SISTEMA DE GESTIÓN DE CIBERSEGURIDAD INDUSTRIAL ENFOCADO A LAS TECNOLOGÍAS DE LA OPERACIÓN PARA MITIGAR POSIBLES RIESGOS EN LAS PLATAFORMAS INDUSTRIALES DEL SECTOR MANUFACTURA-TEXTIL

Dominio 3: Estrategia de ciberseguridad industrial

CREADO POR IVÁN DARÍO LOPERA SALCEDO

FECHA DE CREACIÓN: OCTUBRE 2023

APROBADO POR: LA ORGANIZACIÓN

La estrategia de ciberseguridad es un enfoque integral y planificado que la organización adopta para gestionar y mitigar los riesgos asociados con las amenazas cibernéticas y la seguridad de la información. Esta estrategia abarca un conjunto de acciones, políticas, procedimientos y medidas diseñadas para proteger los activos de información, mantener la confidencialidad, integridad y disponibilidad de los datos, y garantizar el funcionamiento ininterrumpido de los sistemas y servicios digitales.

La estrategia de ciberseguridad se apoya en los fundamentos del negocio donde se identifica la estrategia de la compañía y sus necesidades, partiendo de estos, se generan 3 pilares fundamentales a abordar los cuales se describen a continuación:

- *Ámbito del Sistema de Gestión de Ciberseguridad Industrial (SGCI)*
- *Política de Ciberseguridad Industrial*
- *Estructura de Ciberseguridad*

Ámbito del Sistema de Gestión de Ciberseguridad Industrial (SGCI)

El ámbito del SGCI para nuestra organización se centra en fortalecer la disponibilidad, integridad y confidencialidad de nuestros sistemas industriales. Este ámbito abarca aspectos tecnológicos y organizacionales los cuales permiten que nuestras operaciones continúen siendo eficientes, seguras y alineadas a nuestra misión y objetivos estratégicos. El ámbito de aplicación del SGCI involucra a todos los empleados de la organización, contratistas y proveedores.

Política de Ciberseguridad Industrial

La política de ciberseguridad industrial tiene como objetivo proteger los activos industriales críticos, fortalecer la operación continua de la organización y mitigar los riesgos de las tecnologías de la operación (OT). Esta política está enfocada en los siguientes pilares:

- Alcance
- Responsabilidades
- Gestión del riesgo industrial
- Gestión de incidentes
- Segmentación de redes y control de acceso industrial
- Continuidad de los sistemas de operación industrial
- Gestión, mejora y sostenibilidad del SGCI
- Promoción de la cultura de ciberseguridad industrial

Alcance

Esta política aplica y deberá ser cumplida por los empleados de la organización, independiente de su nivel o función, contratistas y proveedores que interactúen con nuestros sistemas o tengan acceso a nuestra información industrial.

El alcance incluye pero no se limita a los diferentes sistemas:

- Sistemas de control de procesos industriales.
- Sistemas de supervisión y adquisición de datos (SCADA).
- Sistemas de automatización de maquinaria y procesos.
- Sistemas de gestión de activos industriales.
- Redes de comunicación industrial.
- Datos confidenciales y de propiedad intelectual.
- Información de clientes y socios comerciales.
- Activos críticos para las operaciones industriales.

Esta política se aplica a todas las ubicaciones de la organización incluyendo:

- Sedes corporativas.
- Plantas de producción.
- Instalaciones de investigación y desarrollo.

- Ubicaciones on-premise y cloud donde se encuentren plataformas o información industrial de la organización.
- Cualquier otra ubicación que utilice sistemas de control industrial o maneje información industrial.

Todos los empleados, contratistas y proveedores están obligados a cumplir con esta política de ciberseguridad industrial en todo momento. El incumplimiento de esta política puede dar lugar a acciones disciplinarias y legales, según corresponda.

Esta política de ciberseguridad industrial se revisará y actualizará periódicamente para asegurar su relevancia y eficacia en un entorno de amenazas en constante evolución.

Responsabilidades

A continuación, se establecen las responsabilidades relacionadas con la política de seguridad industrial de la organización:

Alta dirección:

- Establecer y comunicar la misión, visión, objetivos y el compromiso de la organización con la ciberseguridad industrial y con el SGCI.
- Asignar los recursos necesarios para implementar y mantener el SGCI.
- Revisar, validar y aprobar las políticas y procedimientos relacionados con el SGCI.

