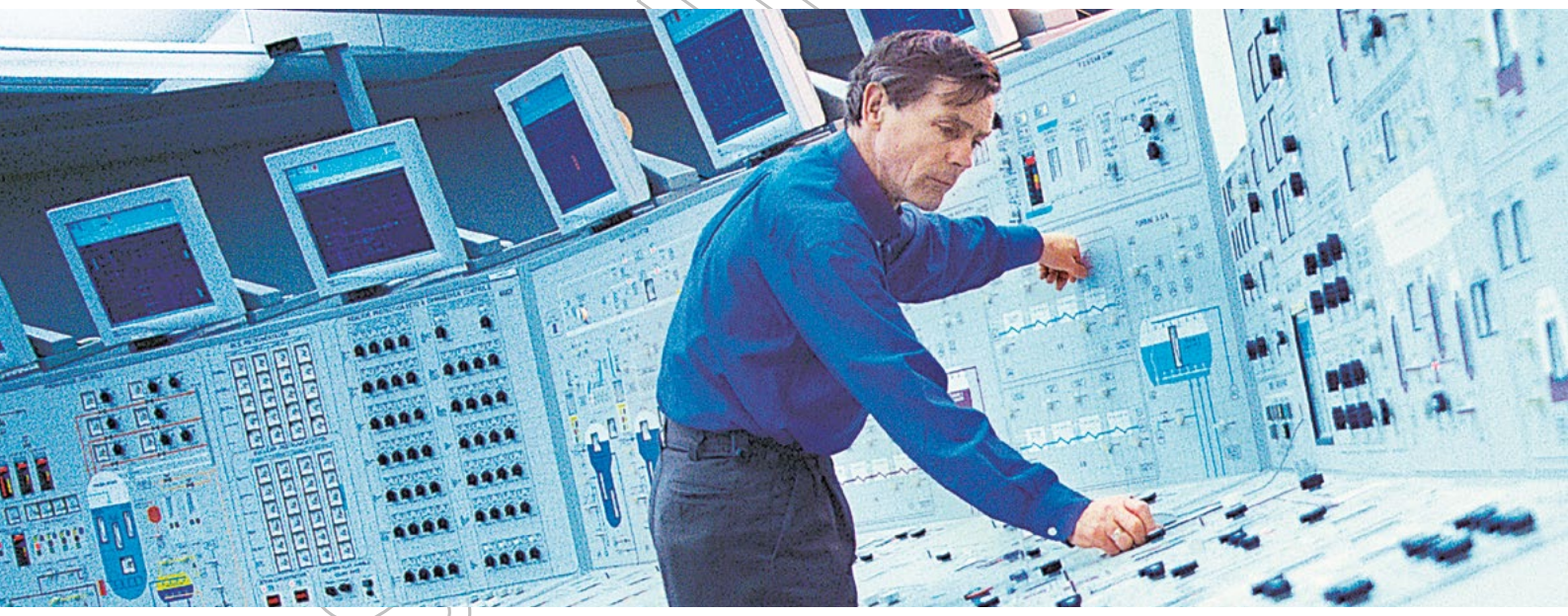
CENTRO DE CIBERSEGURIDAD INDUSTRIAL

Sección Española

BASQUE CYBERSECURITY CENTRE

GUÍA SGCI PARA EL RESPONSABLE DE CONSTRUIR UN SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

Esta Guía ha sido elaborada por el CCI en colaboración con ISA Sección Española.



Primera edición: marzo de 2016 ISBN: 978-84-942379-8-0
Segunda edición: agosto 2018 ISBN: 978-84-947727-5-7

El Centro de Ciberseguridad Industrial (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la Sociedad actual, como puntales del estado del bienestar.

CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

ISA Sección Española (http://www.isa-spain.org/) es una asociación profesional sin ánimo de lucro a la que pertenecen profesionales interesados en la medida, automatización y gestión de procesos, y que forma parte de ISA (The International Society of Automation) una organización internacional sin ánimo de lucro enfocada a ayudar a sus más de 30.000 miembros repartidos por todo el mundo y a todos los profesionales del sector. Se encarga también del desarrollo de estándares relacionados con el mundo de la instrumentación, el control y la automatización en general. Asimismo, proporciona formación y publica numerosos libros, revistas y artículos técnicos para divulgar el conocimiento en todo el mundo.

Maiquez, 18 · 28009 MADRID
+34 910 910 751
info@CCI-es.org
www.CCI-es.org
blog.CCI-es.org
@info_CCI

Consejos

Alt+flecha izquierda para volver a la vista anterior

Haz click en nuestro icono y visita nuestra web

El BASQUE CYBERSECURITY CENTRE (en adelante, BCSC), es una iniciativa que se enmarca en la SOCIEDAD PARA LA TRANSFORMACIÓN COMPETITIVA-ERALDAKETA LEHIAKORRERARO SOZIETATEA, S.A. (en adelante Grupo SPRI), sociedad dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

El BCSC es un instrumento del Gobierno Vasco para elevar la cultura de la ciberseguridad en la sociedad vasca y aspira a erigirse como punto de encuentro entre oferentes y demandantes de servicios especializados, generando con ello una oportunidad para la innovación, potenciando la competitividad de las empresas y facilitando que la ciudadanía desarrolle hábitos para una actividad digital más segura.

Para alcanzar sus objetivos, el BCSC se define como una iniciativa transversal que desde su inicio involucra a cuatro Departamentos del Gobierno Vasco, el ya antes citado de Desarrollo Económico e Infraestructuras, el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación.

La actividad del centro incluye proyectos de investigación, iniciativas de emprendimiento y colaboración coordinada con otros agentes competentes a nivel estatal e internacional. No en vano se trabaja en estrecha colaboración con agentes de la Red Vasca de Ciencia Tecnología e Innovación que forman parte de su Comité Permanente.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución proyectos de colaboración entre actores complementarios en los ámbitos de la innovación tecnológica, de la investigación y de la transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

El BCSC ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CSIRT, por sus siglas en inglés “Computer Security Incident Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar su capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca.

Parque Tecnológico de Álava
+34 945 010 059
info@bcsc.eus
www.basquecybersecurity.eus
@basquecscentre
www.linkedin.com/company/basque-cybersecurity-centre/

0 **INTRODUCCIÓN** 8

1 **DOMINIO 1:**
DEFINICIÓN DE UNA ESTRATEGIA DE CIBERSEGURIDAD INDUSTRIAL 20

2 **DOMINIO 2:**
GESTIÓN DE LOS RIESGOS PARA LA CIBERSEGURIDAD INDUSTRIAL 36

3 **DOMINIO 3:**
PROMOCIÓN DE UNA CULTURA DE LA CIBERSEGURIDAD INDUSTRIAL 56

4 **DOMINIO 4:**
ESTABLECIMIENTO DE MEDIDAS DE CIBERPROTECCIÓN EN INSTALACIONES INDUSTRIALES 68

5 **DOMINIO 5:**
GARANTÍA DE RESILIENCIA Y CONTINUIDAD DE LOS SISTEMAS DE OPERACIÓN 100

6 **DOMINIO 6:**
GESTIÓN, REVISIÓN, MEJORA Y SOSTENIBILIDAD DEL SGCI 120

7 **GLOSARIO** 132

8 **BIBLIOGRAFÍA** 133

9 **ANEXOS** 134

10 **AUTORES Y COLABORADORES** 135

0

Introducción

CONTENIDOS

ANTECEDENTES

MOTIVACIÓN, OBJETIVO Y FUENTES DE REFERENCIA

MOTIVACIÓN

OBJETIVO

FUENTES DE REFERENCIA

MARCO DE REFERENCIA DEL SGCI

ANTECEDENTES

La economía hoy está conectada globalmente. La competencia de las empresas ya no se limita exclusivamente a otras organizaciones que operan físicamente en el mismo territorio. Hoy cualquier organización, independientemente de su tamaño compite con organizaciones internacionales. Salvo excepciones, cualquier cliente de una organización podría adquirir el mismo tipo de producto a una empresa de cualquier otra parte del mundo, todo ello gracias a la tecnología y a las nuevas plataformas virtuales de comercio y su capacidad logística, por ello, aquella empresa industrial que pretenda sobrevivir deberá adaptarse al nuevo hábitat global y digital. En este escenario, los sistemas de información (entre los cuales cabe incluir los sistemas de automatización y control industrial), adolecen de una serie de vulnerabilidades que los exponen a un creciente número de amenazas, internas o externas, y sus consiguientes riesgos. La materialización de dichas amenazas en cualquiera de sus más variadas formas (negligencia o error, ya sean de naturaleza voluntaria o intencionada; fallo; fraude; espionaje; sabotaje; vandalismo; e, incluso, accidente, debido a razones de fuerza mayor o a causas naturales) puede motivar todo tipo de incidentes de seguridad que afecten a los activos de información de una organización.

La transformación digital está penetrando hasta el último rincón, ejemplo de ello es Internet de las Cosas, así como la fuerte tendencia “SMART” de todo, ciudades, hospitales, coches, fabricas e incluso de naciones.

El modelo de negocio que soporta los procesos industriales está ahora en plena evolución, denominándose Industria 4.0 en el ámbito europeo. Este modelo persigue que las organizaciones industriales puedan competir logrando una mayor flexibilidad en la producción, así como sostenibilidad o resiliencia mediante la optimización de los recursos y la capacidad para recuperarse frente a desastres y alteraciones en la operación.

Esta transformación digital en la que estamos inmersos es una gran oportunidad para la industria, así como para la ciberseguridad industrial, cuyo progreso en concienciación y experiencias es creciente, y deberá facilitar que los requisitos de ciberseguridad se incorporen desde el diseño de las tecnologías, en sus nuevas arquitecturas y también en su gestión para dar

soporte a la interoperabilidad, cada vez mayor, entre los sistemas de operación y de información que están adoptando un modelo de industria 4.0.

Siendo esta circunstancia común a todos los sistemas de información, las peculiaridades que presentan los sistemas de automatización y control industrial hacen que su exposición al riesgo se diferencie, también, de la que puedan sufrir el resto de sistemas de información; los llamados sistemas de información corporativos. Como parte de tales peculiaridades se tendrían:

- En la actualidad, cada vez más procesos productivos de carácter industrial están automatizados (informatizados); esto es, sustentados en algún tipo de solución o equipamiento automatizado (informatizado). Ello ha permitido mejorar su eficiencia y, consecuentemente, aumentar la productividad de las organizaciones. Y a ello ha contribuido la evolución de las tecnologías de la información y las comunicaciones y su integración en el mundo industrial. Sin embargo, al tiempo que se han sumado nuevas capacidades tecnológicas a los entornos industriales, también se han introducido vulnerabilidades y creado dependencias que, en muchas ocasiones, permanecen peligrosamente inadvertidas.
- La propia naturaleza de los sistemas de automatización y control industrial dificulta su mantenimiento permanente (o cuasi-permanente) y, por ende, la identificación y eliminación de sus vulnerabilidades. Así, las exigentes necesidades de disponibilidad del proceso industrial impiden el parcheo y actualización continuados de los sistemas de control que lo sustentan, abocando a estos últimos al paulatino y creciente deterioro de su seguridad. Ello es motivo de la existencia, en las instalaciones industriales, de sistemas de control insuficientemente preparados para afrontar los retos de seguridad que plantean las tecnologías de hoy.
- El entorno sociopolítico cada vez se muestra más interesado en las capacidades del ciberespacio como elemento estratégico, en un contexto -como se ha señalado- en el que la integración de las tecnologías de la información y las comunicaciones con el mundo industrial ha provocado que gran parte de los sistemas de control estén, hoy, integrados en ese nuevo espacio. Ello, unido al hecho de que un gran número de las instalaciones industriales existentes carecen de mecanismos para realizar una gestión eficaz de la ciberseguridad de sus sistemas, agudiza los riesgos sobre el correcto funcionamiento de los procesos productivos (procesos de negocio) más críticos; habida cuenta de la relevancia que han adquirido los sistemas de automatización y control industrial para el funcionamiento de dichos procesos.
- La carencia de una cultura de la ciberseguridad en los entornos industriales, dificulta que los individuos implicados en su diseño, adquisición, construcción, puesta en marcha, operación, mantenimiento y desmantelamiento, sean capaces de gestionar los problemas potenciales, de naturaleza cibernética, a los que se han de enfrentar.
- El esmero, la dedicación y la rigurosidad alcanzados en la prevención de riesgos y la protección de la seguridad física en las instalaciones industriales no ha tenido, hasta ahora, su correspondencia en la gestión del riesgo para la ciberseguridad.
- Apenas existen normas comúnmente aceptadas relativas a la seguridad de los sistemas de automatización y control industrial, ya que la gran mayoría de las normas de seguridad tecnológica existentes no tienen en cuenta las peculiaridades del entorno industrial, en general, y de este tipo de sistemas, en particular.
- Finalmente, tampoco existen modelos genéricos de gestión de la seguridad en entornos industriales que ofrezcan un planteamiento aplicable, de forma transversal, a cualquier tipo de sector industrial, empresa u organización. Si bien pueden encontrarse documentos de buenas prácticas, éstas suelen ir dirigidas a sectores específicos y a grandes organizaciones.

Introducción
Motivación, Objetivo y Fuentes de Referencia

MOTIVACIÓN, OBJETIVO Y FUENTES DE REFERENCIA

Motivación

La ya aludida escasa disponibilidad de referencias normativas que traten, de manera particular, la gestión de la ciberseguridad en los sistemas de automatización y control industrial invita al desarrollo de nuevas directrices específicas, y diferenciadas, para un tratamiento eficaz, eficiente y continuado de los riesgos sobre la disponibilidad, la integridad y la confidencialidad de las operaciones y de la información gestionadas por tales sistemas, en línea con las necesidades estratégicas de la organización.

Asimismo, y a fin de favorecer la aplicación práctica de las citadas directrices, nada mejor que dotarlas de un carácter formal -por ejemplo, bajo el formato de lo que podría dar en llamarse un **"sistema de gestión de la ciberseguridad industrial"**- que tenga en cuenta las siguientes premisas:

- Independencia e integración. Todo sistema de gestión [de la ciberseguridad industrial] que se proponga, aun siendo compatible con otros sistemas de gestión ya existentes en la organización, gozará de una cierta autonomía desde el punto de vista de su implantación. De ese modo, se facilitará su puesta en marcha cuando la madurez, en ciberseguridad industrial, de otros departamentos de la organización resulte insuficiente; e, incluso, cuando el objetivo último de la integración de los diferentes sistemas de gestión esté presente.
- Agilidad y operatividad. Todo sistema de gestión [de la ciberseguridad industrial] que se proponga deberá, igualmente, primar la operatividad, al menos inicialmente, potenciando la adopción de medidas que cubran requisitos de ciberprotección básicos sobre los sistemas de automatización y control industrial; requisitos que podrán ir ampliándose, posteriormente.

El Centro de Ciberseguridad Industrial (CCI), consciente de la conveniencia de disponer de una especificación que contemple la implantación de sistemas de gestión de la ciberseguridad en las empresas del sector industrial, ha abordado la elaboración de la presente **"Guía para el responsable de construir un SGCI (Sistema de Gestión de la Ciberseguridad Industrial)"**, que parte de la presentación del marco de referencia general del sistema y, a continuación, desarrolla, a lo largo de una serie de seis capítulos aquellos dominios que conforman y desarrollan dicho marco general.

Objetivo

El objetivo final es poner a disposición de los responsables de las organizaciones industriales, de los de sus procesos productivos, de los de la operación de tales procesos, de los de las áreas técnicas, de los de las áreas de ciberseguridad y, en suma, de quienes se vean afectados por el funcionamiento de los sistemas de automatización y control industrial de una instalación, cuantos recursos y elementos sean necesarios para llevar a cabo una gestión eficaz, eficiente y continuada de los riesgos para la ciberseguridad asociados a dichos entornos:

Fuentes de Referencia

A la hora de desarrollar esta guía para la construcción de un SGCI, y con el fin de satisfacer el principio de la compatibilidad y, con él, la premisa de la integración, mencionada más arriba, se han tomado en consideración las siguientes fuentes de referencia:

- *IEC 62443-2-1:2010. Industrial communication networks. Network and system security. Part 2-1: Establishing an industrial automation and control system security program. (ISA-62443-2-1. Requirements for an IACS security management system).*
- *IEC 62443-2-2 Ed. 1.0. Network and system security. Part 2-2: Operating a manufacturing and control systems security program. (ISA-62443-2-2. Implementation guidance for an IACS security management system).*
- *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements.*
- *ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls.*

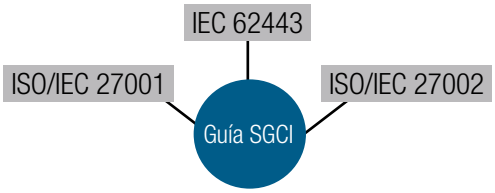


Figura 1: Principales fuentes de referencia de la "Guía para la Construcción de un SGCI"

Introducción
Marco de Referencia del SGCI

MARCO DE REFERENCIA DEL SGCI

El alcance de la propuesta para la construcción de un SGCI, recogida en esta guía, queda delimitado por un **marco de referencia** constituido por los seis dominios que se describen a continuación:

Figura 2: Marco de referencia del SGCI

› **Dominio 1: Definición de una Estrategia de Ciberseguridad Industrial.** Con carácter general, la ciberseguridad industrial y su estrategia se reconocen como una consecuencia de la estrategia corporativa, con la que estarán integradas y de la que formarán parte. Se hará, por ello, necesario observar los fundamentos del negocio como punto de partida de toda iniciativa de ciberprotección de los activos de carácter industrial (incluidos los procesos) de que disponga la organización.

- Fundamentos del negocio.
  - La visión, misión, metas y objetivos de la organización, así como su contexto, e interrelaciones, cultura, micro-políticas y particularidades constituirán el punto de partida para la construcción del SGCI. El conocimiento de esa coyuntura particular permitirá determinar los requisitos de ciberseguridad de la organización y los riesgos que está dispuesta a asumir. Permitirá, asimismo, identificar y delimitar el alcance del propio SGCI.
- Alcance del sistema de gestión de la ciberseguridad industrial.
  - El perímetro de aplicación del SGCI vendrá marcado, en cada caso, por las prioridades que determine el negocio en función de sus necesidades (requisitos) de protección.
- Política de ciberseguridad industrial.
  - Las directrices generales en materia de ciberprotección industrial habrán de contar con el impulso y el respaldo de los responsables de la organización al más alto nivel, comenzando por su consejo de administración u órgano equivalente, y deberán quedar recogidas en un documento -preferentemente breve- que no sea sino reflejo de los valores que mueven a la empresa en el medio y largo plazo. La política de ciberseguridad industrial tendrá, por ello, carácter permanente. (Por contra, las normativas específicas que desarrollen esta política sí tendrán un carácter más dinámico. A ellas hace referencia, principalmente, el dominio 4, más adelante).
- Organización para la ciberseguridad industrial.
  - En el marco de este primer dominio deberán especificarse, igualmente, los patrones de rendición de cuentas, de derecho a la toma de decisiones y de otras responsabilidades en materia de ciberseguridad industrial. Patrones en los que quedarán reflejados los diversos actores presentes en los distintos niveles de la organización; particularmente, dentro del alcance fijado para el SGCI.

› **Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial.** Se propone un método sencillo que facilite a los responsables de la operación de una planta, llevar a cabo evaluaciones del riesgo vinculado a la ciberseguridad industrial de su instalación.

