sean ejecutables y efectivos en el momento en que sean requeridos. Deberán incluirse además emergencias no ocasionadas en el proceso, pero que pudieran afectar adversamente el mismo o bien desencadenar otros escenarios, por ejemplo: desastres naturales como inundaciones, huracanes o tornados y otros.

11.2. Proporcionar recursos que ejecuten el plan

La dirección de la organización debe asegurar que los planes y procedimientos de respuesta a la emergencia tengan asignado un dueño, y que estén definidos roles y responsabilidades claros para ejecutarse y mantenerse, así como también deberán garantizar los recursos materiales para la respuesta a las diferentes emergencias posibles, medios de comunicación efectiva ante diferentes situaciones, y cualquier otro equipo y/o instalación necesarios para la correcta ejecución del plan en caso de ser necesario. Dichos equipos deberán contar con revisiones y pruebas que aseguren su funcionamiento.

11.3. Practicar y mejorar continuamente el plan

Es responsabilidad de la dirección asegurar que los planes de respuesta a emergencias sean ejercitados regular y rigurosamente mediante simulacros y otras actividades, a fin de capturar posibles aprendizajes y oportunidades de mejora. Los mismos servirán para actualizar y/o modificar los planes, y para mantener su vigencia constante, a la vez que refrescar su utilización en campo.

11.4. Entrenar y/o informar, según corresponda, a los empleados, contratistas, comunidad y autoridades locales sobre qué hacer, cómo serán notificados, y cómo reportar una emergencia

La dirección deberá asegurar que todos los empleados y contratistas que prestan servicio en la/s unidad/es operativas, y cualquier otra persona que ingrese a la instalación, sean entrenados respecto a las diferentes emergencias que puedan ocurrir, cómo reportarlas y cómo proceder en cada caso.

Las personas que tengan un rol activo en la emergencia deberán participar además en entrenamientos específicos, y deberán tener un plan de competencias requeridas para dichas tareas.

La dirección también es responsable de comunicar a las autoridades, comunidad y demás partes interesadas qué tipos de emergencias pueden ocurrir, cómo se les dará aviso, y en caso de ser necesario, informarlos sobre las medidas de protección que deberán tomar.

PROCESO PRINCIPAL III
PRÁCTICAS OPERATIVAS

12. ELEMENTO 12: PROCEDIMIENTOS OPERATIVOS

Objetivo: Establecer los requerimientos para desarrollar, implementar y controlar procedimientos de operación, inspección, mantenimiento, abandono y cambio de turno de forma tal de garantizar una operación segura de la instalación y la ejecución consistente de las tareas.

12.1. Actividades que requieren procedimientos

La organización debe desarrollar, implementar y controlar procedimientos escritos para las operaciones, las tareas de inspección, de mantenimiento, de abandono y para los cambios de turnos operativos que se realizan en la instalación.

12.2. Información para documentar

Los procedimientos deben contener instrucciones claras y específicas para la ejecución segura de las tareas. El nivel de detalle se ajustará a las especificidades operativas, la complejidad de las actividades y los riesgos involucrados. Incluyendo cuando fuera necesario la siguiente información,

a. Comentarios aclaratorios, diagramas, fotografías
b. Límites seguros de operación
c. Pasos necesarios para prevenir y corregir desviaciones de los límites seguros de operación
d. Riesgos de la actividad o etapa/paso del procedimiento (emisiones, fuego, explosiones, etc.)
e. Equipo de protección personal (EPP) específico para ejecutar la tarea, precauciones necesarias para evitar la exposición y medidas a ejecutar en caso de contacto físico o exposición.
f. Mención o referencia a las propiedades y riesgos de los insumos y productos manejados o utilizados en la instalación (Hojas de Seguridad del Producto)
g. Otros de utilidad para clarificar y asegurar la ejecución de las tareas en forma segura.

12.3. Validación y revisión

Los procedimientos deben ser escritos y/o revisados por personal calificado y experimentado, deben ser específicos e inequívocos, y en un idioma que pueda comprenderlo quien realizará la tarea. Los mismos deben estar actualizados por lo que deben ser revisados a intervalos regulares o cada vez que se produzca un cambio. Deben estar disponibles en la instalación para todo el personal involucrado.