Equipo de ciberseguridad OT:

- Diseñar, implementar y mantener las medidas de seguridad industrial.
- Realizar evaluaciones de riesgos y gestión de vulnerabilidades en activos y procesos industriales.
- Supervisar y analizar los registros y eventos de ciberseguridad industrial.
- Coordinar la respuesta a incidentes de seguridad industrial.
- Proponer políticas y guías que permitan mitigar los riesgos de seguridad industrial.

Equipo TI/TO:

- Implementar, operar y mantener medidas técnicas de seguridad, como firewalls, antivirus, segmentación de redes y sistemas de detección de intrusiones.
- Fortalecer los controles de la infraestructura de tecnología de la operación.
- Aplicar parches de seguridad y actualizaciones de software de manera oportuna.
- Monitorear y responder a las amenazas cibernéticas en tiempo real.

Equipo de recursos humanos:

- Coordinar la incorporación y desvinculación de empleados y contratistas, solicitando crear y revocando los accesos no autorizados (altas y bajas de usuarios).
- Socializar las políticas y guías del SGCI.
- Crear planes de cultura respecto a las tecnologías de la operación.

Empleados:

- Cumplir a cabalidad las políticas y procedimientos definidos en el SGCI.

- Utilizar las credenciales de acceso de manera segura y no compartirlas con terceros.
- Informar de inmediato cualquier incidente o brecha de seguridad a la organización a través del área de Seguridad de los equipos TI/TO.

Contratistas y proveedores:

- Cumplir con los estándares de seguridad industrial establecidos por la organización.
- Informar de inmediato cualquier incidente o brecha de seguridad a la organización a través de sus empleados.
- Proporcionar documentación de seguridad industrial según sea necesario.

Gestión del riesgo industrial

A continuación, se comparten los lineamientos respecto a la gestión del riesgo industrial en la organización:

- El área de OT debe identificar y documentar los activos relacionados con las operaciones industriales. Adicionalmente, debe evaluar la criticidad de cada uno de los activos con el fin de determinar la gestión del riesgo industrial.

- Las áreas de IT y OT deben realizar evaluaciones periódicas de las amenazas que puedan afectar los activos críticos industriales, esto incluye amenazas internas y externas.

- Las áreas de IT y OT deben llevar a cabo evaluaciones de vulnerabilidades incluyendo pruebas de penetración, hacking ético, servicios de red team sobre las plataformas y activos industriales con el fin de identificar posibles debilidades en las plataformas o activos industriales y deberá generar el plan de mitigación o remediación de las vulnerabilidades encontradas, este procedimiento se debe realizar por lo menos 3 veces al año.

- Las áreas de IT y OT deben diseñar, contratar y tener documentado los controles que permitan proteger y mitigar los riesgos de seguridad en los activos industriales.

- Las áreas de riesgos, IT y OT deben realizar el análisis de riesgos de los activos y procesos industriales generando así el tratamiento y el seguimiento del plan de gestión de riesgos.

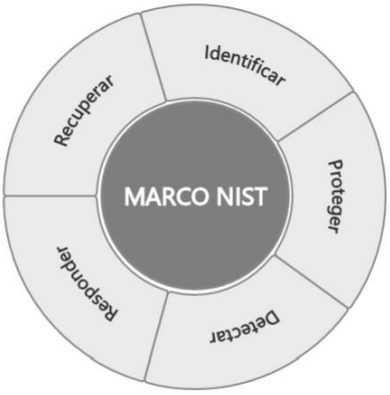
- Las áreas de IT y OT deberán generar e implementar los procedimientos de manejo de incidentes que incluyan la notificación, registro y respuesta adecuada a incidentes de seguridad.

- La organización determinar implementar un equipo de respuesta a incidentes capacitado y establecerá un plan de continuidad del negocio con los resultados de la gestión del riesgo industrial.

Política de Gestión de Incidentes de Seguridad Industrial

El propósito de esta política es establecer un marco de gestión de incidentes de seguridad industrial para identificar, responder y mitigar incidentes que comprometan la seguridad de las operaciones y los activos en la organización. Esta política se basa en el framework de ciberseguridad NIST donde se describen las pautas de seguridad y tiene como objetivo minimizar el impacto de los incidentes y garantizar la continuidad segura de las operaciones industriales.

Tabla 1. Primeros pasos de NIST Marco de ciberseguridad



Nota. Guía de inicio rápido estándar NIST. Fuente: Adaptado [34]

Alcance
Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que trabajan en instalaciones o entornos industriales de la organización y están sujetos a su cumplimiento.