- Metodología de análisis del riesgo.
  - Como se ha indicado, la guía tratará de proponer una aproximación sencilla a las actividades de evaluación de riesgos de naturaleza cibernética. A dicho fin, se hará un breve recorrido por los principales elementos a tener en cuenta en todo análisis de riesgos, particularizándolos para el entorno industrial.
- Identificación de activos.
  - El punto de entrada al análisis habrá de ser, necesariamente, la identificación e inventariado de los activos clave contenidos en el alcance del análisis planteado. Dicha identificación se realizará a partir de un modelo desarrollado durante la etapa de delimitación del alcance.
- Listado de vulnerabilidades en el ámbito industrial.
  - El concepto de vulnerabilidad hace referencia a cualquier punto débil de un activo y tiene un carácter intrínseco al mismo. Las vulnerabilidades, por sí solas, no son peligrosas; lo serán ante la presencia de una amenaza que pueda explotarlas. Se proporciona un catálogo de vulnerabilidades propias de los entornos industriales que facilitará la asignación, de forma sencilla, de ciertos grupos de vulnerabilidades a aquellos activos que, previamente, se hayan identificado como críticos.
- Listado de amenazas en el ámbito industrial.
  - El concepto de amenaza se interpreta como una condición que se da en el contexto de los activos, y de sus vulnerabilidades, y que tiene el potencial de afectar a los primeros a través de las segundas. Se vuelve a ofrecer un nuevo catálogo, donde figuran las amenazas más habituales, propias del ambiente industrial.

› **Dominio 3: Promoción de una Cultura de la Ciberseguridad Industrial.** El tercer dominio de esta guía trata, de forma específica, cuanto tiene que ver con el personal, su implicación y formación, en materia de ciberseguridad, en el contexto industrial.

- Selección de medidas de protección.
  - Se establecerá el ámbito y el propósito general de aquellas medidas que estén orientadas a determinar la manera en que el personal que gestiona, opera y mantiene los sistemas de automatización y control industrial haya de desarrollar dichas actividades. El objetivo será garantizar la protección del propio personal, de los sistemas y de las instalaciones.
- Establecimiento de una normativa de ciberseguridad del personal.
  - La primera de las referidas medidas será el establecimiento de una normativa específica para el personal, la cual habrá de contemplar aspectos como: funciones y obligaciones del personal (incluido el establecimiento de acciones disciplinarias); comprobación de los antecedentes personales; segregación de funciones; asignación y delegación de autorizaciones; etc.
- Formación y concienciación.
  - Se reconoce la criticidad de ambos aspectos para garantizar la ciberseguridad de las instalaciones industriales. Ello es debido a que aquella depende, en gran medida, de las acciones realizadas por el personal durante el desempeño de su actividad profesional.

› **Dominio 4: Establecimiento de Medidas de Ciberprotección en Instalaciones Industriales.** Como desarrollo de la política general de ciberseguridad industrial abordada en el primer dominio de esta guía, y aparte de otras normativas de seguridad específicas, como la de personal, contemplada en el dominio 3, se planteará la elaboración de una serie de medidas en ámbitos concretos como los relativos a: clasificación de activos y datos de control de proceso; control de acceso lógico a los sistemas de automatización industrial; seguridad física y del entorno; protección de las redes de comunicaciones; protección del software de control industrial; o protección en las relaciones con terceros.

- Consideraciones generales sobre medidas de clasificación y protección de datos e información en el contexto de la automatización industrial.
  - Los diferentes sistemas de control, presentarán diferentes criticidades. De igual modo, a la información y los datos que tratan en su operativa normal corresponderán grados de sensibilidad y criticidad diferentes. Debe, por tanto, realizarse una identificación y clasificación de tales datos, y de sus propietarios, que permita definir un conjunto adecuado de niveles de protección y favorezca el incremento del grado de implicación individual en la misma.
- Consideraciones generales sobre medidas de control de acceso lógico a los sistemas en el contexto de la automatización industrial.
  - El acceso lógico a los sistemas de control industrial debe hacerse sobre la base de los requisitos del proceso industrial objeto de dicho control y, por extensión, de la propia organización, resumidos en el principio de "la necesidad de conocer". Se promoverá la puesta en marcha de procedimientos formales de asignación de derechos de acceso a los referidos sistemas y equipos, que habrán de seguir el citado principio.
- Consideraciones generales sobre medidas de seguridad física y del entorno en el contexto de la automatización industrial.
  - Deberá recoger las medidas orientadas a evitar los accesos físicos no autorizados a las áreas donde estén albergados los sistemas de control; así como cualquier daño o interferencia en la operativa de la instalación.
- Consideraciones generales sobre medidas de protección de las redes de comunicaciones en el contexto de la automatización industrial.
  - Las comunicaciones a través de redes de datos son, con toda seguridad, un elemento crucial, tanto por su potencial como habilitadoras de la automatización del proceso industrial, como por el peligro que pueden suponer en tanto que puerta de entrada de posibles conexiones no deseadas. Consecuentemente, en el marco de este subdominio se propondrá la elaboración de una serie de directrices (normas) que tengan en cuenta los distintos niveles de conectividad presentes en una instalación industrial y que promuevan medidas como la segmentación de redes u otras.
- Consideraciones generales sobre medidas de protección del software en el contexto de la automatización industrial.
  - Las nuevas soluciones de control industrial habrán de incorporar los requisitos de ciberseguridad pertinentes y alineados con las necesidades de la instalación u organización. Las soluciones antiguas (basadas en software antiguo) deberán, además, ajustarse a unos controles y contramedidas específicos, como los relativos a la obsolescencia de dicho software, que en el entorno industrial adquieren una relevancia particular.
- Consideraciones generales sobre normativa de ciberseguridad en las relaciones con terceros en el contexto de la automatización industrial.
  - El complejo panorama de la automatización actual (múltiples soluciones, múltiples proveedores; fabricantes, integradores; etc.) hace necesario extender el rigor del marco de ciberprotección más allá de los confines de la instalación o de la empresa. Esta circunstancia deberá quedar reflejada oportunamente en el SGCI.

› **Dominio 5: Garantía de Resiliencia y Continuidad de los Sistemas de Operación.** En el contexto de

esta guía la resiliencia se interpreta como aquella capacidad de que goza la organización para resistir, responder y recuperarse ante posibles incidentes que afecten a los sistemas de automatización y control industrial hasta el punto de poner en peligro la continuidad del proceso productivo al que sustentan. Se promoverá el desarrollo de mecanismos que permitan mejorar la resiliencia de dichos sistemas frente a tales incidentes.

- Organización para la resiliencia en los sistemas de operación.
  - En este apartado se determinará el alcance particular de las medidas de ciber-resiliencia, estableciéndose sus objetivos, métricas y responsabilidades.
- Análisis de impacto de las tecnologías de operación y su evaluación.
  - Se identificarán los posibles escenarios de riesgo, se analizará el impacto sobre el negocio de dichos escenarios y se determinarán los recursos necesarios para poner en práctica la estrategia de ciber-resiliencia.
- Procedimientos de resiliencia.
  - Se definirán los mecanismos de respuesta ante ciberincidentes, como los planes de recuperación y los de comunicación/formación asociados.
- Pruebas.
  - Se definirán y ejecutarán los pertinentes planes de prueba que permitan verificar la estrategia de ciber-resiliencia y, en su caso, recoger las lecciones aprendidas.

› **Dominio 6: Gestión, Revisión, Mejora y Sostenibilidad del SGCI.** Este último dominio del marco general para la construcción de un SGCI fija el marco sobre el que deberán desarrollarse y mantenerse, tanto el SGCI, propiamente dicho, como su documentación; facilitando la integración con otros posibles sistemas de gestión existentes.

- Desarrollo y mantenimiento del SGCI.
  - Se ofrecerán directrices que determinen el desarrollo y mantenimiento del marco de gestión del SGCI.
- Gestión documental.
  - Se definirán los requisitos y procedimientos de aprobación, revisión y modificación de cuantos productos formen parte del repositorio documental del SGCI.

Se buscará la permanente mejora y la sostenibilidad del SGSI, mediante un continuado proceso de supervisión y revisión del sistema y de aquellos indicadores que permitan determinar si los controles establecidos son eficaces.

- Auditoría interna.
  - Se incluirán los requisitos de las evaluaciones y auditorías internas y su planificación.
- Revisión por la dirección.
  - Se establecerá un proceso para la revisión del SGCI por parte de la dirección de la organización.
- Supervisión y mejora.
  - Se incluirán los pertinentes procedimientos de supervisión y mejora del SGCI.

1

Dominio 1: Definición de una Estrategia de Ciberseguridad Industrial

CONTENIDOS

CONTEXTO

DISEÑO DE LA ESTRATEGIA DE C.I.

FUNDAMENTOS DEL NEGOCIO
BENEFICIOS
CONSECUENCIAS POTENCIALES Y RIESGO ASUMIBLE

ALCANCE DEL SGCI
DEFINICIÓN DEL ALCANCE
PLANIFICACIÓN DE RECURSOS PARA IMPLANTACIÓN DEL SGCI

ORGANIZACIÓN DE LA CIBERSEGURIDAD
RESPONSABILIDADES DE LA DIRECCIÓN
RESPONSABILIDADES DEL COMITÉ DEL SGCI
RESPONSABILIDADES DEL DIRECTOR DEL PROGRAMA SGCI (RESPONSABLE DEL SGCI)
RESPONSABILIDADES DE LOS USUARIOS DENTRO DEL ALCANCE DEL SGCI

POLÍTICA DE CIBERSEGURIDAD

Dominio 1: Definición de una Estrategia de Ciberseguridad Industrial

Contexto

CONTEXTO

El presente capítulo de esta guía describe el primero de los dominios del marco de referencia del SGCI: Definición de una Estrategia de Ciberseguridad Industrial.

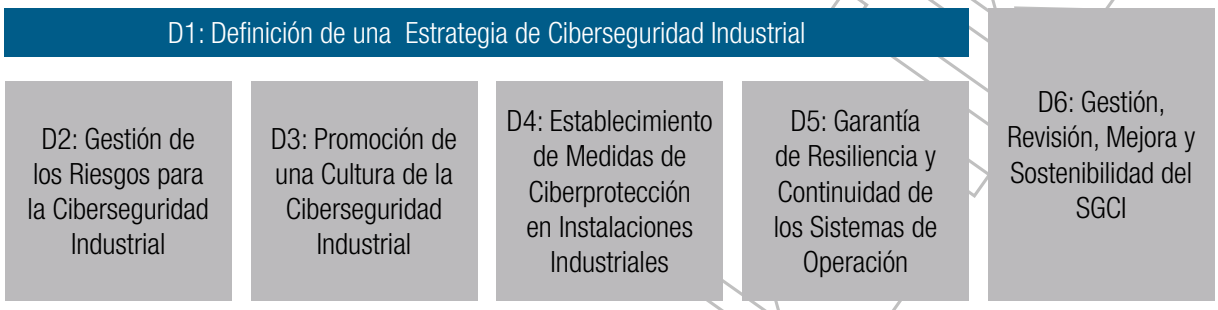


Figura 3: Marco de referencia del SGCI. Dominio 1

Toda estrategia de ciberseguridad industrial descansa sobre cuatro pilares de carácter básico:

- Los fundamentos del negocio, que definen una estrategia alineada con los requisitos del negocio y permiten determinar los requisitos de seguridad y los riesgos que la organización está dispuesta a asumir.
- El alcance del SGCI, que identifica el ámbito de aplicación del SGCI, de acuerdo a los requisitos del negocio.
- La política de ciberseguridad industrial, que formaliza los requisitos de seguridad que deben ser de aplicación sobre el alcance definido y los impulsa dentro de la entidad, estableciendo las responsabilidades generales para su consecución.
- La organización para la ciberseguridad, que recoge todas aquellas unidades, personas o roles que deben satisfacer, dentro del alcance del SGCI, las responsabilidades generales establecidas en la política de ciberseguridad industrial, identificando dichos roles, sus funciones, responsabilidades concretas, jerarquías y dependencias, etc.

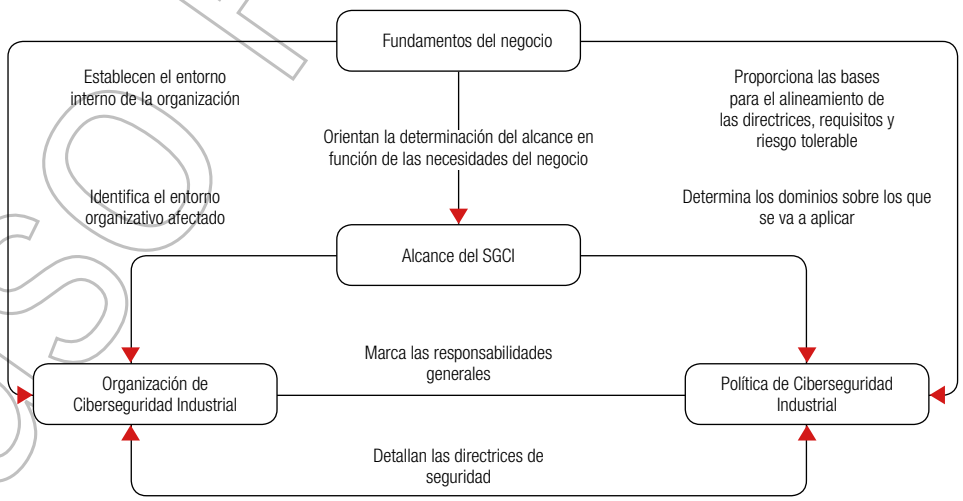


Figura 4: Pilares básicos de una estrategia de ciberseguridad industrial

Dominio 1: Definición de una Estrategia de Ciberseguridad Industrial
Diseño de la Estrategia de Ciberseguridad Industrial

DISEÑO DE LA ESTRATEGIA DE CIBERSEGURIDAD INDUSTRIAL

Fundamentos del Negocio

El objetivo de los fundamentos del negocio es determinar cuáles son las necesidades, en materia de ciberseguridad, que tiene la organización. Estas necesidades deben tener en cuenta aspectos de los procesos del negocio, industriales, financieros, de salud laboral y seguridad física, medioambientales, y en general cualquier elemento que pueda influir en el correcto funcionamiento de los procesos de negocio de la organización.

Los fundamentos del negocio deben identificar claramente la dependencia que la organización tiene de sus sistemas de control, y por tanto la necesidad de garantizar su seguridad física y lógica, de manera que sirvan como herramienta de venta interna para lograr que la dirección de organización apoye la creación del SGCI.

Los fundamentos del negocio deben reflejar las preocupaciones que la dirección tiene respecto al correcto funcionamiento del negocio. Los fundamentos deben ser construidos a partir del conocimiento y experiencia del personal que trata diariamente con los riesgos que afectan a la organización.

Deben proporcionar información objetiva acerca de posibles impactos sobre el negocio y facilitar al responsable del sistema argumentos para involucrar a la dirección de la organización en la creación de un SGCI. Entre la información que deben contener se contarán los posibles beneficios, impactos potenciales sobre la continuidad del negocio, el medio ambiente y la sociedad, así como recursos necesarios para llevarlo a cabo.

Beneficios

Los beneficios de disponer de un SGCI alineado con los fundamentos del negocio deben ser claramente detallados, ya que servirán para apoyar la decisión de implantar un SGCI dentro de la organización.

Evidentemente, el principal beneficio, aspecto principal del SGCI, será lograr una disminución de los riesgos que afronta la organización, pero deberán tenerse en cuenta otros beneficios como:

- Identificar cual es el riesgo tolerable de la organización (esto es, el riesgo que la organización está dispuesta a asumir), lo que servirá de base a la hora de identificar el perfil de riesgo de la misma.
- Establecer el marco para alinear el SGCI con la misión, visión y objetivos de la organización.
- Considerar, con la importancia debida, los impactos de carácter relevante en las cadenas de suministro. Y tomar las medidas necesarias para minimizarlos y garantizar la continuidad de los procesos propios.
- Reducir los costos vinculados a los incidentes.
- Demostrar que se actúa con la diligencia debida (due-diligence), lo cual es un aspecto fundamental en la determinación de las responsabilidades legales derivadas de incidentes con efectos adversos.
- Proporcionar el enfoque para:
  - el establecimiento de responsabilidades de ciberseguridad.
  - adquirir un conocimiento preciso de los componentes contenidos en el alcance del SGCI.
  - el desarrollo de la política de ciberseguridad industrial.
- Orientar los esfuerzos en la mejora de la fiabilidad y disponibilidad de los sistemas más críticos para la organización; y, en consecuencia, para el desarrollo e implantación del SGCI.
- Mejorar las condiciones de trabajo de los empleados, disminuyendo la rotación laboral.
- Facilitar la capacitación de personal especializado en ciberseguridad para los sistemas contenidos en el alcance.
- Mejorar la imagen y reputación de la compañía, la opinión pública y la de terceros afectados acerca del funcionamiento de la instalación.
- Incremento de la confianza de los inversores.
- Disminuir la responsabilidad civil.
- Mejorar las condiciones con las aseguradoras.
- Contribuir al cumplimiento de los requisitos legales, reglamentarios o contractuales que sean de aplicación.
- Garantizar la resiliencia y la continuidad del negocio.

Consecuencias potenciales y riesgo asumible

Con el fin de reforzar la necesidad de la existencia de un SGCI alineado con los fundamentos del negocio de la organización, deben detallarse con claridad, y dentro del contexto de la ciberseguridad, cuáles serían las consecuencias potenciales (impactos en el negocio) de no asegurar los sistemas de control, y los riesgos que la organización está dispuesta a asumir en cada caso. Las consecuencias potenciales deben ser detalladas teniendo en cuenta la naturaleza del negocio y deben incorporar una priorización con el fin de determinar cuáles son las más probables y las de mayor impacto y criticidad.

Los posibles impactos en los sistemas de control vendrán determinados por la materialización de una serie de amenazas que deben ser priorizadas teniendo en cuenta las características de la organización y los componentes existentes dentro del alcance elegido.

Como ayuda para la identificación de amenazas, el siguiente capítulo de la presente guía, que recoge el Dominio 2. Gestión de riesgos para la ciberseguridad industrial del marco de referencia para el SGCI, contiene un catálogo de amenazas propias del ámbito industrial.

Los impactos potenciales pueden encuadrarse dentro de las siguientes categorías:

- Impacto físico: Consecuencias directas de fallos en los sistemas de control. Los efectos potenciales de este tipo de impacto son de la máxima importancia ya que pueden incluir pérdida de vidas humanas o daños al medio ambiente, así como pérdida de activos de la organización.
- Impacto económico: Con un nivel de gravedad inferior que los anteriores, este tipo de impacto debe considerarse critico por afectar directamente a la viabilidad económica y continuidad del negocio, y poder tener consecuencias en la economía de la región o del país. Naturalmente, los impactos físicos, tendrán, también impacto económico.
- Impacto social: También de criticidad inferior a los impactos físicos, este tipo de impactos, no deben ser desdeñados ya que pueden afectar a la imagen de la organización.

Algunas de las consecuencias potenciales que deberán ser tenidas en cuenta son:

- Impacto a la seguridad nacional.
- Pérdida de producción y del negocio.
- Daños o muerte de empleados.
- Daños o muerte a la población.
- Daño al equipamiento.
- Daño ambiental.
- Incumplimiento legal.
- Responsabilidad civil y criminal.
- Pérdida de información confidencial.
- Daños a la imagen o a la marca de la organización.

Las consecuencias potenciales listadas con mayor prioridad, deben ser evaluadas detalladamente para estimar su impacto anual. Siempre que sea posible, dicho impacto deberá ser evaluado desde el punto de vista financiero, aunque dada la complejidad que esto presenta en algunas ocasiones, es aceptable realizar la evaluación desde un punto de vista cualitativo. La información para desarrollar este punto debe proceder del conocimiento y la experiencia existente dentro de la organización.