12.4. Alcance de los procedimientos

Los procedimientos operativos deben contemplar todas las fases de la operación incluyendo operación normal, operación temporal (no rutinaria), puesta en marcha, parada normal o programada, parada de emergencia (incluyendo cuando se requiere la misma) y abandono o parada por períodos largos (hibernación).

12.5. Comunicación y entrenamiento

El personal involucrado en la ejecución de una tarea debe ser informado y capacitado cada vez que se produzca un cambio en un procedimiento que lo involucre.

13. ELEMENTO 13: GESTIÓN DEL CAMBIO

Objetivo: Definir los requisitos que debe considerar el Sistema de Gestión de Seguridad de Procesos para garantizar que los cambios permanentes, temporales o de emergencia que se realicen en las instalaciones cumplan con los requisitos de Seguridad de Procesos establecidos en esta Práctica Recomendada.

13.1 Procedimientos de control

La dirección establecerá e implementará un procedimiento para administrar los cambios que puedan afectar la seguridad operativa.
Este procedimiento debe incluir la definición de cambio, el alcance, roles y responsabilidades y el proceso de gestión para cada cambio especifico.

La Gestión de Cambio debe considerar como mínimo:

a. La descripción del cambio propuesto, incluida la justificación de este
b. La evaluación de los riesgos e impactos del cambio en las actividades antes de la implementación de las modificaciones.
c. La actualización de los procedimientos y la documentación afectada por el cambio
d. La autorización para los cambios propuestos emitida por el nivel de gestión apropiado.
e. La capacitación y comunicación para todo el personal cuyo trabajo se ve afectado por los cambios.
f. La gestión de cambios debe documentarse, archivarse y estar disponible para su consulta.

13.2 Cambios temporales

Los cambios temporales también deben cumplir con los puntos establecidos en la sección anterior, y se debe establecer la duración del cambio temporal, contando con un sistema para gestionar la extensión del cambio.

13.3 Cambios de emergencia

Dada la naturaleza de los cambios de emergencia, la gestión de los mismos podrá tener un tratamiento acelerado y por ende diferenciado, que debe como mínimo contar con etapas de revisión y aprobación por la función responsable de la instalación con anterioridad a la ejecución del mismo.

14. ELEMENTO 14: REVISIÓN DE SEGURIDAD PREVIA A LA PUESTA EN MARCHA (PSSR)

Objetivo: Contar con un proceso de verificación para garantizar una puesta en servicio segura y operación confiable de todas las instalaciones nuevas, modificadas, que hayan estado fuera de servicio o paradas por mantenimiento.

14.1 Proceso de verificación

Se deberá contar con un proceso cuyo alcance y profundidad dependerá de las tareas efectuadas previas a la puesta en marcha. El proceso contemplará tanto la revisión documental como la revisión física en campo.

14.2 Equipo

El proceso debe ser llevado a cabo por un equipo multidisciplinario consistente con el alcance del trabajo. El área operativa es la responsable de la aprobación como dueño de las instalaciones.

14.3 Aspectos a verificar

El proceso debe incluir como mínimo:

a. El cumplimento de las especificaciones de diseño,
b. El cumplimiento de las recomendaciones de estudios de riesgos,
c. La disponibilidad de los procedimientos operativos
d. La disponibilidad de los equipos y procedimientos de respuesta a la emergencia;
e. La disponibilidad y operabilidad de sistemas de seguridad
f. La capacitación y entrenamiento de los responsables de la operación
g. La comunicación a otras áreas o procesos impactados.
h. Las condiciones de seguridad para operar el equipo o la instalación
i. Permisos y/o habilitaciones legales de existir.

14.4 Documentación

Todo el proceso deberá quedar documentado y aprobado. Entre otros deberán documentarse los check-list, las entrevistas, los ítems pendientes y cualquier otra información verificada.

14.5 Ítems críticos

El proceso debe definir que ítems son de cumplimiento imprescindible para la puesta en marcha

15. ELEMENTO 15: PRÁCTICAS DE TRABAJO SEGURO

Objetivo: Establecer e implementar un proceso para gestionar los riesgos de seguridad de procesos asociados a la ejecución de tareas no rutinarias en sus instalaciones definiendo documentación, roles y responsabilidades.