Definiciones
Incidente de Seguridad Industrial: Cualquier evento que tenga el potencial de causar daño a personas, activos, procesos industriales o al medio ambiente, o que comprometa la integridad y seguridad de las operaciones industriales.
Equipo de respuesta a Incidentes de Seguridad Industrial (CSIRT-Industrial): Un grupo de profesionales designados para coordinar y responder a incidentes de seguridad industrial.

Notificación de incidentes:
Cualquier empleado que identifique o sospeche de un incidente de seguridad industrial debe notificar de inmediato al CSIRT-Industrial. La notificación debe incluir una descripción detallada del incidente, su impacto potencial en la seguridad industrial y cualquier información relevante.

Clasificación de incidentes:
El CSIRT-Industrial evaluará cada incidente para determinar su gravedad y clasificarlo de acuerdo con una escala de impacto definida para la seguridad industrial.
Las clasificaciones pueden incluir "Incidente Menor," "Incidente Significativo" y "Incidente Crítico."

Respuesta a Incidentes:

El CSIRT-Industrial coordinará la respuesta a incidentes de seguridad industrial, incluyendo la activación de planes de contingencia y respuesta a emergencias. Se establecerán procedimientos de respuesta específicos para cada clasificación de incidente, con un enfoque en la seguridad de las personas y la protección de los activos industriales.

Notificación a las Autoridades:
Si se determina que un incidente tiene implicaciones legales, regulatorias o de seguridad industrial, el CSIRT-Industrial notificará a las autoridades pertinentes de acuerdo con las leyes y regulaciones aplicables.

Seguimiento y Documentación:
Se llevará un registro de todos los incidentes de seguridad industrial, incluyendo detalles de la respuesta y las acciones tomadas.
La documentación será utilizada para el análisis posterior y la mejora continua de la seguridad industrial.

Cooperación Externa:
La organización colaborará con agencias gubernamentales, organismos reguladores y otras organizaciones industriales para abordar incidentes de seguridad industrial de manera efectiva.

Concienciación y Formación:
Se proporcionará formación en seguridad industrial a los empleados para aumentar su conciencia sobre incidentes y sus responsabilidades en la gestión de incidentes en entornos industriales.

Revisión y Actualización:
Esta política será revisada y actualizada periódicamente para asegurar su relevancia y eficacia en el contexto de la seguridad industrial.

Cumplimiento:
El incumplimiento de esta política de gestión de incidentes de seguridad industrial puede resultar en medidas disciplinarias, incluyendo sanciones laborales y legales, según corresponda.

Esta política permitirá garantizar que la organización esté preparada para responder a incidentes de seguridad industrial de manera eficaz y minimizar los impactos potenciales en la seguridad de las operaciones industriales, la integridad de los procesos y la protección del personal. El CSIRT-Industrial se encargará de coordinar y gestionar la respuesta a los incidentes de seguridad industrial en toda la organización.

Segmentación de redes y control de acceso industrial

La presente política tiene como objetivo fortalecer la seguridad de las tecnologías de operación y deberá ser desarrollada y gestionada por las áreas de IT y OT de la organización:

- Proteger los sistemas de las tecnologías de la operación y los activos críticos de la organización contra amenazas cibernéticas.
- En los sistemas que lo permitan, se debe utilizar autenticación de múltiple factor (MFA) para garantizar la autenticación segura de los usuarios.

- Limitar el acceso a los sistemas de control industrial solo a personal autorizado. Los roles y privilegios de acceso se deben basar en las necesidades laborales de los usuarios, limitando el acceso a lo estrictamente necesario.
- Los permisos de acceso se deben revisar y actualizar periódicamente.

- Identificar, segmentar y proteger las redes de control industrial.

- Implementar medidas de segmentación físico y lógico que permitan mitigar los riesgos de seguridad industrial en el entorno OT.

- Implementar control de seguridad para reducir los riesgos en activos vulnerables, tenerlos identificados y monitoreados.

- Implementar mecanismos de autenticación y autorización para garantizar que solo el personal autorizado tenga accesos a los sistemas industriales.

- Establecer contraseñas robustas que incluyan la rotación regular de contraseñas de los activos industriales.

- Las contraseñas deben cumplir con las políticas de complejidad y ser cambiadas regularmente. Remitirse a la política de contraseñas.