Proceso para alinear el SGCI con los Fundamentos del Negocio

I. Comprender la visión, misión, metas, valores y estrategias de la organización

Es necesario obtener una perspectiva general de la organización con el fin de conocer su visión, misión, principales propósitos, valores y estrategia. Ello permitirá asegurar la consistencia y alineamiento entre los objetivos estratégicos de gestión del riesgo y la misión de la organización, así como el compromiso de la Dirección con este proceso como estrategia del negocio.

II. Analizar el entorno externo

Es crítico considerar la identificación y análisis de las amenazas del entorno y de los requerimientos externos de seguridad relativos al sector de la organización.

III. Analizar el entorno interno

Es necesario comprender la estructura organizativa y los principales actores de la misma en los diversos niveles:

- Estratégico: ¿Quién toma las decisiones estratégicas?
- Táctico: ¿Quién coordina y gestiona las operaciones?

› Operacional: ¿Quién está implicado en la producción y las actividades de soporte a la misma?

Es necesario identificar los roles, responsabilidades, autoridad y comunicación dentro de la organización, así como las funciones externalizadas y los contratistas de las mismas.

IV. Identificar procesos y recursos clave

Es esencial conocer:

› Cuáles son los productos y servicios de la organización.
› Cuáles son los procesos clave que permiten a la organización llevar a cabo su misión.
› Cuáles son los sistemas de control industrial que soportan dichos procesos clave.
› Cuáles son los proveedores clave de los insumos para cada proceso.

Figura 5: Descubrimiento escalonado de procesos y recursos clave

V. Identificación y análisis de las partes interesadas

Es indispensable identificar a todas y cada una de las partes interesadas de forma que sean consideradas en el proceso de evaluación de riesgos y en la implementación del SGCI.

Para cada una de ellas es necesario:

› Analizar sus necesidades y expectativas, incluyendo las relativas a la seguridad.
› Validar si dichas partes interesadas deben verse implicadas en el SGCI.
› Identificar roles y responsabilidades de las partes interesadas, si es el caso, y los niveles requeridos de su participación en el SGCI.

VI. Identificación y análisis de los requisitos del negocio

La organización debe tener en cuenta, y analizar, los diversos requisitos que tengan relevancia en la continuidad de los sistemas de control industrial identificados [véase Dominio 5. Garantía de Resiliencia y Continuidad de los Sistemas de Operación, más adelante].

Se considerarán tanto los requisitos obligatorios, como los voluntarios:

› **Obligatorios:** de carácter **externo** (leyes y regulaciones que la organización debe cumplir) y de carácter **interno** (obligaciones contractuales alcanzadas).
› **Voluntarios:** de carácter **externo** (normas internacionales y códigos de buenas prácticas a las que la organización se adhiera) y de carácter **interno** (políticas internas, códigos de buenas prácticas de la organización, reglas de trabajo, etc.).

VII. Determinación de los criterios de evaluación y de aceptación del riesgo

Resulta clave determinar los criterios de aceptación del riesgo sobre los sistemas de control industrial identificados. Criterios que reflejen los valores y objetivos de la organización. Algunos criterios pueden venir impuestos por razones legales o regulatorias.

Para establecer dichos criterios se tendrán en cuenta aspectos como:

› La naturaleza y el tipo de amenazas, y las consecuencias de su materialización; así como el modo en que dichas consecuencias deben ser medidas.
› Las probabilidades de ocurrencia.
› Cómo se va determinar el nivel de riesgo.
› Cuál es el nivel de riesgo que la organización está dispuesta a asumir.

En el **Anexo I** se proporciona una plantilla para ayudar a la descripción del contexto y los fundamentos del negocio.

Alcance del SGCI

Una vez establecidos los fundamentos del negocio y los requisitos de la organización en cuanto a ciberseguridad y se haya obtenido el compromiso de la Dirección, debe establecerse cuál será el alcance del SGCI.

Esas tres piezas constituyen los cimientos del SGCI. De ellas derivará la política de seguridad que regirá el sistema de gestión y las directrices para el desarrollo de los diferentes componentes de dicho sistema.

El alcance detallará, de manera que no dé lugar a interpretaciones, cuáles son los componentes de la organización que están afectados por el SGCI. El alcance del SGCI será mantenido por el responsable del sistema de gestión y deberá revisarse periódicamente o siempre que haya cambios significativos que afecten al SGCI.

El alcance sirve para establecer, de manera formal, límites al ámbito de aplicación del SGCI. Esto es fundamental para determinar si un determinado activo de la organización está afectado, o no, por las diferentes políticas que establece el SGCI.

El alcance contendrá los elementos de los procesos industriales (procedimientos, componentes, información, etc.) que la organización desea proteger. Por tanto, su elección es fundamental para poder desarrollar un SGCI que aporte valor a la organización. Durante la determinación del alcance deben tenerse en cuenta factores como el número o la complejidad de los diferentes componentes, ya que influirán sobre la dificultad y necesidad de recursos para la puesta en marcha del sistema de gestión.

Es recomendable buscar un equilibrio entre el valor aportado por la protección de los elementos contenidos en el alcance y la dificultad que supondrá construir un SGCI sobre el alcance seleccionado.

A la hora de identificar y describir el alcance, se debe tomar en cuenta:

- El ámbito organizativo: Para ello se examinarán las responsabilidades y áreas de influencia de los principales actores dentro de la organización, los procesos clave de la misma, sus unidades organizativas y estructuras de gestión, etc. Se describirán las fronteras organizativas del SGCI y se documentarán las excepciones, los procesos de negocio afectados por el alcance y los activos de información implicados (con sus correspondientes propietarios).
- El ámbito de los sistemas: Dicha identificación se realizará tomando en consideración todos los componentes que integran los sistemas de control afectados y los sistemas de información que forman parte de los procesos de negocio incluidos en el alcance.
- El ámbito físico: Para ello:
- Se tendrá en cuenta cualquier tipo de localización que sea relevante (total o parcialmente) para los procesos de negocio que constituyen el ámbito organizativo del SGCI.
- Se considerarán todos los recursos requeridos para mantener la operatividad de dichas instalaciones.
- Igualmente, en el caso de localizaciones no incluidas en el alcance, deberán tenerse en cuenta las relaciones e interfaces de comunicación con componentes que sí están incluidos.

Definición del alcance

Se proponen dos métodos de definición del alcance. Ambos métodos no deben verse como mutuamente excluyentes, sino que se complementan entre sí, ofreciendo una visión más precisa del contenido del alcance.

Aproximación por proceso

La aproximación por proceso define el alcance del SGCI mediante la descripción de los procesos que formarán parte del sistema de gestión.

Para cada proceso se detallará quién es el propietario y cada una de las actividades que lo componen. Para cada actividad se señalarán las entradas y salidas de la misma, así como las subtareas relevantes para su mejor comprensión y los recursos requeridos para su desempeño.

La definición del alcance por proceso permite identificar de manera sencilla las dependencias existentes entre las diferentes actividades desempeñadas dentro del alcance, así como los recursos necesarios para llevarlas a cabo.

Aproximación por componente

Aunque la aproximación por proceso proporciona una visión precisa del componente funcional del alcance, ésta estará incompleta si no se complementa con una aproximación que tenga en cuenta a los componentes implicados dentro del alcance. Para abordar esta aproximación, será necesario desarrollar un inventario de componentes que contenga, al menos, la siguiente información:

- Identificador: Identificador único del componente.

› Descripción: Descripción del componente incluyendo sus características hardware y software.
› Propietario: Propietario del componente.
› Tipo: Tipo de componente (sistema físico, sistema lógico, personal, información, servicio, proceso, etc.).

Diagrama de capas

El diagrama de capas permite determinar de manera sencilla las relaciones existentes entre los componentes del alcance y los elementos auxiliares, que pese a no estar dentro del alcance deben ser tenidos en cuenta dentro del SGCI.

Se recomienda contemplar al menos tres niveles:

› Alcance: Componentes nucleares del alcance.
› Recursos Internos: Elementos y recursos pertenecientes a la organización y que interactúan con los componentes del alcance.
› Recursos externos: Elementos y recursos no pertenecientes a la organización y que interactúan con los componentes del alcance.

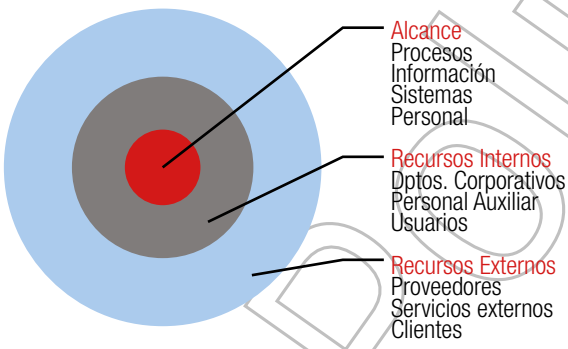


Figura 6: Ejemplo de diagrama de capas

El reparto de los activos del alcance en diferentes niveles permite identificar claramente cuáles son los elementos fundamentales para el SGCI; aquellos que constituirán el principal objetivo de las medidas de protección a implantar.

Diagrama de componentes

Resulta de ayuda incorporar a la descripción del alcance diagramas de red, lógicos y de alto nivel, que permitan comprender de manera sencilla las relaciones entre componentes y los flujos de comunicación existentes.

Entre la documentación típica existente en las instalaciones industriales se encuentran diagramas físicos de red que detallan de manera precisa la ubicación física de cada componente de las redes de control. Sin embargo, no es habitual encontrar diagramas de red que contemplen aspectos lógicos como el direccionamiento de red, segmentación, zonas de seguridad, etc. El desarrollo de estos diagramas es importante ya que permiten identificar fácilmente cuáles son las ubicaciones, desde el punto de vista lógico, de los distintos componentes de la red y por tanto determinar cuáles son las medidas de seguridad más apropiadas.

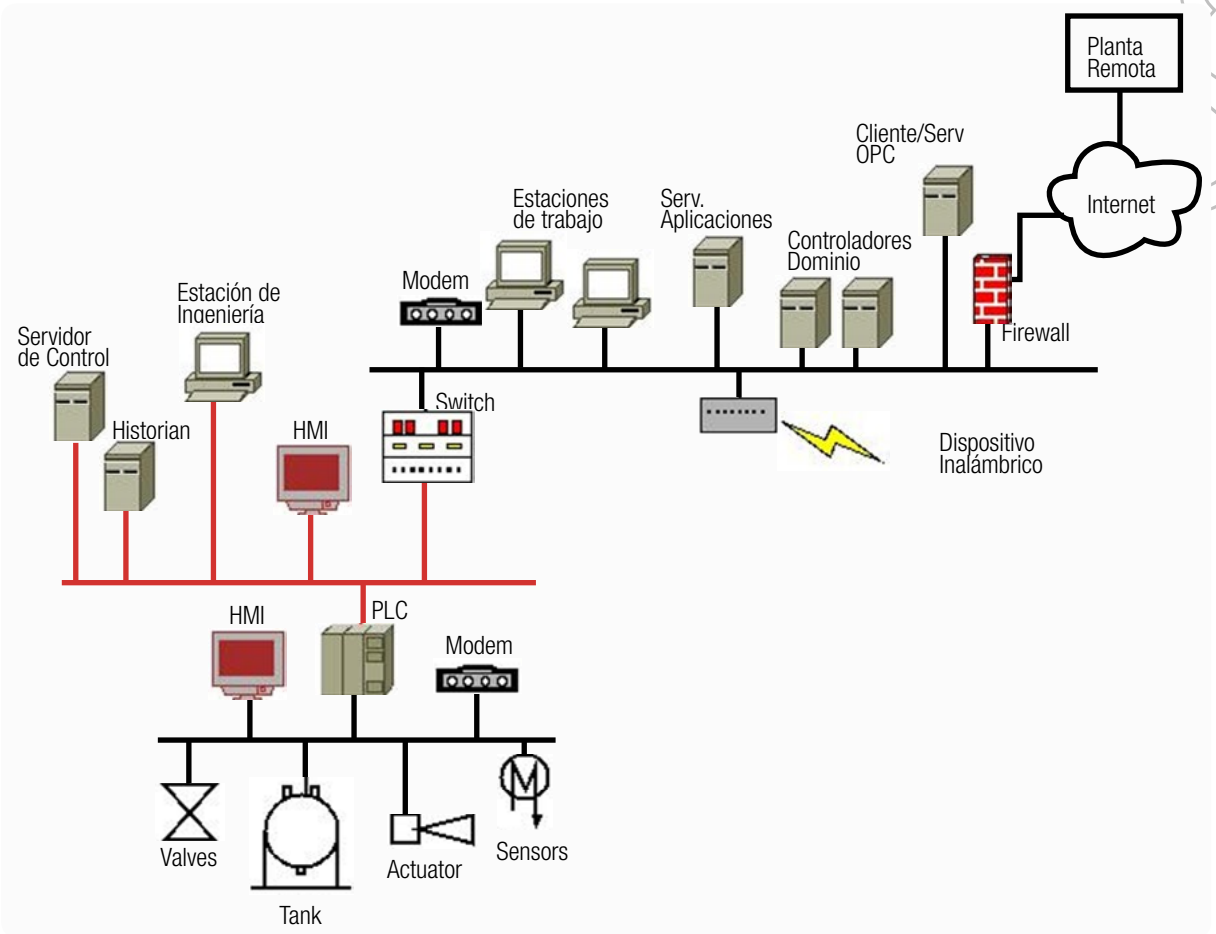


Figura 7: Ejemplo de diagrama de componentes

Planificación de recursos para implantación del SGCI

La identificación del alcance debe dirigir la previsión de recursos para la construcción del SGCI. Se distinguirá entre recursos externos y recursos internos.

- Recursos externos: principalmente relacionados con adquisición de conocimiento experto para el desarrollo, construcción y manejo del SGCI. En este apartado se contemplará la adquisición de equipamiento o documentación o la contratación de servicios de consultoría.
- Recursos internos: recursos existentes en la organización que pueden ser utilizados para la gestión de riesgos de ciberseguridad.

En el **Anexo III** se proporciona una plantilla para ayudar a la descripción del alcance del SGCI.

Organización de la Ciberseguridad

Se deben identificar y fijar las entidades responsables de gestionar y mantener la ciberseguridad de los sistemas de control de la organización. La ciberseguridad no sólo implica a los sistemas y la información que éstos gestionan, sino que debe tener en cuenta el resto de elementos relacionados con los activos que se desea proteger. De esta manera, será necesario tener en cuenta elementos de seguridad física, proveedores, terceras partes, socios, etc., entre otros.

El compromiso de la organización con el SGCI es importante para lograr que la iniciativa llegue a buen puerto. Dicho compromiso debe comenzar en lo más alto, ya que necesitará de conocimiento repartido a lo largo de toda la organización y probablemente requerirá modificaciones a su estructura.

La alta dirección debe establecer una estructura

organizativa que proporcione orientación y dirección para la gestión de la ciberseguridad de los sistemas de control; así como proporcionar los recursos necesarios para la realización de las tareas relacionadas con el mantenimiento y operación del SGCI.

Esta estructura puede tomar la forma de un grupo de interesados, o Comité de Gestión de la Ciberseguridad, que posean el conocimiento necesario para la implantación y operación del SGCI, tengan asignadas las responsabilidades pertinentes en materia de ciberseguridad y reporten directamente a la alta dirección.

El Comité estará compuesto por personal relevante de distintas áreas de la organización que posea conocimiento o responsabilidades sobre la ciberseguridad de los sistemas de control de la compañía.

Si fuese necesario, el Comité se puede complementar de manera permanente o temporal con expertos en una materia determinada.

La formación del comité podría variar a lo largo del tiempo para adaptarse a la evolución de los sistemas de la organización y al incremento de madurez de la organización en cuanto a la ciberseguridad de los sistemas de control.

El Comité de Gestión de la Ciberseguridad tendrá como responsabilidad coordinar la implantación y posterior operación del SGCI. También tendrá la responsabilidad de las decisiones en materia de ciberseguridad que afecten a los sistemas de control de la organización.

El Comité estará coordinado por un responsable designado por la alta dirección. Entre sus labores estarán la organización de las reuniones del Comité y ser el responsable último del funcionamiento del SGCI.

Una pieza fundamental de la estructura organizativa de ciberseguridad es el establecimiento de las responsabilidades de ciberseguridad a diversos niveles de la organización.

Igual de importante es promover la integración de los roles de seguridad derivados del SGCI con el resto de iniciativas organizativas (principalmente en órganos colectivos, como comités, ya operativos en la entidad), con el fin de maximizar en lo posible las sinergias organizativas.

El modelo organizativo, genérico, propuesto, que deberá ser adaptado a la realidad organizativa de cada entidad [véase III. Analizar el entorno interno, más arriba en este mismo capítulo] es el siguiente:

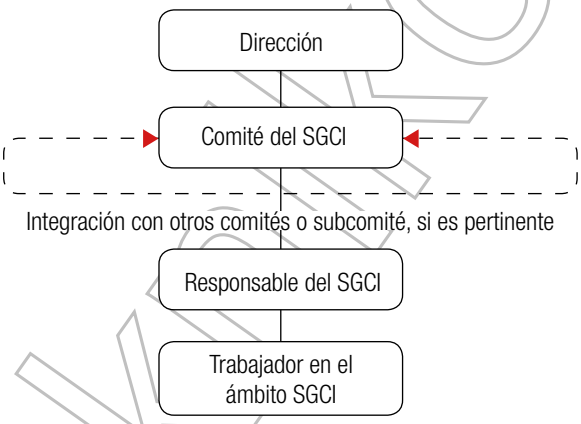


Figura 8: Modelo organizativo genérico propuesto para la gestión de la ciberseguridad industrial

Responsabilidades de la Dirección

Dentro del proceso de desarrollo e implantación del SGCI, la Dirección debiera establecer un Comité de Gestión de la Ciberseguridad (o Comité del SGCI) en el que se traten todas las cuestiones que precisen de la intervención de la dicha Dirección; además de servir como instrumento que materializa el compromiso de aquella con el propio SGCI.

Independientemente de las responsabilidades asignadas a dicho Comité, de forma delegada por parte de la Dirección, ésta debiera responsabilizarse específicamente de:

- Establecer y difundir las política, objetivos y normativas de seguridad.
- Comunicar a toda la organización la importancia de cumplir con los objetivos de seguridad y la necesidad de la mejora continua.
- Establecer el resto de roles y responsabilidades necesarios para el eficaz funcionamiento del SGCI.
- Asegurar la dotación de los recursos necesarios para la planificación, implementación, monitorización, revisión y mejora de la seguridad a través de los procesos y controles definidos, así como por medio de la implantación y operatividad continua del Comité del SGCI.
- Aprobar el alcance del SGCI, el riesgo tolerable y los riesgos residuales asumidos,

› Realizar las revisiones del SGCI tendentes a analizar la adecuación del sistema de gestión, su alineamiento con la política de ciberseguridad industrial del SGCI, y la comprobación de que se mantiene constante la eficacia del sistema, de modo que se garantice que está funcionando correctamente.
› Realización de auditorías anuales que comprueben la eficacia del sistema, los cambios que se hayan producido y establezcan planes de acción que mejoren el sistema.

Responsabilidades del Comité del SGCI

Objetivos del Comité del SGCI:

El objetivo principal del Comité del SGCI es:

› Proporcionar evidencia clara, visible y demostrable del apoyo y compromiso de la Dirección de la entidad en el establecimiento, implantación, revisión y mantenimiento (mejora continua y sostenibilidad) del SGCI.
› Proporcionar muestras de que la organización está desempeñando de manera adecuada los procesos de gestión de la ciberseguridad.

Los objetivos secundarios del Comité del SGCI son:

› Promocionar la ciberseguridad industrial dentro de la entidad, por medio de una dirección y coordinación clara y un compromiso demostrado.
› Apoyar e impulsar las iniciativas de seguridad del SGCI.
› Involucrar a las áreas relacionadas en las tareas de seguridad del SGCI.