15.2. Documentación

El proceso debe estar documentado y debe incluir los siguientes requisitos mínimos:

a. Un formulario que actúe como Permiso de Trabajo
b. Firma del formulario por parte de los responsables del área y de la tarea según el procedimiento correspondiente.
c. Descripción de la tarea
d. Identificación de peligros y evaluación de riesgos de seguridad de procesos asociados a la tarea y al entorno con su correspondiente nivel de aprobación.
e. Barreras y EPP requeridos para la ejecución de la tarea
f. Vigencia del Permiso de Trabajo
g. Emision, Revalidación, Cancelación y Cierre de un permiso de trabajo
h. Documentos y registros complementarios
i. Un método de habilitación y calificación del personal con roles en el proceso.

15.3. Prácticas de Trabajo Seguro

La organización definirá que tareas requieren de Prácticas de Trabajo Seguro. Como ejemplo se sugiere incluir las siguientes tareas:

a. Espacio confinado;
b. Aislamiento de energías
c. Excavación y apuntalamiento;
d. Trabajo en caliente;
e. Trabajar en sistemas energizados;
f. Izajes y levantamientos de cargas sobre equipos de proceso
g. Apertura (ruptura de estanqueidad o contención), ventilación, drenaje y purga de tuberías y equipos de proceso no rutinarias.
h. Trabajos que involucran fuentes ionizantes.
i. Trabajos en altura.
j. Actividades simultáneas realizadas por distintos ejecutantes.

15.4. Disponibilidad y competencias

Los permisos de trabajo finalizados y cerrados deberán estar archivados y disponibles para consulta en la instalación por un período de guarda que será establecido por cada compañía.
La organización deberá asegurar que todo el personal involucrado en el proceso tenga la formación requerida en función a los roles asignados y cuente con las competencias adecuadas para realizar las tareas.

PROCESO PRINCIPAL IV
APRENDIZAJE Y MEJORA CONTINUA

16. ELEMENTO 16: REVISIÓN Y MEJORA CONTINUA

Objetivo: Contar con un proceso mediante el cual se pueda evaluar el desempeño de los elementos del Sistema de Gestión de Seguridad de Procesos, estableciendo y monitoreando actividades e indicadores que permitan su mejora continua.

16.1 Indicadores y valores objetivo

La organización deberá definir un conjunto de indicadores para los elementos del Sistema de Gestión de Seguridad de Procesos, con la finalidad de evaluar su desempeño respecto a los valores objetivo previamente establecidos. Se deberá considerar para los indicadores definidos:

a. Descripción y clasificación (proactivo, reactivo)
b. Método de medición y cálculo
c. Frecuencia
d. Fuentes de información
e. Sistema de registro
f. Responsabilidades asociadas

La organización deberá asegurar que la información esté disponible para los grupos de interés definidos, se recomienda la visualización en un tablero de control.
Es esperable que un Sistema de Gestión de Seguridad de Procesos maduro cuente con indicadores proactivos y reactivos para cada uno de los elementos.

16.2 Aseguramiento

La organización deberá definir el plan de aseguramiento que cubra todos los elementos del sistema de gestión y que incluya como mínimo:

a. Tipo de actividades a realizar
b. Frecuencia
c. Metodología de ejecución, registro y comunicación
d. Responsables de ejecución y seguimiento del plan
e. Recursos necesarios y competencias requeridas
f. Definición y seguimiento de acciones

El plan deberá considerar diferentes niveles de aseguramiento, tales como revisiones y evaluaciones, internas, entre pares o independientes; incluyendo un programa de visitas o recorridas de la Dirección al sitio o instalaciones operativas.

16.3 Revisión por la Dirección y Mejora Continua

La organización deberá establecer un proceso de revisión que incluya:

a. Alcance
b. Frecuencia y metodología
c. Roles y responsabilidades
d. Registro y documentación
e. Conclusiones y recomendaciones
f. Gestión y seguimiento de las acciones de mejora

Durante este proceso se revisarán los resultados de las actividades de aseguramiento y los indicadores de desempeño.