Política de contraseña

La seguridad de las contraseñas es esencial para proteger la información confidencial y los sistemas de la organización. Estas contraseñas deben ser seguras y difíciles de adivinar.

A continuación se establecen los principios y las directrices para crear, gestionar y proteger contraseñas de manera efectiva a nivel de la operación industrial:

- Las contraseñas deben tener al menos ocho caracteres y deben incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
- Las contraseñas no deben incluir información personal, como nombres propios, fechas de nacimiento o palabras fáciles de adivinar.
- Se requiere que los empleados cambien sus contraseñas cada 90 días.
- Los usuarios no pueden reutilizar ninguna de sus 3 contraseñas anteriores.
- Las contraseñas no deben almacenarse en texto plano en ningún sistema o documento. Deben protegerse adecuadamente mediante técnicas de cifrado o hash. Para esto se deberá definir las herramientas que permitan garantizarlo.
- Se debe evitar compartir contraseñas. Cada usuario debe tener sus propias credenciales de inicio de sesión.

Todos los empleados y contratistas deben cumplir con esta política de contraseñas. El incumplimiento de esta política puede resultar en medidas disciplinarias, incluida la suspensión o la terminación de las relaciones laborales.

Esta política de contraseñas se revisará y actualizará periódicamente para reflejar las mejores prácticas respecto a los lineamientos de las políticas de contraseñas.

Continuidad de los sistemas de operación industrial

La continuidad y resiliencia de los sistemas de operación industrial son esenciales para asegurar la disponibilidad, la integridad y la confidencialidad de nuestros procesos y sistemas críticos. Estos procedimientos garantizar la continuidad y resiliencia de los sistemas de operación industrial en la organización.

A continuación, se comparten los objetivos de la continuidad de los sistemas de operación industrial:

- Mantener la continuidad de las operaciones industriales en situaciones de crisis, como desastres naturales, fallas técnicas o amenazas cibernéticas.
- Minimizar el tiempo de inactividad y los impactos operativos en caso de interrupciones.
- Establecer un marco de respuesta eficaz para la recuperación y restauración de sistemas y procesos.

Para lograr los anteriores objetivos se debe:

- Mantener el inventario actualizado de los sistemas de operación industrial considerados cómo riesgo crítico o de alto valor para la organización.

- Realizar una evaluación de impacto del negocio con el fin de identificar los sistemas y procesos más críticos y los requisitos de continuidad.

- Desarrollar un plan de continuidad y resiliencia que permita habilitar la infraestructura crítica en escenarios de crisis, este plan debe incluir procedimientos de recuperación, roles y responsabilidades y los contactos de emergencia.

- Validar por lo menos una vez al año el anterior plan con el fin de para garantizar su efectividad y capacitar al personal que interviene en su ejecución, adicionalmente se debe establecer una ruta de lecciones aprendidas que permita tener documentado las situaciones que se presenten durante la ejecución del plan y cómo fueron solventadas.

- Establecer un equipo de respuesta a incidentes el cual estará disponible las 24 horas del día con el fin de poder gestionar los incidentes y coordinar la recuperación del sistema.

- Implementar un procedimiento de notificación para los incidentes o interrupciones en la operación industrial.

- Desarrollar un plan de capacitación al personal de la organización donde se expongan los procedimientos de continuidad y resiliencia, así como su papel en cada uno de los ejercicios.

- Revisar constantemente esta política de continuidad y resiliencia de sistemas de operación industrial periódicamente para asegurar su eficacia y actualizarla según sea necesario.

- Establecer la mejora continua de los diferentes planes y procedimientos definidos en la presente política con base en las lecciones aprendidas y los ejercicios de prueba.

Gestión, mejora y sostenibilidad del SGCI

Para garantizar el desarrollo y mantenimiento eficiente del Sistema de Gestión de Ciberseguridad Industrial (SGCI), la organización respalda la asignación adecuada de los recursos, la documentación y promueve la comunicación interna y externa, para lo cual se establece que el área de recursos humanos en conjunto con el área OT deberán validar y evaluar las siguientes capacidades:

- Identificar las competencias necesarias del personal para gestionar el sistema y ejecutar las labores necesarias para garantizar la correcta aplicación y verificación del sistema de gestión.
- Asegurar que el personal posea las competencias requeridas, basándose en su educación, formación y experiencia.
- Tomar medidas, cuando sea necesario, para adquirir las competencias necesarias y evaluar su efectividad.
- Mantener un registro documentado que demuestre la competencia del personal.
- Fomentar la concienciación en todo el personal acerca de la política de ciberseguridad, su contribución individual a la eficacia del SGCI y las implicaciones de las no conformidades con el SGCI.
- Incluir toda la documentación que la organización considere relevante para respaldar el SGCI en el sector manufactura textil.
- Definir el contenido que debe ser comunicado y designar a los responsables de estas comunicaciones.
- Planificar las comunicaciones relacionadas con el SGCI.
- Establecer procesos efectivos de comunicación que permitan la fluidez y la efectividad en la difusión de información crítica.