Funciones del Comité del SGCI:

Para conseguir los objetivos establecidos, el Comité del SGCI debe asumir las siguientes funciones principales:

› Establecimiento, implantación, revisión y mantenimiento (mejora continua) del SGCI, mediante la aprobación y aceptación de acciones y sus resultados.
› Creación de un foro donde se discutan y coordinen los aspectos estratégicos afectados dentro del alcance del SGCI a nivel corporativo (tanto a nivel de negocio, organizativo, técnico y de gestión de recursos humanos).
› Desarrollo y publicación de normas y/o procedimientos internos que desarrollen la Política del SGCI.

Responsabilidades del Director del Programa SGCI (Responsable del SGCI)

El Responsable del Sistema de Gestión de la Ciberseguridad Industrial tendrá las siguientes atribuciones:

› Coordinar el Comité de Gestión de la Ciberseguridad (Comité del SGCI).
› Dirigir y mantener el SGCI.
› Realizar labores informativas dirigidas a divulgar aspectos de la ciberseguridad, relacionados con el alcance, dentro de la organización.
› Definir estrategias de ciberseguridad que permitan proteger los procesos contenidos en el alcance y conseguir sus objetivos.
› Identificar los objetivos de protección y sus métricas en consonancia con el plan estratégico corporativo.
› Administrar el desarrollo y la aplicación de la política de seguridad del SGCI, las normas, directrices y procedimientos para garantizar el mantenimiento continuo de la ciberseguridad de los activos y procesos contenidos en el alcance.
› Revisar y aprobar la instalación de sistemas que soporten procesos del alcance, de forma que se garantice el cumplimiento con las políticas y requisitos de seguridad existentes.
› Contribuir a la concienciación y cultura de seguridad de la organización destacando el valor que aporta el SGCI.
› Estar a cargo de la planificación de respuesta de incidentes, así como la investigación de vulneraciones de la seguridad que hayan afectado a sistemas del alcance.
› Prestar apoyo en la revisión de cuestiones disciplinarias y legales relacionadas con infracciones en las que haya implicación de algún sistema contenido en el alcance.
› Dirigir el desarrollo de políticas y normativas de uso y de servicios de seguridad que afecten a los sistemas del alcance.
› Revisar y supervisar todo cambio propuesto sobre los sistemas del alcance para comprobar que no debilite su seguridad.

- Garantizar que la seguridad sea parte de los procesos contenidos en el alcance y se contemple como un requisito más del negocio.
- Evaluar la pertinencia y coordinar la implementación de controles específicos de ciberseguridad para nuevos sistemas o servicios relacionados con el alcance.
- Mantenerse al día de los avances y novedades en materia de ciberseguridad. Para ello deberá mantenerse en contacto con foros y asociaciones profesionales en los que se discutan estas materias.

Responsabilidades de los usuarios dentro del alcance del SGCI

Algunas de las responsabilidades genéricas de ciberseguridad, aplicables a cualquier puesto de trabajo, son las siguientes:

- Garantizar la seguridad de los sistemas que están bajo su responsabilidad.
- Garantizar la confidencialidad de la información tratada durante el desempeño del trabajo.
- Uso responsable (de acuerdo a las normas establecidas por la organización) de los recursos informáticos.
- Utilización de buenas prácticas reconocidas para el desempeño del trabajo.
- Responsabilidad de garantizar la seguridad de los activos que son responsabilidad del trabajador.

Estas responsabilidades deben ser definidas formalmente e incluidas dentro de la descripción de cada puesto de trabajo afectado.

En el **Anexo II** se proporciona una plantilla para ayudar a la definición de roles y funcionalidades.

Política de Ciberseguridad

El objetivo de la política de ciberseguridad es proporcionar directrices para la gestión y el apoyo de la ciberseguridad de acuerdo con los requisitos del negocio y las leyes aplicables.

La política de ciberseguridad debe constituir, por tanto, la herramienta fundamental para:

- Materializar la declaración de intenciones de la Dirección en relación con la ciberseguridad industrial.
- Proporcionar el soporte y guía por parte de la Dirección para establecer una ciberseguridad industrial alineada con los requerimientos del negocio y con el cumplimiento de las regulaciones y leyes que les sean de aplicación.
- Mejorar la concienciación de la organización en relación con la ciberseguridad industrial.

La política de ciberseguridad debe estar respaldada por los responsables finales de los procesos de negocio que se desea proteger y debe demostrar el apoyo y compromiso de aquellos.

La política debe contener al menos los siguientes aspectos:

- Una definición de ciberseguridad, de los objetivos que busca y de su ámbito de aplicación.
- El apoyo explícito de los responsables finales de los procesos de negocio que se desea proteger.
- Una definición de las responsabilidades generales y específicas en materia de ciberseguridad industrial, incluyendo la comunicación de incidentes de seguridad.
- Mención a los mecanismos existentes para identificar y gestionar el riesgo.
- Referencias a la existencia de documentación que apoye a la política (políticas más detalladas y específicas, procedimientos, instrucciones de trabajo, etc.).
- Realización de revisiones para garantizar el mantenimiento de la ciberseguridad a lo largo del tiempo.
- Una breve explicación de los requisitos más importantes a cumplir por la organización, como por ejemplo cumplimiento de los requisitos legales, reglamentarios o contractuales; requisitos de capacitación, formación y concienciación en seguridad; gestión de la continuidad del negocio; consecuencias de la violación de la política de ciberseguridad.

La política estará sujeta a revisiones periódicas con el fin de garantizar que las directrices que establece siguen siendo las más adecuadas a lo largo del tiempo.

La política de ciberseguridad debe ser el punto de entrada al SGCI, y de ella derivarán otros documentos que tratan aspectos de la ciberseguridad de manera más específica.

La política debe proporcionar una visión de alto nivel acerca de la ciberseguridad dentro de la organización, evitando reflejar detalles técnicos u operativos.

Los detalles específicos de la ciberseguridad de los distintos componentes contenidos en el alcance del sistema estarán detallados en otros documentos subordinados a la política. Se recomienda la utilización de diversos niveles de documentación bajo la política, alineando en todo caso los mismos a las directrices que en la materia ya hayan podido establecerse en la entidad:

- Nivel estratégico
  - La propia política de ciberseguridad.
- Nivel táctico
  - Normativas generales o específicas que detallen y concreten la Política de ciberseguridad industrial para componentes / conjuntos de componentes o ámbitos determinados.
- Nivel operativo
  - Procedimientos: Documentos que recogen el conjunto de tareas detalladas, secuenciales y específicas con el fin de soportar, en la operativa diaria, todos los aspectos recogidos en la política y normativas de ciberseguridad industrial. Los procedimientos son documentos que especifican el quién, cómo, dónde y cuándo deben realizarse las tareas específicas
  - Instrucciones de trabajo: Basándose en los procedimientos, y para entornos o sistemas concretos, podrán elaborarse instrucciones de trabajo, que documenten de forma explícita y detallada las acciones técnicas a realizar en la ejecución de dichos procedimientos, estableciendo directrices a nivel técnico muy detallado y concreto.

De esta manera, se facilita la modificación de las piezas del SGCI en caso de que sucedan modificaciones a los componentes del alcance. Por ejemplo, al sustituir un modelo de controlador por otro, la normativa de control de acceso al controlador permanecerá sin cambios, ya que los requisitos de seguridad siguen siendo los mismos; y, sin embargo, habrá que volver a escribir la instrucción técnica que explica la manera, en el nuevo controlador, en la que se deben implementar los requisitos establecidos por dicha normativa.

Como se ha indicado, en la definición de una estructura organizativa para la ciberseguridad industrial, es importante promover la integración de la política y las normativas de ciberseguridad industrial, con la política y las normativas de seguridad establecidas, al efecto, con carácter corporativo, con el fin de alcanzar las mayores sinergias posibles en todos los ámbitos relacionados con la seguridad.

En el **Anexo IV** se proporciona una plantilla para ayudar a la definición de la Política de Ciberseguridad..

2

Dominio 2:
Gestión de los Riesgos para la Ciberseguridad Industrial

DOMINIO 2: GESTIÓN DE LOS RIESGOS PARA LA CIBERSEGURIDAD INDUSTRIAL

CONTEXTO

OBJETIVOS Y ENFOQUE DEL ANÁLISIS DE RIESGOS

METODOLOGÍA DE ANÁLISIS DE RIESGOS

IDENTIFICACIÓN DE ACTIVOS
IDENTIFICACIÓN DE AMENAZAS
IDENTIFICACIÓN DE CONTROLES EXISTENTES
IDENTIFICACIÓN DE VULNERABILIDADES
CÁLCULO DEL RIESGO

TRATAMIENTO DEL RIESGO

Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial
Contexto

CONTEXTO

El presente capítulo de esta guía describe el segundo de los dominios del marco de referencia del SGCI: **Gestión de los Riesgos para la Ciberseguridad Industrial**.

Figura 9: Marco de referencia del SGCI. Dominio 2

No todas las organizaciones, ni todos los ámbitos de aplicación de un análisis del riesgo mantienen la misma postura ante éste (el riesgo que en un ámbito determinado se considera admisible, en otro ámbito podría ser algo completamente inaceptable).

A la hora de analizar los fundamentos del negocio en la estrategia de seguridad, donde se describe el contexto del negocio para la construcción del SGCI, se habrá identificado el riesgo tolerable (riesgo que la organización está dispuesta a asumir).

El cálculo del riesgo permite a la organización conocer si está sobrepasando, o no, dicho riesgo admisible y, en caso de que así suceda, decidir cuál será su respuesta para reducir la probabilidad de las amenazas, solucionar las vulnerabilidades, o reducir las consecuencias de los impactos.

Por ello, el objetivo de este documento es proporcionar, a los responsables de la operación de plantas industriales, un método sencillo para la realización de análisis de riesgos en sus instalaciones.

A los efectos de la presente guía debe entenderse el riesgo como **la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización**; y el análisis del riesgo como el **Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.**

El marco conceptual que regula el método para la realización del análisis de riesgos es el siguiente:


Security
ctrl

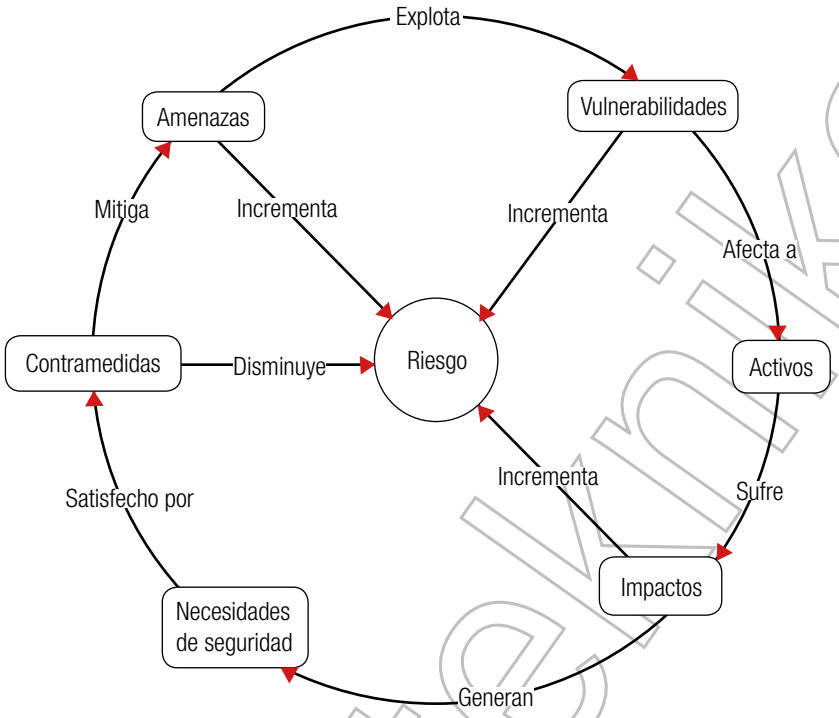


Figura 10: Marco conceptual del riesgo

Por ello, los elementos fundamentales que deben ser analizados a la hora de abordar el análisis de riesgos son:

- Activo: Recurso del sistema de operación o información, o relacionado con éstos, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su Dirección.
- Vulnerabilidad: Debilidad intrínseca de un activo. Por sí misma no debería ser perjudicial. Lo será ante la presencia de una amenaza que actúe sobre dicha debilidad.
- Amenaza: Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza.
- Riesgo: Estimación de la exposición efectiva de un activo a una amenaza que pueda afectar a alguna de sus vulnerabilidades. El riesgo puede determinarse por medio de dos medidas: frecuencia de ocurrencia y degradación causada.

Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial

Objetivos y enfoque del análisis de riesgos

OBJETIVOS Y ENFOQUE DEL ANÁLISIS DE RIESGOS

El objetivo del análisis de riesgos es identificar los riesgos cibernéticos que pueden afectar a la instalación, estimar su impacto potencial y la probabilidad de que se materialicen.

Existen múltiples metodologías de análisis de riesgos, muchas de ellas de aplicación válida en los entornos de sistemas de control. Este documento tan sólo explicará cuáles son los componentes que debe tener una metodología válida para analizar los riesgos en estos entornos; y propondrá un sencillo ejemplo de metodología aplicable.

Existen dos aproximaciones diferentes para el análisis de riesgos basadas en la manera en que se caracteriza el riesgo: análisis cuantitativo y análisis cualitativo.

Los análisis cuantitativos buscan dar una valoración del riesgo basada en cantidades, habitualmente pérdidas financieras. Aunque los resultados del riesgo obtenidos por este tipo de metodologías son fácilmente interpretables desde el punto de vista del negocio y la organización, son difíciles de obtener de manera precisa, ya que dependen de la correcta valoración de las probabilidades de ocurrencia de amenazas y vulnerabilidades y del impacto que supone el deterioro o pérdida de cada activo.

El enfoque cualitativo está basado en el conocimiento y experiencia de expertos y especialistas, tanto internos como externos, así como en la de los usuarios de los activos. Además, emplea un conjunto de niveles de probabilidad y severidad que son de aplicación a los distintos componentes del análisis (activos, amenazas, vulnerabilidades).

En la metodología propuesta, debido a la escasez de recursos que permitan determinar valores históricos sobre amenazas, vulnerabilidades e impactos en entornos industriales, se ha adoptado la decisión de adoptar un enfoque cualitativo para la realización del análisis de riesgos.

Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial

Metodología de Análisis de Riesgos

METODOLOGÍA DE ANÁLISIS DE RIESGOS

A continuación, se describen someramente las distintas fases metodológicas para la ejecución del análisis de riesgos sobre el alcance definido.

Identificación de activos

El primer paso en la realización del análisis de riesgos es la identificación e inventariado de los activos contenidos en el ámbito de aplicación del análisis. Esta identificación se realizará a partir del modelo desarrollado durante el establecimiento del alcance (ver plantilla para la descripción del alcance del SGCI). A partir de dicho modelo se realizará una identificación detallada de los activos existentes.

Entendemos por activo cualquier componente o funcionalidad de un sistema de información u operación, con valor para la organización y que es susceptible de ser atacado de forma deliberada o accidental con consecuencias para la organización. [1]

Los activos pueden ser de distinta naturaleza, incluyendo:

- Control físico automatizado.
- Los recursos lógicos como el software.
- Los recursos físicos como el hardware.
- La información.
- Servicios.
- Personal.
- Intangibles (propiedad intelectual, reputación, imagen).

Los activos dentro del alcance deberán ser estudiados ya que son la base para identificar a qué amenazas están expuestos y qué vulnerabilidades contienen, con el fin de determinar la manera en que su la materialización de una amenaza afectaría al funcionamiento de los procesos de la instalación.

A continuación, se propone una posible estructura para inventariar activos.

Aspectos Organizativos

- Unidad/Ubicación: Unidad o ubicación de la organización dentro de la que el activo desempeña su función.
- Usuario: Individuo o entidad organizacional que tiene relación con el activo.
- Proceso: Proceso de producción del que forma parte el activo.

Características del Activo

- Propietario: Responsable del activo. El propietario es la voz más autorizada para determinar el valor del activo y las medidas de protección que éste requiere.
- Activo: Nombre del activo.
- Id-Activo: Identificador único para referenciarlo durante el análisis.
- Descripción: Descripción del activo.
- Valor: Valoración máxima de las distintas dimensiones de la seguridad.
- Tipo: Tipo del activo (información, hardware, software, servicio, personal, otros.)
- Clasificación: público, privado, restringido, …
- Interrelación con otros activos: Identificar dependencias entre activos.

Aspectos de protección

- CID: Valoración en las distintas dimensiones de la seguridad en las que el activo debe ser protegido (C)onfidencialidad, (I)ntegridad, (D)isponibilidad. Dada la naturaleza de las instalaciones a las que está dirigido este documento, es probable que la dimensión más importante, con diferencia, sea la disponibilidad, y que, por tanto, las medidas que se implanten contribuyan a mejorar dicha dimensión.
- Medidas implantadas: Medidas de seguridad existentes que contribuyen a mejorar la seguridad del activo.
- Identificar legislación aplicable.
- Responsable de aplicar medidas.
- Responsable de comprobar aplicación y efectividad.

En el **Anexo V** se proporciona una plantilla para ayudar a la realización del inventario de activos.

La recopilación e identificación de activos se realizará mediante entrevistas con el personal relevante de la instalación. Durante las entrevistas, además de recopilar la información requerida para inventariar los activos, se obtendrá información importante para el posterior desarrollo del análisis de riesgos, entre dicha información se contarán detalles técnicos y de configuración de los sistemas. En el Anexo VI se puede

encontrar una plantilla de caracterización de redes de sistemas de control y automatización industrial.

La identificación de activos en los entornos industriales puede ser tremendamente compleja debido a la cantidad y variedad de dispositivos involucrados. Para facilitar esta tarea, es recomendable la utilización de alguna herramienta software que permita la clasificación de los distintos dispositivos involucrados atendiendo a su participación en distintos procesos de producción, ubicaciones geográficas u otros factores. Por otra parte, cuando se realiza la identificación de dispositivos de control, es importante mantener la visión más allá del mero dispositivo que realiza el control del proceso, ya que existe un gran número de componentes implicados en el proceso, que deben ser incluidos en el análisis. Esto incluye:

- Sistemas de control distribuido (DCS) y sus dispositivos asociados.
- Sistemas SCADA y dispositivos asociados.
- PLCs y dispositivos asociados.
- Estaciones HMI.
- Sistemas Instrumentados de Seguridad (SIS).
- Ordenadores de propósito general.
- Sistemas de Gestión de la Información del proceso (PIM) y Sistemas de Ejecución de la Manufactura (MES).
- Sistemas de modelado y control de la automatización industrial.
- Sistemas expertos.
- Sistemas de inspección.
- Sistemas de seguimiento y manejo de material.
- Analizadores.
- Sistemas de medida.
- Sistemas Batch.
- Sistemas de gestión y/o monitorización de la energía eléctrica.
- Sistemas de telemetría remota.
- Sistemas de comunicación a dispositivos remotos.
- Sistemas de condición de operación estándar (SOC) y procedimiento operativo estándar (SOP).
- Sistemas de gestión documental.
- Ordenadores para desarrollo software.
- Sistemas de Aire Acondicionado, calefacción y ventilación (HVAC).
- Electrónica de red (switches, hubs, routers).
- Dispositivos de protección de red (firewalls, IDSs).

Dado el elevado número de activos potenciales que existen en cualquier organización, es importante tratar de mantener un equilibrio entre el detalle con el que se realiza el modelado de la instalación y la operatividad del análisis. Para esto, suele resultar de ayuda utilizar categorías y grupos de activos.

Las categorías servirán de guía a la hora de determinar las amenazas y vulnerabilidades a las que están expuestos los activos mediante el uso de catálogos que clasifican amenazas y vulnerabilidades para cada categoría de activo.