17. ELEMENTO 17: INVESTIGACIÓN DE INCIDENTES Y APRENDIZAJE DE LA EXPERIENCIA

Objetivo: Establecer con un proceso de gestión de incidentes de seguridad de procesos para registrar, investigar y desplegar acciones de mejora asociadas a los mismos. Adicionalmente, establecer mecanismos para identificar, comunicar y capturar aprendizajes de eventos propios y de la industria.

17.1 Reporte de incidentes

La organización deberá contar con un proceso de registro y reporte de incidentes de seguridad de procesos.
Se debe asegurar la comunicación a las autoridades de aplicación en los casos que correspondiese

de acuerdo con la normativa legal vigente.
La organización deberá definir el nivel de comunicación inicial requerido en base al tipo de incidente.

17.2 Procedimientos de investigación
El proceso de investigación de los incidentes de seguridad de procesos deberá documentarse mediante un procedimiento que debe incluir:

a. Criterios para determinar el nivel de investigación acorde a la magnitud y potencialidad del incidente.
b. Conformación del equipo de investigación (si aplica) y las competencias requeridas de los integrantes, con la asignación de roles y responsabilidades.
c. Lineamientos para conducir la investigación, incluyendo:
preservación de la evidencia física en el lugar del incidente,
programa de entrevistas,
recopilación e identificación de evidencia como documentos, datos, fotografías y registros apropiados en papel o digital del estado del proceso, equipos y sistemas.
d. Técnicas de investigación que permitan identificar las causas de acuerdo con la gravedad del incidente y complejidad del proceso a investigar: diagrama de tiempos, método “5 ¿Por qué?”, árboles lógicos de causas, listado de factores causales, entre otros.
e. Metodología para la identificación y seguimiento de acciones, con definición de responsable y fecha de implementación.
f. Metodología para documentar los resultados de la investigación y establecer mecanismos y alcance de la comunicación interna y externa (si correspondiese), así como el período de guarda de informes de acuerdo con requisitos legales y organizacionales.
La investigación de incidentes debe considerar la evaluación de casos anteriores, así como la recurrencia y frecuencia de eventos similares y debe realizarse considerando los requisitos legales.

17.3 Divulgación y aprendizaje de incidentes
La Organización deberá establecer los mecanismos para identificar los destinatarios del proceso de divulgación, alcanzando a los grupos de interés.
La comunicación no debe limitarse a personal propio, sino a todos los impactados o interesados, generando espacios que permitan el aprendizaje.
Se recomienda establecer vínculos con organismos externos con el objeto de compartir lecciones aprendidas de incidentes mayores de seguridad de procesos, como también replicar acciones de mejora identificadas que ameriten su despliegue en la organización.

18. ELEMENTO 18: AUDITORÍAS
Objetivo: Contar con un proceso mediante el cual se pueda auditar la efectividad y cumplimiento del Sistema de Gestión de Seguridad de Procesos.

18.1 Planificación
La organización deberá elaborar un plan de Auditorias que incluya:
a. Alcance
b. Frecuencia
c. Equipo auditor
Las auditorias podrán ser realizadas por un equipo interno propio de la organización o un equipo externo. Las auditorías deben ser ejecutadas por personal que no tenga responsabilidades asociadas al proceso, sistema o instalación a auditar, y cuyo resultado no conlleve un conflicto de interés entre área auditada y auditor.

Se deberán definir las competencias que deberá tener el equipo auditor.
El plan de auditorías será revisado periódicamente en función del riesgo, complejidad de la instalación y desempeño de las ultimas auditorías.

18.2 Proceso de auditoria
El resultado de las auditorías deberá quedar documentado y ser comunicado al sitio o instalación auditada mediante un informe que incluya:

a. Las no conformidades y los hallazgos
b. Las conclusiones y recomendaciones

18.3 Seguimiento de la Auditoría

El sitio o instalación auditada deberá generar un plan de acción para abordar las no conformidades y observaciones identificadas, priorizando las acciones según el nivel de riesgo para su ejecución, y contar con un registro y documentación del cierre de las acciones.