La gestión de la documentación dentro del Sistema de Gestión de Ciberseguridad Industrial (SGCI) es crucial para garantizar el desarrollo y el mantenimiento del sistema, es por esto que la documentación debe estar controlada y debe garantizar los siguientes frentes:

- Garantizar que la documentación esté disponible y sea apropiada para su uso en el momento y lugar necesarios en las operaciones industriales.
- Salvaguardar la documentación de manera adecuada contra amenazas como la pérdida de confidencialidad, el uso indebido o la alteración de su integridad, entre otras posibles vulnerabilidades.
- Definir mecanismos del cómo se distribuirá la documentación, cómo se recuperará cuando sea necesario y quiénes tendrán acceso a ella de manera adecuada.
- Determinar los métodos de almacenamiento que aseguren la integridad y la disponibilidad de la documentación durante su ciclo de vida.
- Especificar el período durante el cual la documentación se mantendrá y cómo se eliminará o archivará apropiadamente al final de su utilidad.

La organización generará continuamente planes de auditorías internas desde el área de Auditoría, estas auditorías deberán cumplir con los siguientes aspectos:

- Compartir el plan de auditoria considerando la importancia de los procesos y áreas que serán auditados.
- Los auditores designados deben asegurar que las auditorías se realicen de manera objetiva e imparcial, evitando auditar su propio trabajo.
- Establecer claramente los criterios y el alcance de la auditoría.
- Los resultados de la auditoría deben comunicarse de manera efectiva a la alta dirección, asegurando que estén al tanto de cualquier hallazgo significativo.
- Las responsabilidades en torno a las auditorías internas deben estar definidas claramente, incluyendo la planificación, los requisitos, la presentación de resultados y la gestión de registros.

La alta dirección de la organización es responsable de garantizar que las áreas auditadas tomen las acciones necesarias para abordar cualquier no conformidad identificada durante la auditoría interna y que se presenten explicaciones claras sobre las causas de dichas no conformidades. Además, se debe llevar a cabo un seguimiento de las acciones realizadas, incluyendo una verificación de los resultados obtenidos.

Promoción de la cultura de ciberseguridad industrial

La promoción de la cultura de la ciberseguridad industrial en la organización busca crear una mayor concienciación entre los empleados sobre la importancia de proteger los recursos y sistemas de la organización contra posibles amenazas cibernéticas. En este aspecto, la organización define los siguiente numerales los cuales deben ser cumplidos por el área de recursos humanos y las áreas que intervengan en la consecución de la promoción de la cultura ciber-industrial:

- Desarrollar planes de formación en ciberseguridad para el personal que opere las tecnologías de la operación.
- Desarrollar planes de formación en ciberseguridad para el personal que opere las tecnologías de la información.

Para lograr la ejecución de los anteriores planes, el área de recursos humanos deberá crear o contratar materiales educativos y de concienciación tales como presentaciones, infografías, videos, folletos, plataformas de evaluación, entre otros, que expliquen los conceptos básicos y avanzados de la ciberseguridad industrial, los riesgos asociados y las medidas de protección que deben ser tomadas. Este plan deberá ser planificado y desarrollado por niveles, de acuerdo a las competencias de los empleados y su rol en la compañía.

Los anteriores planes y el desarrollo de las actividades deberán ser comunicados a través de la intranet, carteleras digitales y correos electrónicos a los empleados.

Posterior a la aplicación de los planes de concientización, el área de recursos humanos deberá realizar la medición de la promoción de la cultura de ciberseguridad industrial, para esto debe generar mecanismos de evaluación que ayuden a identificar las oportunidades de mejora de los empleados frente a los temas evaluados y definir y asignar un plan de acción.

Las acciones de formación y concienciación deben ser continuas en el tiempo para garantizar la retención de conocimientos y fomentar las prácticas de seguridad industrial en los empleados.

- **Estructura de Ciberseguridad**