Los grupos de activos permiten disminuir la complejidad del análisis mediante la agrupación de activos que dentro de la instalación están sujetos a las mismas condiciones de operación y funcionamiento; y por tanto a las mismas amenazas.

Una gran ayuda para realizar la categorización de sistemas es utilizar la división en niveles de la arquitectura de referencia propuesta por ISA-99/IEC 62443.

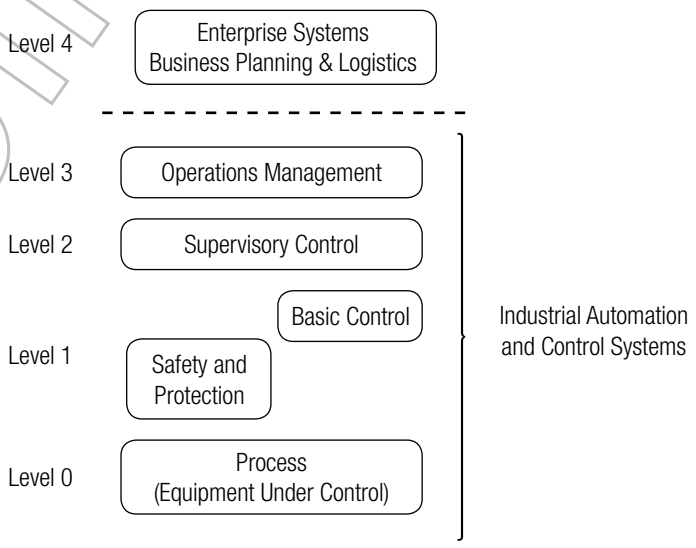


Figura 11: Jerarquía de niveles en la automatización industrial

Por ello tras la realización del inventario de los activos que forman el alcance del SGCI, será conveniente realizar dicha agrupación con el fin de facilitar en lo posible la realización del análisis, con el fin de evitar que el mismo se realice de forma individualizada para cada uno de los activos inventariados. A la hora de realizar dicha agrupación es necesario considerar que un nivel de agrupación pequeño dificultaría la realización del análisis sin aportar especial valor al mismo, y un nivel de agrupación excesivo restaría calidad a los resultados del análisis de riesgo.

Es recomendable que la organización desarrolle tablas con criterios objetivos que dirijan el proceso de valoración de la manera más determinista posible evitando valoraciones subjetivas o personales.

Identificación de amenazas

Las amenazas tienen el potencial de dañar activos tales como la información, los procesos y los sistemas, y por tanto, influir en el correcto funcionamiento de los procesos de producción. Las amenazas pueden ser deliberadas (D) o accidentales (A), pueden proceder del exterior o del interior de la organización y ser de diferentes tipos. Independientemente de estos factores, es importante identificar las distintas amenazas que afectan a los activos contenidos en el alcance.

La identificación de las amenazas y la probabilidad de su materialización requiere del conocimiento experto que debe ser aportado por los propietarios de los activos, los usuarios, personal implicado en la utilización o mantenimiento de los activos, expertos en ciberseguridad y profesionales o entidades capacitadas para realizar opiniones bien formadas sobre la materia.

En el **Anexo VII** se presenta un catálogo de amenazas para entornos de automatización y control industrial.

Tipo	Amenazada	Descripción	Código	Origen (Accidental/ deliberado)
Daño físico	Fuego	Daños causados por fuego al equipamiento y las instalaciones	DF1	D,A
	Agua	Daños causados por agua al equipamiento y las instalaciones	DF2	D,A
	Factores ambientales	Daños en el equipamiento causados por humedad, temperatura, partículas en suspensión	DF3	D,A
	Sabotaje	Daños físicos al equipamiento a la instalaciones	DF4	D
	Robo	Robo de equipamiento	DF5	D
Fallos de servicios de soporte	Susceptibilidad a variaciones de voltaje	El fallo del aire acondicionado puede causar una temperatura de funcionamiento no adecuada para el equipamiento.	FS1	D,A
	Fallo de suministro energético	Parada de los sistema debida a un fallo del suministro de energía	FS2	D,A

Figura 12: Ejemplo de catálogo de amenazas

Identificación de controles existentes

Es necesario identificar los controles que ya están implantados para evitar trabajos y costes innecesarios. Durante esta identificación, se verificará el correcto funcionamiento de los controles ya implantados y si estos, a su vez, están introduciendo nuevas vulnerabilidades en el alcance.

Para la identificación de controles existentes se pueden utilizar las siguientes fuentes:

- Documentos que contengan información sobre los controles (por ejemplo, planes de tratamiento de riesgos).
- Documentos de gestión interna (i.e. controles de entrada y salida de personal).
- Logs de los sistemas.
- Históricos de monitorización.
- Personal con responsabilidades en seguridad o en la operación y manejo de los activos del alcance.
- Revisiones on-site, de los controles físicos existentes.
- Informes de auditoría.

Identificación de vulnerabilidades

Las vulnerabilidades son puntos débiles en los activos. La existencia de una vulnerabilidad por si misma no es dañina, ya que requiere la existencia de una amenaza para que sea explotada. Las vulnerabilidades que no tengan amenazas asociadas no requerirán la implantación de ningún control, pero deberán ser documentadas y monitorizadas para detectar posibles cambios.

Las vulnerabilidades están categorizadas por tipo y para cada una se proponen amenazas capaces de explotar la vulnerabilidad. La categorización mediante tipos de vulnerabilidad permite realizar, de manera sencilla, la asignación de grupos de vulnerabilidades a tipos de activos.

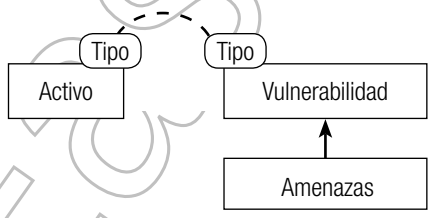


Figura 13: Relación ACTIVO-VULNERABILIDADES-AMENAZAS

En el **Anexo VII** se presenta un catálogo de vulnerabilidades para entornos de automatización y control industrial.

Tipo	Vulnerabilidad	Amenaza asociada
Hardware	Mantenimiento insuficiente	FT1
	Instalación incorrecta	FT1
	Susceptibilidad a factores ambientales	DF3
	Sensibilidad a interferencias	RA1
	Control de cambios poco eficiente	CF5
	Susceptibilidad a variaciones de voltaje	FS2
	Almacenamiento sin protección	DF5
Software	Pruebas insuficientes	CF1
	Fallos conocidos en el software	CF1
	Sesiones permanentemente abiertas	CF1

Figura 14: Ejemplo de catálogo de vulnerabilidades

Cálculo del riesgo

El riesgo, es un valor que combina el impacto (Consecuencia) que produciría el deterioro o pérdida de un activo (o grupo de activos) junto con la probabilidad de que una vulnerabilidad existente en el activo sea explotada por una amenaza.

$$\text{Riesgo} = \text{Probabilidad}_{\text{AmenazaxVulnerabilidad}} \times \text{Consecuencia}$$

En una aproximación cualitativa, la probabilidad de ocurrencia de la explotación de una vulnerabilidad por parte de una amenaza podría representarse mediante tres niveles como se indica a continuación.

Escala de probabilidad

Nivel	Descripción
Alto	Es probable que la amenaza explote la vulnerabilidad durante el próximo año
Medio	Es probable que la amenaza explote la vulnerabilidad durante los próximos diez años
Bajo	Es poco probable que la amenaza explote la vulnerabilidad y no existen datos históricos de su ocurrencia

Tabla 1: Ejemplo de escala de probabilidad

› La aproximación cualitativa a las consecuencias (impacto) del deterioro o pérdida de un activo (o grupo de activos) se podría determinar con una tabla similar a la siguiente:

Áreas de Riesgo									
	Continuidad del negocio		**Seguridad de la información**			**Seguridad en operaciones**		**Seguridad ambiental**	**Impacto nacional**
Categoría	Interrupción de la producción en una ubicación	Interrupción de la producción en múltiples ubicaciones	Coste (millones €)	Legal	Confianza del público	Personal en la ubicación	Personal fuera de la ubicación	Entorno	Infraestructuras y servicios
A (alta)	> 7 días	> 1 día	> 500	Delito grave	Daño a la imagen de marca	Muerte	Muerte o incidente grave	Citación por autoridad nacional o impacto significativo a largo plazo en el entorno	Impacto a múltiples sectores o interrupción grave de servicios públicos
B (media)	> 2 días	> 1 hora	> 5	Delito menor	Pérdida de confianza de los clientes	Heridas mayores	Quejas o impacto a la comunidad local	Citación por autoridad local	Impacto potencial sobre un sector o sobre los servicios públicos
C (baja)	< 1 día	< 1 hora	< 5	N/A	N/A	Heridas	No hay quejas	Daños pequeños y contenidos	Pequeño impacto a un sector o a los servicios públicos

Tabla 2: Ejemplo de escala de consecuencias

Esta tabla es un ejemplo de las posibles consecuencias causadas por diferentes áreas de riesgo creadas por incidentes de cualquiera de las tres dimensiones de la seguridad, que pueden afectar a una instalación industrial. Este ejemplo puede ser ampliado y calibrado para ajustarlo a las necesidades de cada organización.

A partir de las tablas propuestas se puede realizar un sencillo cálculo del riesgo de manera similar a la establecida en la siguiente tabla:.

		Categoría de Consecuencias		
		A	B	C
Probabilidad	Alta	Riesgo alto	Riesgo alto	Riesgo medio
	Media	Riesgo alto	Riesgo medio	Riesgo bajo
	Baja	Riesgo medio	Riesgo bajo	Riesgo bajo

Tabla 3:. Ejemplo de matriz de riesgo

Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial
Tratamiento del riesgo

TRATAMIENTO DEL RIESGO

La eliminación total del riesgo es virtualmente imposible, ya que, debido a la complejidad de los entornos industriales, siempre existirán amenazas y vulnerabilidades con el potencial de afectar al correcto funcionamiento de los procesos industriales. Para realizar el tratamiento del riesgo, debe determinarse cuáles son los riesgos prioritarios que deben ser tratados con el fin de reducirlos a un nivel aceptable. Esta selección de los riesgos estará guiada por los riesgos de mayor nivel, pero también se tendrán en cuenta los que puedan ser tratados obteniendo una solución rápida (quick-wins), ya que su reducción contribuirá a hacer visibles y difundir entre la organización los resultados del sistema de gestión de la ciberseguridad industrial.

La decisión de qué contramedidas se deben implementar se realizará teniendo en cuenta el equilibrio entre coste, beneficio y operación. En los entornos industriales, el factor fundamental es garantizar que la operación de los sistemas no se verá afectada por la implantación de la contramedida.

Las contramedidas pueden adoptar la forma de nuevos dispositivos, cambios a la configuración, desarrollo y aplicación de procedimientos o cualquier otro elemento o variación en la instalación que contribuya a la disminución del riesgo.

Una posible clasificación de las contramedidas aplicables a los entornos industriales es la propuesta en [3]:

Control de Acceso	
Autenticación e identificación de usuarios	Se debe identificar y autenticar de manera única e inequívoca a sus usuarios.
Gestión de cuentas	Se debe gestionar las cuentas de usuarios, incluyendo la generación, activación, modificación, desactivación y borrado.
Políticas de acceso	Debe garantizarse el cumplimiento de las políticas de acceso
Gestión de identificadores	Se deben gestionar los identificadores por usuario, grupo, role o sistema.
Gestión de mecanismos de autenticación	Se debe ser capaz de inicializar el contenido del autenticador (contraseña, token, certificado, biométrico, etc.), modificar su valor por defecto tras la instalación y cambiarlo periódicamente.
Autenticación segura	No se debe proporcionar información durante el proceso de autenticación, por ejemplo, ocultando la contraseña cuando el usuario la introduce.
Accesos sin éxito	Se debe ser capaz de establecer un límite al número de intentos de autenticación fallidos. Superado el límite el sistema debe denegar el acceso temporal o permanentemente.
Notificación de uso del sistema	El sistema debe tener la capacidad de mostrar un mensaje de notificación ante la entrada de usuarios que indique que el uso del sistema puede estar monitorizado, el acceso por partes no autorizadas está prohibido y sujeto a penas.
Notificación de login previo	El sistema, tras la entrada de un usuario, debe notificarle la fecha y hora de la última entrada, así como el número de intentos de acceso fallidos.
Bloqueo de sesiones	El sistema debe ser capaz de prevenir accesos al sistema mediante el bloqueo de la sesión tras un tiempo de inactividad.
Terminación de la sesión remota	El sistema terminará de manera automática las sesiones remotas tras un periodo de inactividad.
Acceso remoto	El sistema proporcionará la capacidad de monitorizar y controlar todos los métodos de acceso remoto.
Identificación y autenticación de dispositivos	Los dispositivos que intercambian información con los SGCI deben estar previamente identificados y autorizados.

Tabla 4: Medidas de control de acceso lógico

Control del uso	
Restricciones de acceso inalámbrico	Deben restringirse las condiciones de utilización de conexiones inalámbricas, así como autorizar y monitorizar su uso; y utilizar mecanismos de autenticación adecuados para proteger los accesos inalámbricos.
Control de la utilización de dispositivos portátiles	Deben restringirse las condiciones de uso de dispositivos portátiles y proporcionar la capacidad de monitorizar su utilización.
Código móvil	Deben establecerse restricciones para la utilización de código móvil (Java, Javascript, ActiveX, PDF, Flash, etc.), así como monitorizar su uso.
Control de sesiones concurrentes	Debe limitarse el número de sesiones concurrentes de cada usuario.
Auditoría	El sistema debe ser capaz de generar registros de auditoría, al menos para: control de acceso, errores, eventos del sistema, cambios de configuración. Los registros, contendrán al menos los siguientes campos: día y hora, origen del evento, categoría, tipo, identificador del evento.
Capacidad de almacenamiento de auditoría	El sistema debe proporcionar capacidad suficiente para almacenar los registros de auditoría de acuerdo a las recomendaciones comunes de gestión de logs.
Respuesta a fallos en el proceso de auditoría	El sistema debe ser capaz de alertar de errores producidos durante la generación de registros de auditoría. Como mínimo será capaz de sobrescribir registros antiguos cuando se llegue a la capacidad máxima de almacenamiento.
Marcas de tiempo	El sistema debe ser capaz de generar marcas de tiempo precisas para su utilización en los registros de auditoría.
Protección de la información de auditoría	El sistema debe proteger la información y herramientas de auditoría de accesos no autorizados.
No repudio	El sistema debe ser capaz de determinar si un usuario dado ha realizado una acción particular.

Tabla 5: Medidas de control del uso de recursos tecnológicos

Integridad de datos	
Integridad de las comunicaciones	El sistema debe proteger la integridad de la información que transmite.
Protección contra código malicioso	El sistema incorpora mecanismos de protección contra código malicioso.
Verificación de la funcionalidad de seguridad	El sistema debe proporcionar mecanismos para soportar la verificación de las funciones de seguridad y emitir alertas en caso de que se descubran anomalías.
Integridad del software y la información	El sistema debe detectar, registrar, reportar y proteger contra cambios no autorizados al software y la información.
Uso de correo electrónico en el sistema de control	Deben incorporarse sistemas para prevenir la introducción de malware a través de mensajes de correo electrónico.
Restricciones a la entrada de información	El sistema sólo aceptará entradas procedentes de entidades autorizadas, excepto para los propósitos de autenticación inicial.
Autenticidad e integridad de la información	El sistema comprobará la integridad y autenticidad de cualquier información generada en fuentes externas y que son utilizadas como entradas al sistema.
Manejo de errores	El sistema identificará y gestionará condiciones de error en hardware y software, de manera que no se proporcione información que pueda ser explotada por adversarios para atacar el sistema.
Autenticidad de sesiones	El sistema proporcionará mecanismos para proteger la autenticidad de las comunicaciones de sesiones.

Tabla 6: Medidas de integridad de datos

Confidencialidad de datos	
Persistencia de la información	El sistema debe prevenir el envío de información no autorizada a través de recursos del sistema.
Confidencialidad de la comunicación	El sistema protegerá la confidencialidad de la información transmitida.
Gestión de claves criptográficas	Donde se requieran capacidades criptográficas, el sistema debe ser capaz de gestionar sus claves mediante mecanismos automatizados.
Uso de criptografía	El sistema implementará capacidades criptográficas cuando se requiera garantizar la confidencialidad de los datos que éste gestiona.
Certificados PKI	Cuando se utilice criptografía asimétrica, el sistema deberá ser capaz de interactuar con la PKI existente en la organización para obtener las claves públicas requeridas.

Tabla 7: Medidas de confidencialidad de datos

Restricción del flujo de datos	
Control del flujo de información	El sistema utilizará autorizaciones asignadas para controlar el flujo de información entre zonas de acuerdo a la política aplicable.
Particionado de aplicaciones	El sistema soportará el particionado de datos, aplicaciones y servicios.
Aislamiento de las funciones de seguridad	El sistema deberá aislar las funciones de seguridad de las que no lo son.
Protección de límites	El sistema monitorizará y controlará las comunicaciones entre zonas.

Tabla 8: Medidas de restricción del flujo de datos

Respuesta a eventos	
Generación de informes	El sistema debe proporcionar acceso a los registros de auditoría para permitir a herramientas externas la generación de informes.
Técnicas y herramientas de monitorización	El sistema debe permitir el uso de técnicas y herramientas para la monitorización continua de su funcionamiento.

Tabla 9: Medidas de respuesta a eventos

Disponibilidad de recursos	
Protección ante denegación de servicio	El sistema debe proporcionar protección contra los efectos de denegaciones de servicio intencionales o casuales.
Gestión de los recursos de red	El sistema debe limitar el uso de los recursos de red para evitar interferencias en su correcto funcionamiento.
Copias de seguridad	El sistema debe soportar la identificación de sus archivos críticos y permitir la realización de copias de seguridad.
Recuperación del sistema	El sistema debe proporcionar mecanismos para la recuperación del sistema a un estado seguro tras un fallo o mal funcionamiento.
Suministro eléctrico de emergencia	El sistema debe soportar la conmutación automática a y desde una fuente de suministro eléctrico de emergencia sin afectar a la seguridad o funcionamiento del sistema.
Configuración de red y seguridad	El fabricante del sistema debe proporcionar recomendaciones para la configuración de la red y el sistema. El sistema proporcionará mecanismos para realizar la configuración.
Mínima funcionalidad	El sistema proporcionará las capacidades necesarias para prohibir y/o restringir el uso de funciones, puertos, protocolos y servicios innecesarios.
Inventario de componentes	El sistema proporcionará la capacidad de reportar la lista de componentes instalados y sus propiedades asociadas.

Tabla 10: Medidas de disponibilidad de recursos

3

Dominio 3:
Promoción de una Cultura de la Ciberseguridad Industrial

CONTENIDO

CONTEXTO

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ESTABLECIMIENTO DE LA NORMATIVA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS
COMPROBACIÓN DE ANTECEDENTES
DESCRIPCIÓN DE LOS PUESTOS DE TRABAJO
ESTABLECIMIENTO DE RESPONSABILIDADES DE SEGURIDAD
REVISIÓN PERIÓDICA DE PERMISOS
SEGREGACIÓN DE TAREAS
SUPERVISIÓN DEL USO DE LOS SISTEMAS
USO ACEPTABLE DE RECURSOS

FORMACIÓN Y CONCIENCIACIÓN

ACCIONES DE CONCIENCIACIÓN
ACCIONES FORMATIVAS

Dominio 3: Promoción de una Cultura de la Ciberseguridad Industrial

Contexto

CONTEXTO

El presente capítulo de esta guía describe el tercero de los dominios del marco de referencia del SGCI: **Gestión de los Riesgos para la Ciberseguridad Industrial**.

Figura 15: Marco de referencia del SGCI. Dominio 3

Este documento define cuales deben ser las medidas que deben ser implantadas para garantizar la ciberseguridad de la instalación industrial en lo relacionado con la seguridad del personal y la formación y concienciación del mismo.

No es objeto de este documento establecer las maneras en las que dichas medidas se implantarán, sino establecer su ámbito y propósito general. Para cumplir con lo establecido en este documento, la organización deberá desarrollar políticas que hagan efectivas las medidas aquí planteadas. Como ejemplo de dichas políticas se proporcionan los siguientes documentos que pueden resultar de valiosa ayuda a la hora de ejecutar su desarrollo:

› **Anexo IX** – Seguridad de personal.

› **Anexo X** – Formación y concienciación.

Los controles establecidos en estos anexos serán consolidados en la sección "Contramedidas" del **Anexo VII** "Amenazas y Vulnerabilidades en el ámbito industrial".

Seguridad ligada a los recursos humanos

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Debe establecerse un marco para la seguridad de personal en el que se determine la manera en que el personal que gestiona, opera y mantiene los sistemas de automatización y control industrial debe realizar su trabajo para garantizar la seguridad de los sistemas y la instalación.

La Seguridad de personal debe contemplar al menos los siguientes aspectos:

Establecimiento de la política de seguridad ligada a recursos humanos

La política debe establecer claramente el compromiso de la organización con la seguridad y cuáles son las responsabilidades, en cuanto a ciberseguridad de todo el personal, incluyendo empleados, contratistas, proveedores y terceras partes.

Dicha Política debiera recoger aspectos relativos a:

- La seguridad física.
- La seguridad de la información.
- El uso correcto de los recursos puestos a disposición de los usuarios por la organización.
- Compromisos de confidencialidad.
- Las Incidencias de seguridad.

Igualmente debieran establecerse las acciones disciplinarias a emprender por la Organización ante incumplimientos de dicha Política.

Comprobación de antecedentes

Cuando la criticidad de los sistemas a los que el personal tendrá acceso lo justifique, y siempre de acuerdo a la legislación vigente, se comprobará la identidad, cualificación y credenciales de todo el personal cuyo trabajo implique acceso físico o lógico a los sistemas de automatización y control industrial. El objetivo de esta comprobación será verificar la capacidad, conocimientos, experiencia y adecuación del trabajador para realizar las tareas que le han sido asignadas. Con el fin de garantizar que la comprobación se realiza de manera adecuada, deberá integrarse dentro del procedimiento de contratación utilizado por la organización. [1]

La profundidad de la comprobación de antecedentes dependerá del nivel de criticidad asociado al puesto que el empleado va a desempeñar. Al menos consistirá en la verificación de la identidad y de las cualificaciones profesionales presentadas, pero si así se considerara necesario, podría incluir la investigación de antecedentes penales y la veracidad del currículo profesional presentado.

Descripción de los puestos de trabajo

Todos los puestos de trabajo relacionados con la gestión, operación o mantenimiento de los sistemas de automatización y control industrial deben estar claramente definidos, estableciendo de manera concisa y objetiva cuáles son las tareas que deben realizarse en cada puesto.

Establecimiento de responsabilidades de seguridad

Las descripciones de todos los puestos de trabajo relacionados con la gestión, operación o mantenimiento de los sistemas de automatización y control industrial deben incluir de manera específica las responsabilidades de seguridad asociadas al puesto. La descripción de las responsabilidades debe establecer de manera inequívoca cuáles son las expectativas que, en materia de ciberseguridad, la organización tiene respecto a cada puesto de trabajo.

El establecimiento de responsabilidades de seguridad no se limitará a los empleados de la organización, sino que deberá incluir a terceras partes relacionadas con la gestión, operación o mantenimiento de los sistemas de control industrial.

Revisión periódica de permisos

Los permisos de acceso por parte de los usuarios a los sistemas de control industrial deben ser revisados periódicamente con el fin de garantizar que son los necesarios y suficientes para la realización de las tareas y cumplimiento de las responsabilidades del usuario.

Segregación de tareas

Las tareas relacionadas con la gestión, operación y mantenimiento de los sistemas de control y automatización industrial deben estar repartidas entre distintos puestos de trabajo de manera que se evite que un solo individuo tenga control total sobre acciones capaces de cambiar la operativa y funcionamiento de los sistemas.

Supervisión del uso de los sistemas

La supervisión del uso de los sistemas de control y automatización industrial deberá realizarse con carácter periódico, mediante la revisión y análisis de los registros de seguimiento existentes, estableciéndose dicha periodicidad en función de los correspondientes análisis de riesgos realizados, y teniendo en cuenta principalmente la criticidad de la disponibilidad de los procesos y servicios.

Por ello el derecho a dicha supervisión debe quedar expreso en la Política de Personal

Uso aceptable de recursos

La política de uso aceptable de recursos tiene como objetivo establecer las normas de uso correcto de los distintos recursos puestos a disposición de los usuarios de la organización. Esta política contemplará, al menos, los siguientes aspectos:

- Conexión de sistemas a las redes de control: Se definirán las condiciones en las que resultará aceptable la conexión de un sistema o dispositivo a la red de control, estableciéndose un procedimiento que garantice que dicha conexión se realizará de manera que no se comprometa la seguridad de las redes o sistemas de la organización.

Dominio 3: Promoción de una Cultura de la Ciberseguridad Industrial

Formación y concienciación

FORMACIÓN Y CONCIENCIACIÓN

La formación y la concienciación del personal son aspectos críticos para garantizar la ciberseguridad de las instalaciones industriales, ya que, en gran medida, aquella dependerá de las acciones realizadas por el personal durante el desempeño de sus funciones laborales.

Mediante la formación y la concienciación se busca:

- Mejorar la concienciación general sobre ciberseguridad para proteger recursos y sistemas.
- Desarrollar habilidades y conocimientos que permitan que los trabajadores realicen sus tareas de manera más eficiente y segura.

En el ámbito que nos ocupa, la formación y concienciación tiene una característica fundamental que contribuye a incrementar su complejidad, se trata de la necesidad de afrontar las acciones de formación y concienciación desde dos vertientes diferentes:

- Formación en ciberseguridad y tecnologías de la información para el personal relacionado con los sistemas de control y automatización industrial.
- Formación para el personal de tecnologías de información, en aspectos específicos del entorno industrial, incluyendo tecnologías de automatización y control industrial, seguridad física y procesos industriales.

La necesidad de afrontar todas las acciones de formación y concienciación desde ambos puntos de vista, añade complejidad a una tarea de por si complicada, por lo que deberá prestarse una especial atención a los perfiles de los destinatarios de las acciones formativas durante el desarrollo de sus contenidos.

Las acciones de formación y concienciación deben suponer un esfuerzo continuado con el fin de garantizar la permanencia de sus efectos, y que estos no se diluyan a lo largo del tiempo. Por ello, el responsable del sistema de gestión de ciberseguridad industrial, tendrá entre sus responsabilidades, planificar a lo largo del tiempo este tipo de acciones.

Acciones de concienciación

Las acciones de concienciación están destinadas a mantener alerta de las implicaciones de ciberseguridad a todos los empleados implicados en la operación, gestión y mantenimiento de los sistemas de control industrial.

Las acciones de concienciación incluirán, al menos, los siguientes aspectos:

- Información acerca de qué se considera un incidente de ciberseguridad y cómo detectarlo.
- Formas, canales y vías para el reporte de incidentes de ciberseguridad.
- Posibles consecuencias e impactos de incidentes de ciberseguridad.

Las acciones de concienciación deben realizarse con frecuencia y suponer una carga mínima para los receptores de las mismas.

Los métodos por los que se realizarán estas acciones son diversos, incluyendo:

- Notas en la intranet u otros métodos online (boletines, correos electrónicos, …).
- Posters.
- Avisos de audio.
- Videos (en relación principalmente con incidentes acaecidos de carácter público).

Acciones formativas

Las acciones formativas tienen como objetivo lograr que los trabajadores relacionados con la operación, mantenimiento y gestión de los sistemas de control industrial adquieran los conocimientos necesarios para garantizar la ciberseguridad de dichos sistemas.

Las acciones formativas deben ser diseñadas teniendo en cuenta el perfil y las competencias de los destinatarios de las mismas, y deben tener en cuenta las procedencias de los implicados, garantizando que los trabajadores procedentes del mundo de las tecnologías de la información adquieran conocimientos de sistemas de control industrial, y que los procedentes de las tecnologías de operación adquieran conocimientos de ciberseguridad.

En el diseño, selección y evaluación de las acciones formativas deben estar implicados los responsables de los departamentos que realicen la operación, mantenimiento y gestión de los sistemas de control industrial.

Las acciones formativas, se realizarán en forma de seminarios, cursos, talleres prácticos o laboratorios.

Con el fin de mantener un control sobre los conocimientos adquiridos por los trabajadores, se deberá mantener un registro de las acciones formativas realizadas por los trabajadores de la organización.

4

Dominio 4:
Establecimiento de Medidas de Ciberprotección en Instalaciones Industriales

DOMINIO 4: ESTABLECIMIENTO DE MEDIDAS DE CIBERPROTECCIÓN EN INSTALACIONES INDUSTRIALES

CONTEXTO

MEDIDAS DE CLASIFICACIÓN Y PROTECCIÓN DE DATOS E INFORMACIÓN

MEDIDAS DE CONTROL DE ACCESO LÓGICO

ADMINISTRACIÓN DE CUENTAS
AUTENTICACIÓN
AUTORIZACIÓN

MEDIDAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

ORGANIZACIÓN DE LA SEGURIDAD FÍSICA
ÁREAS FÍSICAS
CONTROL DE ACCESO FÍSICO
DETECCIÓN DE INTRUSIONES FÍSICAS

MEDIDAS DE PROTECCIÓN DE LAS REDES DE COMUNICACIONES

JERARQUÍA DE NIVELES EN EL CONTROL DE PROCESOS INDUSTRIALES
REDES DE CAMPO
REDES DE CONTROL
REDES DE SUPERVISIÓN
REDES DE PROCESO
REDES DE OPERACIÓN
REDES DE INFORMACIÓN
REDES CORPORATIVAS Y REDES DE ÁREA AMPLIA (WAN)

SEGMENTACIÓN DE REDES
CRITERIOS DE UBICACIÓN
MODELOS DE SEGMENTACIÓN

REDES INALÁMBRICAS
PLAN DE DIRECCIONAMIENTO

MEDIDAS DE PROTECCIÓN DEL SOFTWARE

MEDIDAS DE CIBERSEGURIDAD EN LAS RELACIONES CON TERCEROS

Dominio 4: Establecimiento de Medidas de Ciberprotección en Instalaciones Industriales

Contexto

CONTEXTO

El presente capítulo de esta guía describe el cuarto de los dominios del marco de referencia del SGCI: **Gestión de los Riesgos para la Ciberseguridad Industrial**.

Figura 16: Marco de referencia del SGCI. Dominio 4

Este documento establece los contenidos mínimos que deberían contemplar las medidas de Ciberseguridad de una instalación industrial en lo relativo a aspectos como:

- la clasificación y salvaguarda de los datos e información generados por el proceso industrial, así como los empleados en el control del propio proceso;
- la prevención de accesos lógicos no autorizados a los sistemas de control industrial;
- la seguridad física de dichos sistemas y su entorno;
- la protección de las redes de comunicaciones;
- las medidas para la protección del software de control industrial; o,
- la interacción con terceros, dentro de la actividad de automatización del proceso industrial.

No es objeto de esta guía describir dichas medidas de forma detallada, sino, únicamente, ofrecer una orientación sobre su ámbito y propósito general. Consecuentemente, para cumplir con lo establecido en este documento, la organización deberá desarrollar su propia medida específica, que haga efectivos los controles que se quieren adoptar. A ese fin, y como anexo a esta guía, se proporcionan los siguientes documentos que pueden resultar de utilidad a la hora de abordar el desarrollo de su normativa en su propia organización:

- **Anexo XI**. Procedimiento de administración de cuentas de usuario.
- **Anexo XII**. Directrices de segmentación de redes.
- **Anexo XIII**. Plan de direccionamiento.

Los controles establecidos en estos anexos, serán consolidados en la sección “Contramedidas” del **Anexo VII** de la guía general “Vulnerabilidades y Amenazas en el ámbito industrial”.

Medida de clasificación y protección de datos e información

MEDIDA DE CLASIFICACIÓN Y PROTECCIÓN DE DATOS E INFORMACIÓN

En el entorno industrial resultará clave fijar **directrices que permitan la clasificación y salvaguarda de los datos, información u otros activos digitales** generados por el proceso industrial, así como los empleados en el control del propio proceso. Dicha clasificación favorecerá el establecimiento de las pertinentes medidas de control, en cada caso. Asimismo, proporcionará garantía de que la protección es apropiada para todos los activos, de acuerdo a su categoría o clasificación.

Los diferentes sistemas de control, presentan diferentes criticidades. De igual modo, a la información y los datos que tratan corresponderán grados de sensibilidad diferentes, atendiendo a criterios como su importancia, criticidad o ubicación. Deberá, por tanto, realizarse una identificación y clasificación de estos activos que permita definir un conjunto adecuado de niveles de protección.

Una posible aproximación puede ser la ofrecida por la tabla 1, a continuación. En ella se detallan una serie de niveles que atienden al grado de sensibilidad de los sistemas de control industrial, desde el punto de vista de la ciberseguridad, en el contexto del proceso industrial al que dan servicio.

Categoría	Impacto	Sensibilidad
I	Bajo	Baja
II	Significativo	Moderada
III	Crítico	Alta

Tabla 11: Categorías de sistemas de control industrial, según su sensibilidad en el contexto del proceso industrial

De ese modo, se tendría que un activo de control industrial caería en la:

- Categoría I (sensibilidad BAJA), cuando un impacto potencial, sobre la ciberseguridad de tal activo, resultase BAJO, con efectos adversos limitados sobre el proceso industrial al que sirve; esto es, cuando se requiriesen reparaciones o acciones correctivas menores, asumibles de manera autónoma;
- Categoría II (sensibilidad MODERADA), cuando un impacto potencial, sobre la ciberseguridad de tal activo, resultase SIGNIFICATIVO, con efectos adversos serios sobre el proceso industrial al que sirve; esto es, cuando se requiriesen reparaciones o acciones correctivas más extensas que pudiesen requerir la colaboración de terceros; y,
- Categoría III (sensibilidad ALTA), cuando un impacto potencial, sobre la ciberseguridad de tal activo, resultase CRÍTICO, con efectos adversos graves o catastróficos para el proceso industrial al que sirve (e incluso para instalación, o para terceros); esto es, cuando, por ejemplo, sea causa de interrupción de la actividad productiva en el centro/planta en la que está ubicado por un tiempo prolongado, afecte a la integridad física de las personas o suponga la pérdida de los principales bienes de la organización propietaria, requiriendo necesariamente la intervención de terceros (autoridades u otros).

Ese **inventario de activos**, que habrá de mantenerse en todo momento actualizado, contemplará no sólo datos vinculados al proceso industrial en cuestión, sino también documentación, manuales, software, hardware, configuración y cualquier otro elemento que contribuya a la sostenibilidad del proceso industrial.

Paralelamente, habrán de **identificarse los propietarios y/o custodios de los referidos activos**. Ello favorecerá el incremento del grado de implicación individual (imputabilidad) en la misma. Todos los activos tendrán un custodio, responsable de aplicar las medidas que garanticen su seguridad, aunque será el propietario de los activos, el responsable último de rendir cuentas (imputable) por su seguridad.

También serán los propietarios de los activos los responsables de su clasificación/categorización, la cual habrá de revisarse periódicamente, con objeto de no caer en una “sobre clasificación” o “sobreprotección”.

Medida de control de acceso lógico

MEDIDA DE CONTROL DE ACCESO LÓGICO

El establecimiento de una medida de control de acceso lógico a los sistemas de automatización de un proceso industrial, responde a un múltiple objetivo que pasaría por varios frentes: desde controlar el acceso a la información u otros activos de la organización, evitando accesos no autorizados o de usuarios no autorizados a equipos, sistemas o redes; hasta garantizar la seguridad de la información cuando se utiliza informática móvil y teletrabajo; pasando por la detección de actividades no autorizadas.

La medida de control de accesos deberá tener en cuenta la categorización de los sistemas de automatización industrial que se haya establecido previamente, en función de los niveles de sensibilidad de cada uno de ellos ante impactos que afecten a su ciberseguridad.

Asimismo, el acceso lógico a los sistemas de control industrial debería concederse sobre la base de los requisitos del proceso industrial objeto de dicho control y, por extensión, de la propia organización, resumidos en el principio de "mínimo privilegio"; esto es, todo individuo debería tener una libertad de acceso restringida específicamente a cuanto requiera para el desempeño de su labor profesional. (¡Pero no más amplia que eso!). Los procedimientos formales de asignación de derechos de acceso a los referidos sistemas y equipos, habrían, por tanto, de seguir el citado principio.

Por tal motivo, habrían de ser los representantes al más alto nivel de la organización -o, por delegación de su autoridad, los dueños de los procesos industriales específicos- quienes estableciesen las responsabilidades generales sobre los criterios de autorización de los accesos.

El control de acceso permite supervisar cuando, quién, o qué, puede acceder a los equipos e instalaciones, y la manera en la que se realiza dicho acceso.

Las medidas de control de acceso deben definir cuáles son las reglas de control y los mecanismos para aplicarlas. Además, deben ser comunicadas a todo el personal que requiera acceder a los sistemas o las instalaciones, incluyendo personal interno, trabajadores temporales, contratistas u otros terceros.

Se deberán contemplar los siguientes aspectos clave en la elaboración de las normas de control de acceso lógico:

- la administración de cuentas;
- la autenticación; y,
- la autorización.

Administración de cuentas

Por norma general, en los sistemas de control industrial, la administración de cuentas está dirigida por las acciones que el propietario de la cuenta realizará sobre el sistema, en vez de por la información a la que accederá, como es habitual en los entornos de TI tradicionales.

La organización debe establecer una serie de reglas que permitan determinar el tipo de privilegios de acceso de los usuarios a los sistemas y las instalaciones. Como se ha indicado, dichas reglas se construirán de acuerdo al principio de mínimo privilegio; pudiendo ser estos privilegios relativos a:

- acciones sobre el sistema;
- acceso a información;
- horarios de acceso; u,
- otros.

Otro aspecto importante es que, siempre que sea posible, habrán de incluirse criterios de segregación de funciones, con el fin de separar tareas "incompatibles": por ejemplo, las de ingeniería/mantenimiento, de las de operación de una línea de producción.

Deberá existir un proceso administrativo que dirija la creación de las cuentas de usuario. El proceso definirá un flujo de trabajo que incluirá, al menos, los siguientes pasos:

- Solicitud.
- Revisión.
- Aprobación/Denegación.
- Aplicación (alta del nuevo usuario y/o sus nuevos privilegios de acceso).

Autenticación

Los trabajadores con acceso a los sistemas de la instalación industrial deberán tener una identidad única que les permita identificarse inequívocamente ante los sistemas.

Los mecanismos de autenticación de los sistemas deberán permitir contraseñas complejas, en cuanto a longitud y alfabeto, para resistir ataques de fuerza bruta y diccionario. Asimismo, deberán utilizar mecanismos criptográficos, al menos durante los procedimientos de autenticación.

Autorización

Para facilitar la asignación de privilegios a los usuarios de los sistemas, se recomienda la definición de roles que agrupen privilegios y autorizaciones requeridas para hacer trabajos determinados, y, posteriormente, se asocien los identificadores de usuario correspondientes a los roles definidos.

Medida de seguridad física y del entorno

MEDIDA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Entre los objetivos de toda medida de seguridad física y del entorno han de contarse: prevenir, disuadir e impedir actos deliberados con el fin de producir daños generados tanto en el exterior como en el interior de las instalaciones de la organización; de manera específica, evitar accesos no autorizados que lleven a usos indebidos, daños o interferencias en los sistemas de control industrial y, en última instancia, en la producción misma; proteger las instalaciones (salas eléctricas y/o de mantenimiento, salas de control, …) que albergan equipos y sistemas de control industrial susceptibles de robo, sabotaje, etc.; y, en suma, salvaguardar la continuidad de la actividad productiva.

Las medidas de seguridad física deberán ser capaces de lograr que el tiempo mínimo requerido, por un intruso capaz y motivado, para alcanzar componentes, equipos y sistemas vitales para la organización sea significativamente superior al tiempo mínimo necesario para que los mecanismos de respuesta entren en funcionamiento y neutralicen la amenaza.

Las medidas de seguridad física deberán proporcionar métodos para:

- realizar un control estricto del acceso a la instalación;
- detectar y confirmar de manera rápida posibles intrusiones;
- detener a tiempo las acciones que puedan poner en peligro a la instalación o los procesos que en ella se realizan; y,
- custodiar y entregar los posibles intrusos a las autoridades correspondientes.

Organización de la seguridad física

Debe establecerse y mantenerse una organización de seguridad física, en caso de que no exista, que habrá de estar constituida, al menos, por los siguientes perfiles:

- un jefe de seguridad;
- personal (equipo) de la organización;
- personal operativo (equipo) de vigilancia.

Todo el personal implicado en la organización de la seguridad física deberá recibir formación y entrenamiento según un plan de capacitación que garantice la permanente actualización de sus conocimientos y habilidades.

Deberán existir, igualmente, procedimientos escritos que documenten la estructura de la organización de seguridad física y detallen las tareas y funciones a desarrollar por cada uno de sus miembros (perfiles). Entre ello cabría contemplar, al menos, los mostrados en la tabla 2, a continuación:

Procedimiento	Descripción
Comunicación de incidentes de seguridad	Mecanismos existentes en la organización para que los empleados y usuarios notifiquen incidentes de seguridad física. Estos incidentes incluirán los relativos a accesos no autorizados, sabotajes, pérdida, desaparición o robo de material, etc.
Plan de formación y concienciación	Planificación de acciones formativas adecuadas a cada perfil implicado en la organización de la seguridad física.
Restricción de acceso	Criterios para otorgar autorizaciones de acceso según la norma de privilegios mínimos y mecanismos para garantizar que los accesos físicos a la instalación se realizan de acuerdo a dichos privilegios.
Reglamento de visitas	Normas a cumplir por los visitantes a la instalación.
Inspección de personal	Métodos para la inspección de personas y recipientes personales (mochilas, carteras) a la entrada y salida de las zonas de seguridad de la instalación.
Verificación de antecedentes	Verificación de antecedentes penales, de acuerdo a las leyes vigentes, de empleados y personal con acceso a las zonas seguras de la instalación.
Finalización de la relación laboral (despido, jubilación, otros)	Procedimientos para la retirada de privilegios a empleados o terceros, asegurando que éstos devuelvan documentos, tarjetas, claves y otras informaciones importantes.

Tabla 12: Procedimientos de seguridad física y del entorno

Áreas físicas

Todas las áreas físicas de la instalación se clasificarán según sus necesidades de seguridad. Se propone una clasificación en tres niveles:

- Áreas Públicas: Áreas de la instalación con acceso público. No requieren medidas de seguridad específicas.
- Áreas Privadas: Áreas de la instalación accesibles sólo para personal de la organización o personal externo supervisado. Requieren medidas de control de acceso para garantizar que sólo personal de la organización (o autorizado) puede acceder a ellas.
- Áreas Vitales: Áreas que contienen sistemas, equipos, componentes, dispositivos o materiales cuyo fallo o pérdida podría suponer directa o indirectamente un riesgo para la instalación, las personas o el medio ambiente. Estas áreas requerirán medidas de seguridad física estrictas para garantizar que sólo el personal debidamente autorizado puede acceder a las mismas.

Se proponen las siguientes medidas de seguridad para áreas físicas:

Medida	Descripción
Vallado perimetral	Toda la instalación deberá estar debidamente protegida por barreras físicas que determinen el perímetro de la misma.
Aberturas del perímetro	Todas las ventanas, puertas, y otras aberturas del perímetro deberán estar convenientemente aseguradas. Las ventanas de planta baja deberán estar protegidas mediante barreras físicas y las puertas deberán estar reforzadas para retrasar una entrada forzada mediante herramientas o asaltos con vehículo.
Sistemas de CCTV	Deberán existir sistemas de circuito cerrado de televisión que den cobertura, al menos, a los puntos de entrada y salida, y a los lugares donde se realicen los procesos vitales de la instalación. Es recomendable, asimismo, que los sistemas de CCTV sean capaces de proporcionar imágenes del exterior de la instalación.
Iluminación	Los sistemas de iluminación deben abarcar las áreas donde se realicen trabajos o haya tránsito de personal. Además, deben proporcionar cobertura exterior e interior que permita el correcto funcionamiento de los sistemas de CCTV.
Alarmas	El perímetro deberá disponer de sensores capaces de activar alarmas en caso de que se produzca un intento de acceso no autorizado. Las alarmas deberán estar gestionadas desde una consola centralizada.

Tabla 13: Medidas de seguridad física y del entorno

Control de acceso físico

Las medidas de control de acceso son mecanismos fundamentales para garantizar la seguridad de la instalación. Todos los puntos que den paso a las áreas privadas y vitales deben disponer de mecanismos de control de acceso en los que se verifique que las personas que solicitan el acceso tienen la autorización necesaria para hacerlo y se cumplan las condiciones del acceso como las áreas visitadas, el tiempo máximo de permanencia y cualquier otra información necesaria para garantizar la seguridad de la instalación.

En toda entrada y salida a las áreas vitales debe realizarse un proceso de inspección acorde con la normativa laboral vigente. Este proceso deberá revisar paquetes, bolsas y objetos transportados para garantizar que éstos o sus contenidos no pueden dañar a la instalación o a sus contenidos.

Detección de intrusiones físicas

Un factor determinante para gestionar correctamente los incidentes de seguridad física es la capacidad de detección temprana de intrusiones. Debido a esto, es importante disponer de sistemas y procedimientos que garanticen que los intentos de intrusión sean detectados en un tiempo tal que se garantice una respuesta adecuada al incidente.

Debido a la importancia de su contenido, las áreas vitales deberán contar, al menos, con dos tecnologías diferentes, alternativas, de detección de intrusiones.

Medida de protección de las redes de comunicaciones

MEDIDA DE PROTECCIÓN DE LAS REDES DE COMUNICACIONES

Las comunicaciones a través de redes de datos son, sin lugar a dudas, un elemento crucial -si no el más determinante- desde el punto de vista de la problemática de la ciberseguridad en los entornos industriales. Ello viene motivado porque, junto a su capacidad habilitadora de las soluciones de automatización industrial, lleva asociado el peligro de constituirse en puerta de entrada de posibles visitas no deseadas.

Una medida de protección de las redes de comunicaciones en el contexto industrial buscará, por tanto, salvaguardar las redes y resto de infraestructuras de soporte de las comunicaciones, dentro y fuera de la planta, y prevenir, disuadir y evitar esos accesos no autorizados.

Una medida tal, deberá, a su vez, tener en cuenta el amplio abanico de posibilidades de conexión (niveles) que ofrece el escenario industrial, como recuerda la siguiente sección.

Jerarquía de niveles en el control de procesos industriales

La figura 1 ofrece una perspectiva de los diferentes niveles de control en el contexto de la automatización industrial.

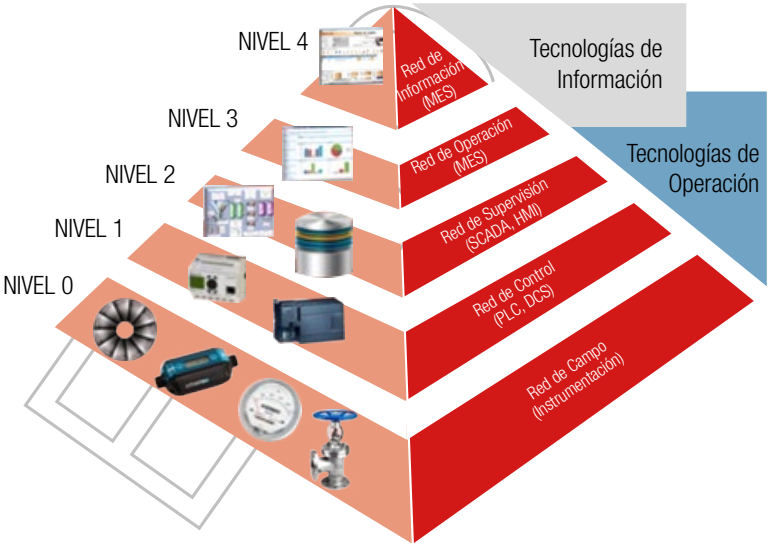


Figura 17: Pirámide de la automatización industrial (jerarquía de niveles)

Cada uno de los niveles de la pirámide de la automatización ofrecerá un plano particular en el que también estará habilitada, al menos, una categoría de comunicaciones. Se detallan en los siguientes apartados.

Redes de campo

El Nivel 0 de la anterior pirámide se corresponde con la "red de campo", donde los elementos de control son sensores o actuadores que constituyen la instrumentación de campo, básica en la jerarquía de la automatización. A ese nivel se produce una interacción directa con el proceso productivo.

Redes de control

El Nivel 1, correspondiente a la "red de control" propiamente dicha, es aquel en el que se ubican elementos como PLCs o DCSs. En este punto la interacción con el proceso productivo no es estrictamente directa, sino que se produce una "detección" y manipulación del proceso productivo a través de la recepción de valores de campo procedentes de los sensores de nivel 0 y la emisión de consignas hacia los actuadores del nivel inferior que son los que actúan directamente sobre el proceso.

Redes de supervisión

El Nivel 2 se corresponde con la "red de supervisión", en la que se encuentran los sistemas SCADA, propiamente dichos, y sus consolas de interfaz hombre-máquina (HMI, del inglés "Human-Machine Interface"). En este punto se produce la supervisión y el control automatizado del proceso productivo y en él las interacciones pueden durar desde fracciones de segundo, hasta minutos.

En la interacción entre este nivel y el nivel 1 se produce el control por lotes, el control continuo o de control discreto del proceso industrial (según sea la naturaleza de éste).

Redes de proceso

El conjunto de las redes de campo, control y supervisión constituyen la "Red de Proceso" propiamente dicha. Es el territorio natural de las Tecnologías de Operación y de los sistemas de tiempo real (o cuasi-real).

Los sistemas en estas redes requieren comunicación con los sistemas de las redes de proceso y deben ser accesibles desde la red corporativa, por tanto, el control del tráfico debe hacerse en ambos sentidos, tratando siempre de habilitar los mínimos accesos que permitan mantener la operativa normal de la instalación.

Las redes de control y supervisión, debido a la naturaleza de los sistemas que albergan (estaciones de operación, estaciones de ingeniería, historiadores, etc.) pueden estar subsegmentadas, permitiendo, de esta manera un control mucho más detallado del tráfico entre segmentos.

Los elementos del nivel superior (nivel 3), donde se localizan otros sistemas como los de ejecución de la fabricación (MES, del inglés "Manufacturing Execution Systems") forman parte, también del control del proceso, si bien pueden calificarse de sistemas fronterizos entre el territorio TO (por "abajo") y el TI (por "arriba").

Redes de operación

El Nivel 3: Se corresponde con la "red de operación", en la que estarían ubicados los sistemas de ejecución de la fabricación (MES, Manufacturing Execution Systems, por sus siglas en inglés), encargados de la gestión de las operaciones y de la fabricación.

En este punto se realizan los procesos de programación, detalle y despacho de la producción y de garantía de fiabilidad.

Los flujos de trabajo, el control para generar los productos deseados, el mantenimiento de registros de producción y la optimización del proceso se realizarían en este nivel. Dichas actividades pueden durar segundos, minutos, horas e, incluso, más de un turno.

Redes de información

En el Nivel 4, finalmente, estaría representada la "red de información" de la planta, donde habitualmente tienen su ubicación natural los sistemas ERP y otras soluciones de negocio relacionadas con la planificación y la logística.

Son propias de este nivel 4 las actividades de programación y seguimiento de la producción de la planta. Se establece la programación básica de la planta, el uso de materiales y su distribución, en procesos que duran días, semanas o meses.

Desde una perspectiva de la ciberseguridad industrial estas redes se consideran un entorno inseguro, ya que contienen sistemas heterogéneos que generan grandes cantidades de tráfico para múltiples aplicaciones, así como accesos remotos y multitud de usuarios, componentes todos ellos, de los que pueden proceder incidentes que afectarían a la operación de los sistemas de control.

Redes corporativas y redes de área amplia (WAN)

En los casos de grandes corporaciones cabe hablar de un nivel adicional, no reflejado en la figura. Se trataría del nivel superior en el que se localizarían las redes de información (como en el nivel 4); pero a nivel global, no a nivel particular (local) de una determinada planta. Piénsese, por ejemplo, en una organización que tuviese sus instalaciones distribuidas en varias sedes (oficinas centrales, planta industrial 1, planta industrial 2, etc.) o en un holding que agrupara varias compañías con sus diferentes factorías.

Las comunicaciones a ese nivel tendrían un tratamiento, salvando la distancia, similar al de las redes de nivel 4. Es el territorio natural de las Tecnologías de la Información.

Segmentación de redes

Una de las medidas más habituales para abordar la problemática ligada a las comunicaciones en el ámbito industrial es la segmentación de redes.

La segmentación de la red debe ser coherente con los niveles del proceso industrial, facilitando la ubicación lógica de los dispositivos atendiendo a su funcionalidad y requisitos de seguridad.

La segmentación de redes es una pieza fundamental de la arquitectura de ciberseguridad en las organizaciones industriales, ya que contribuye a mejorar la protección de los sistemas de control mediante el establecimiento de diferentes zonas de seguridad destinadas a controlar y filtrar los flujos de datos o información entre dispositivos diversos.

Según el estándar IEC 62443 2-1 se define una nomenclatura y el establecimiento de zonas y canales que facilitan la protección mediante niveles de seguridad.

Establecimiento de zonas y conductos

Para sistemas industriales de gran envergadura o complejos quizás no sea recomendable o necesario aplicar el mismo nivel de seguridad a todos sus componentes. Es por ello por lo que se crean los conceptos de Zona y Conducto los cuales deber ser identificados dentro del SuC, "**Sistema bajo Consideración**" (SuC – "System under Consideration").

Una **Zona** se define como la agrupación lógica o física de activos industriales (dichos activos puedes ser físicos, aplicaciones o información) los cuales comparten los mismos requisitos de seguridad.

Un **Conducto** es un tipo particular de zona que agrupa las comunicaciones que permiten transmitir información entre diferentes zonas.

Por último, se agrega el concepto de **Canal** el cual se define como un determinado vínculo de comunicación establecido dentro de un conducto.

Zonas

Las zonas pueden ser una agrupación de activos independientes, un grupo de subzonas o una combinación de ambos. A su vez, las zonas poseen atributos de herencia, lo cual significa que las zonas "hijas" (o subzonas) deben cumplir con todos los requisitos de seguridad de su zona "padre". Cuando nos referimos a activos, hacemos alusión a "activos necesarios para el proceso industrial" lo cual definiremos como "todo elemento perteneciente a un sistema industrial (PLCs, RTUs, estaciones de operación e ingeniería, equipamiento de comunicaciones etc.) que tiene valor o potencial valor para una organización". Las cotas en el valor a partir de cuándo un elemento es considerado activo varían dependiendo de las organizaciones y su magnitud.

Cada zona posee un conjunto de características y requisitos de seguridad que constituyen sus atributos:

- Políticas de seguridad y niveles de seguridad
- Inventario de activos
- Requisitos de acceso y controles
- Amenazas y vulnerabilidades
- Consecuencias de una brecha de seguridad
- Tecnología autorizada
- Proceso de gestión de cambios.

Cada zona definida debe contener un documento que describa sus requisitos de seguridad y como asegurar que los niveles de riesgos tolerables son alcanzados. Este documento debe incluir, entre otros, el alcance de la zona, su nivel de seguridad, la estructura organizacional a la cual pertenece y sus responsabilidades, los riesgos asociados a la zona, la estrategia de seguridad adoptada, los tipos de actividades que son permitidas dentro de ella etc. Toda esta información debe estar documentada para cada zona ya que sirve como guía para la construcción y el mantenimiento de los activos contenidos en ella.

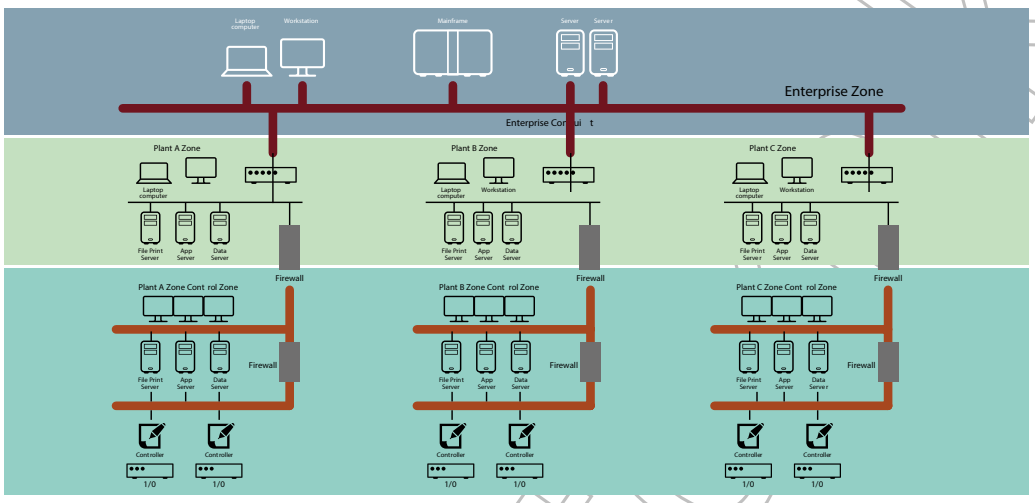
Al definir una zona, claramente estamos acotando un determinado segmento dentro del sistema y/o proceso industrial, y como consecuencia debería existir un número reducido de requisitos y medios para obtener acceso a la misma. Una política de acceso debe establecer con precisión el personal que está autorizado para acceder a cada zona, los medios a través de los cuales se realiza el acceso y los mecanismos de control sobre los mismos. Es aquí donde cobra importancia el concepto de conducto el cual desarrollaremos más adelante.

Una zona posee sus propias vulnerabilidades, y se encuentra expuesta a un determinado número de amenazas. Es por ello por lo que realizar un análisis de vulnerabilidades periódicamente sobre ellas (o sobre el proceso industrial completo) resulta de vital importancia para identificar potenciales amenazas que provoquen que los activos industriales no cumplan con sus objetivos de negocio.

Los sistemas industriales, en general, deben acompañar los cambios en las necesidades y reglas de negocio a los que pertenecen. Estos cambios pueden impactar en las diferentes zonas identificadas a partir de la incorporación de nuevas tecnologías,

necesidades extras de acceso, creación de nuevos conductos, entre otros. Resulta por ello imprescindible contar con mecanismos de control de cambios que permitan asegurar que cualquier modificación relacionada con una zona no altere los niveles de seguridad requeridos para ella.

Figura 18. Ejemplo de zonas



Conductos

Los "conductos" son zonas particulares que se aplican a procesos de comunicación específicos proporcionando funciones de seguridad que permiten a dos zonas comunicarse de manera segura. Toda comunicación entre diferentes zonas ha de realizarse a través de un conducto.

Al igual que una zona, los conductos constituyen una agrupación lógica y/o física de activos (activos de comunicación en este caso). Un "conducto de seguridad" protege la seguridad de los canales que éste contiene, de la misma manera que un conducto físico protege los cables de daños físicos.

Los conductos pueden ser pensados como los "tubos" que unen diferentes zonas o bien que son utilizados para unir componentes dentro de una misma zona. Ya sea internos (dentro de una zona) o externos (fuera de una zona) los conductos protegen los canales que proveen vínculos de comunicación entre activos industriales. Generalmente en los sistemas industriales, los conductos constituyen dispositivos de red (switches, routers, firewalls etc.) que forman parte de su arquitectura, pero en algunos casos también se pueden presentar como servidores o Gateway de comunicaciones utilizados para la conversión de diferentes protocolos.

Los conductos se utilizan como uno de los principales "inputs" para determinar las amenazas a las cuales se encuentra expuesta una zona. Identificando con claridad los conductos podremos conocer cuáles son los puntos de acceso que la zona posee, y analizar si pueden convertirse en un potencial vector de ataque. Un análisis de riesgos detallado debe incluir tanto las zonas, como sus conductos asociados para obtener mejores resultados.

Al ser un tipo particular de zona, de la misma manera que ellas cada conducto posee un conjunto de características y requisitos de seguridad que constituyen sus atributos.

- Políticas de seguridad y niveles de seguridad
- Inventario de activos
- Requisitos de acceso y controles
- Amenazas y vulnerabilidades
- Consecuencias de una brecha de seguridad
- Tecnología autorizada
- Proceso de gestión de cambios
- Zonas que interconecta
- Protocolos de comunicaciones (muy heterogéneo por la naturaleza de cada industria y fabricante)

A diferencia de las zonas, los conductos deben incluir el detalle de las diferentes zonas a las cuales interconectan, asegurando que la tecnología utilizada

para la creación de canales de comunicación cumple con los requisitos fundamentales de seguridad especificados según el nivel de seguridad asociado.

Al finalizar el análisis de Riesgos tecnológicos propuesto por la IEC-62443 se llegará a la agrupación de Zonas y Conductos óptima, de tal forma que se pueda asegurar el sistema por diseño, logrando los niveles de seguridad objetivo, y de riesgo tolerable para la organización; sin gastar de más, ni invertir de menos. Esta aproximación es válida para sistemas existentes normalmente llamados "base Instalada" o para sistemas nuevos que van cumpliendo con sus diferentes etapas de ingeniería (Ingeniería básica, ingeniería de detalle, diseño, compras, construcción, pruebas, puerta en marcha, operación, mantenimiento, hasta su retiro o decomisionado).

Niveles de seguridad

Los Niveles de Seguridad (SL, por sus siglas en idioma inglés) proveen una aproximación cualitativa para la ciberseguridad de una determinada zona. Al ser un método cualitativo, la definición de niveles de seguridad sirve para comparar y gestionar la seguridad de diferentes zonas dentro de una organización. Según el estándar es necesaria la identificación de tres tipos diferentes de niveles de seguridad:

- **Nivel de Seguridad Objetivo** (SL-T): Es el nivel de seguridad deseado para un sistema particular. Es determinado usualmente a través de la realización de evaluaciones de riesgos las cuales determinan un nivel de seguridad particular para asegurar la correcta operación.
- **Nivel de Seguridad Alcanzado** (SL-A): Es el nivel de seguridad actual para un sistema particular. Éste es medido una vez que el diseño del sistema está disponible o cuando un sistema ya se encuentra instalado. Se utilizan para establecer si la seguridad de un sistema alcanza los niveles definidos según el SL-T.
- **Nivel de Seguridad según Capacidad** (SL-C): Son los niveles de seguridad que los componentes o sistemas pueden otorgar cuando son configurados apropiadamente. Estos niveles permiten saber si un determinado sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) de forma nativa sin medidas compensatorias o contramedidas adicionales cuando es configurado e integrado apropiadamente.

Durante el proceso de diseño o adecuación, es necesario evaluar las capacidades de seguridad de cada componente o subsistema. Los proveedores o integradores del producto deberán proveer dicha información como parte de sus tareas. Esta información es de suma utilidad ya que permite determinar si un componente o sistema es capaz de alcanzar el nivel de seguridad objetivo (SL-T) deseado. Es probable que en un diseño particular haya algunos componentes o sistemas que no pueden alcanzar el SL-T. En aquellos casos en que el nivel de seguridad según capacidad (SL-C) de estos es menor al deseado como SL-T, se deberán considerar medidas compensatorias o contramedidas para reducir esa brecha. Dichas contramedidas pueden requerir cambios en los diseños e incluso la selección de componentes adicionales. Cada vez que se realice una modificación en los sistemas industriales, su nivel de seguridad debe ser evaluado obteniéndose así el nivel de seguridad alcanzado (SL-A) y comparar el mismo con el SL-T).

La siguiente figura muestra este proceso:

Figura 19. Ejemplo de zonas

Criterios de ubicación

La política de segmentación de redes deberá contener criterios objetivos que permiten determinar la correcta ubicación de un dispositivo dentro de las redes de la organización. Estos criterios deben incluir conceptos tales como los requisitos de seguridad y comunicación del dispositivo, así como atender a sus funciones dentro de la red.

Modelos de segmentación

La segmentación mínima consistirá en la separación de la red corporativa de las redes de proceso, control y supervisión,

La separación se realizará mediante un dispositivo capaz de filtrar el tráfico atendiendo a sus características (direcciones IP de origen y destino, puertos, protocolos, contexto de las aplicaciones).

Una segmentación más avanzada incluirá el despliegue de una zona desmilitarizada (DMZ) en la que se ubicarían los sistemas que requieren ser accedidos desde la red corporativa y simultáneamente necesitan acceder a sistemas ubicados en las redes de control, supervisión y proceso.

Redes inalámbricas

Las redes inalámbricas de la organización industrial deben estar correctamente identificadas, su alcance físico debe estar documentado con el fin de conocer cuál es su ámbito de actuación y por tanto los posibles puntos de la instalación desde los que la red puede ser accedida.

Siempre que una red inalámbrica forme parte de las redes de la instalación industrial, su comunicación con el resto de redes deberá estar controlada por un dispositivo de filtrado capaz de restringir los tráficos salientes y entrantes a los estrictamente necesarios y que permita contener los efectos de posibles incidentes de seguridad que ocurran en la zona inalámbrica.

Plan de direccionamiento

Debe existir un plan de direccionamiento coherente que facilite la asignación de direcciones a nuevos sistemas, y permita un crecimiento ordenado del direccionamiento utilizado por los dispositivos en la organización.

Medida de protección del software

MEDIDA DE PROTECCIÓN DEL SOFTWARE

Actualmente la operativa diaria de las organizaciones industriales, que han de competir en un mercado global, no se entiende sin la capacidad habilitadora de la tecnología. Ello convierte a la tecnología misma y a sus componentes en elementos clave sobre los que descansa una buena parte de la elasticidad de los negocios.

Dicha elasticidad, en el caso del software industrial, va más allá de los programas o aplicaciones de automatización, incluyendo también su documentación, datos y el soporte del producto necesario para garantizar el comportamiento adecuado del software, así como eliminar errores, fallos y debilidades de seguridad; es decir, proporcionar un "software resiliente" es imprescindible para garantizar las operaciones del negocio.

En el ámbito de la automatización y el control de los procesos industriales, el software se caracteriza por una serie de particularidades específicas, entre las que cabría señalar:

- largos períodos de uso/servicio de las soluciones de automatización desplegadas;
- escasa (nula) disciplina de actualización de versiones del software base y de aplicación de que están dotados los elementos y equipos de control, en aras de la disponibilidad plena;
- primacía de la fiabilidad (de nuevo, en busca de la plena disponibilidad) frente a la [ciber-]seguridad de los sistemas de control de procesos;
- mantenimiento, por lo general, externalizado en el fabricante o integrador.

Todo lo cual contribuye a la necesidad de identificar medidas específicas que den cobertura a las mejores prácticas en materia de ciberprotección de este tipo de activos.

Medidas recomendadas:

- Identificar las aplicaciones que se están ejecutando en los sistemas, así como los proveedores del software, su instalación y mantenimiento.
- Contactar con cada uno de los proveedores para conocer su estrategia de actualización y herramientas recomendables para facilitar la preparación y actualización.
- Realizar un análisis de riesgos de las distintas alternativas con la información recopilada.
- Realizar pruebas de seguridad y análisis de código fuente de software.
- Establecer un plan de actualización en aquellos sistemas en los que sea posible llevar a cabo la operación de actualización teniendo en cuenta:
  a. Condiciones de fabricante en cuanto a coste y soporte.
  b. La clasificación de criticidad para el negocio de cada sistema.
  c. Los riesgos de actualizar el software.
  d. Plan de Rollback.
- Para aquellos equipos cuya actualización aún no es posible, analizar la implementación de medidas compensatorias que permitan mitigar su exposición.
- Establecer un periodo de verificación y seguimiento del comportamiento después de realizar los cambios.

La recomendación más importante en un entorno crítico, como es un proceso productivo, pasa por garantizar mediante SLAs o requisitos contractuales, que el fabricante de software evolucionará su producto incorporando aquellas funcionalidades que permitan garantizar la confidencialidad, integridad y disponibilidad requeridas.

Seguridad en el ciclo de vida del desarrollo de software industrial

El ciclo de vida del software es el proceso que se sigue para construir, entregar y hacer evolucionar el software desde la concepción de una idea hasta la entrega y retirada del sistema, y que podemos dividir en siete fases, que recordamos a continuación:

- **Análisis:** Definir una necesidad que se quiere cubrir, definiendo claramente la necesidad creada y el objetivo que cubre esta necesidad.
- **Diseño:** Es el proceso de utilizar la información recolectada en la etapa de análisis, para desarrollar las especificaciones que el software debe cumplir durante el desarrollo
- **Codificación:** Crear los componentes software que cumplan los objetivos definidos en la fase de diseño y creación de especificaciones
- **Pruebas:** Asegurar el correcto funcionamiento de los componentes software creados en la etapa de desarrollo.
- **Validación/paso a producción:** Consiste en poner el software desarrollado a disposición del cliente para cubrir la necesidad identificada durante la etapa de análisis y diseño.
- **Mantenimiento y evolución:** Consiste en corregir problemas del software desarrollado que no fueron descubiertos en las fases de desarrollo y pruebas, implementar mejoras y cambios para que responda a los nuevos requisitos, distribuyendo la nueva revisión.

Pueden clasificarse en acciones correctivas, adaptativas y preventivas.

- Fin del ciclo: Realizar todas las tareas necesarias para asegurar que los clientes del producto puedan adaptarse a otro nuevo software, ya que el desarrollo del actual no será soportado y entra en el estado de obsolescencia.

Es primordial contemplar la seguridad lo antes posible, y en todas y cada una de estas fases. Comenzando con una caracterización de las amenazas. Existen diversas metodologías para realizar formalmente la caracterización de amenazas, pero a alto nivel todas comparten (en mayor o menor medida) los siguientes pasos:

- Identificación de activos
- Definición de superficie de ataque
- Descomposición del ecosistema
- Identificar vectores de ataque
- Listar actores de amenaza

El resultado del modelo deberá alimentar el proyecto y garantizar que los controles resultantes (contramedidas) son adecuados y suficientes para satisfacer la seguridad de la automatización.

No existe un único resultado de modelado de amenazas. Cada proyecto de automatización es diferente y deberá ser tratado de forma única. Por este motivo, integrar la actividad de modelado de amenazas en una fase temprana del diseño, permitirá anticipar debilidades criticas de seguridad, y adoptar una actitud preventiva ante las amenazas ya comentadas, puesto que el coste será mucho menor cuanto antes se incluyan.

Cada organización, típicamente, cuenta con unas actividades de ingeniería de software establecidas que marcan las directrices a seguir en esta materia. Estas actividades planifican y controlan el proceso de desarrollo de aplicaciones conformando un "framework" que permite homogeneizar los desarrollos de software. Independientemente del tipo de metodología de desarrollo de software elegida, ésta debe introducir la seguridad en cada una de sus fases de forma que se garanticen los pilares básicos que deben contemplar todos los desarrollos.

Esta incorporación de la seguridad puede verse en forma de actividades, y siempre deberá complementarse sin pretender sustituir los procesos de la metodología software usados.

Medidas recomendadas

- Identificar las aplicaciones que se están ejecutando en los sistemas, así como los proveedores del software, su instalación y mantenimiento.
- Contactar con cada uno de los proveedores para conocer su estrategia de actualización y herramientas recomendables para facilitar la preparación y actualización.
- Realizar un análisis de riesgos de las distintas alternativas con la información recopilada.
- Concienciación y formación de los equipos de desarrollo.
- Realizar pruebas de seguridad y análisis de código fuente de software.

› Establecer un plan de actualización en aquellos sistemas en los que sea posible llevar a cabo la operación de actualización teniendo en cuenta:
  - a. Condiciones de fabricante en cuanto a coste y soporte.
  - b. La clasificación de criticidad para el negocio de cada sistema.
  - c. Los riesgos de actualizar el software.
  - d. Plan de Rollback.
› Para aquellos sistemas cuya actualización aún no es posible, analizar la implementación de medidas compensatorias que permitan mitigar su exposición.
› Establecer un periodo de verificación y seguimiento del comportamiento después de realizar los cambios.

La recomendación más importante en un entorno crítico, como es un proceso productivo, pasa por garantizar mediante SLAs o requisitos contractuales, que el fabricante de software evolucionará su producto incorporando aquellas funcionalidades que permitan garantizar la confidencialidad, integridad y disponibilidad requeridas.

Seguridad en la integración con aplicaciones corporativas

Las plantas industriales son cada vez más parecidas a una torre de Babel tecnológica: equipos a nivel de campo con distintos protocolos y métodos de comunicación, conectados a estaciones remotas o periferias descentralizadas, comunicadas por Profibus, Modbus o Profinet a PLC´s, que a su vez envían información a PC´s servidores como maestros de una red de clientes de operación accesibles vía web, y que intercambian datos con otras aplicaciones de planta tales como software de gestión (ERP), de fabricación (MES) y bases de datos.

El intercambio de datos de forma fiable entre estos sistemas facilita las tareas de organización y control de plantas industriales.

Las organizaciones están focalizándose en una gestión más integrada en lo que `podemos llamar como “la empresa conectada”, convergiendo las redes IT, correspondientes a la informática de gestión, con las redes OT, correspondientes a las utilizadas en la operación de planta, y adoptando tecnologías de redes estándar, como puede ser Ethernet.

Ello implica que se está utilizando la misma tecnología para objetivos diferentes. Las aplicaciones de IT, están diseñadas para el uso de información por parte de las personas; información de negocio que deberá estar disponible y protegida. Las aplicaciones de OT, están diseñadas para el uso de datos por parte de las máquinas, por lo que cualquier modificación o cambio en señales y variables de proceso, pueden poner en peligro a las personas, la producción, sus instalaciones o el medio ambiente.

Aspectos de seguridad en la integración con aplicaciones corporativas

Algunos aspectos que deben considerarse para proteger la comunicación e integración entre los sistemas del negocio y los sistemas de proceso, de una forma segura, son los siguientes:

› La integración de datos entre las redes industriales y las redes del negocio debe ser realizada con protocolos de comunicación estándar, abiertos; pero a su vez seguros, que protejan la integridad del dato leído.
› La provisión de una arquitectura software modular y escalable que permita adaptarse a las nuevas necesidades que demande la industria.
› La interoperabilidad del software en un entorno multiplataforma.
› La definición de diferentes perfiles de usuarios de acceso a los datos, que identifiquen si son locales o externos con permisos de lectura y escritura de los mismos.
› La autenticación del usuario.
› El cifrado de datos con una configuración adecuada.

Además, de una configuración segura del protocolo, se debe proteger el tráfico entre ambas redes, para lo cual, el seguimiento del estándar IEC 62443, aconseja lo siguiente:

› Un cortafuego "de tres conexiones" evita el tráfico directo entre la red industrial y las redes de negocio. En su lugar, todo el tráfico deberá terminar en la zona industrial desmilitarizada (DMZ), actuando como una obstrucción y permitiendo sólo el acceso autorizado a los datos y sistemas entre las dos zonas.
› Un sistema de prevención de intrusión (IPS) inspecciona el tráfico entre las redes industriales y de negocio, y puede configurarse para bloquear el tráfico

si determina que éste es dañino.

- Redes de área local virtuales (VLANs) ayudan a segmentar el tráfico entre dispositivos y puertos en las redes industriales.
- Los servicios de identidad con listas de control de acceso descargables (dACL) utilizan una lista de declaraciones de 'permiso y denegación' que se aplican a usuarios, direcciones IP y protocolos. Pueden ayudar a impedir que usuarios y tipos de tráfico no autorizados accedan a la red industrial.
- El acceso de los usuarios debe gestionarse adecuadamente. La política de acceso debe definirse por su identidad corporativa. Se deben establecer listas de control estrictas, basadas en servicios de identidad, para un conjunto limitado de usuarios, direcciones IP y puertos a ser utilizados por las aplicaciones.
- Los usuarios que accedan a datos y aplicaciones de la red industrial deberán hacerlo a través de navegadores web compatibles con el protocolo HTTPS. Esta característica de seguridad se utiliza comúnmente en aplicaciones web en Internet, y proporciona cifrado y autenticación adicional.
- Se deben establecer sesiones VPN (SSL) para proporcionar un nivel adicional de protección. Estas sesiones utilizan cifrado para establecer transacciones seguras entre el usuario y el cortafuego de DMZ. El usuario se autentica para verificar qué servicio requiere y el cortafuego confirma que el usuario está autenticado y autorizado para utilizar dicho servicio.

Seguridad en el despliegue de software

Ante una realidad donde las amenazas y vulnerabilidades evolucionan rápidamente, las arquitecturas de despliegue no se encuentran libres de esta problemática. Aún más, los conceptos de integración continua y la inmediatez de los cambios hacen necesario anticiparse a los potenciales atacantes y garantizar la seguridad.

Amenazas como la suplantación de identidad, la divulgación de información o la manipulación pueden aprovechar vulnerabilidades como el almacenamiento o transporte inseguro de credenciales, la existencia de roles insuficientes o el compromiso de los hipervisores o contenedores, entre otras.

Un análisis detallado del modelo de la arquitectura de despliegue y sus particularidades será necesario para mejorar la estabilidad y seguridad. Adicionalmente, será preciso seleccionar las contramedidas adecuadas que permitan reducir el riesgo al máximo aceptado por la compañía.

Aspectos de seguridad en la infraestructura de despliegue

La seguridad en la infraestructura de despliegue debe garantizar que los productos (aplicaciones) finales sean más seguros y para ello es necesario que el área de ciberseguridad participe en todo el ciclo de vida de integración y despliegue continuo, siendo algunas de las medidas recomendables:

- Limitar el acceso a las tecnologías a un rango de redes concreto (ni las herramientas ni los proyectos deben exponerse públicamente).
- Uso de protocolos seguros y de cifrado de las comunicaciones.
- El uso de un segundo factor (2FA) de autenticación (incluyendo accesos remotos de los desarrolladores).
- Monitorización del uso de los accesos remotos y actividad de los usuarios y registro del mismo.
- Gestionar accesos y permisos basándose en el principio de mínimo privilegio.
- La gestión de usuarios de forma descentralizada en varias tecnologías puede ser compleja, por lo que se recomienda valorar el uso de servicios tipo LDAP para realizar la autenticación de usuarios a fin de simplificar el mantenimiento y operación.
- Se recomienda el uso de usuarios no privilegiados, si se necesita utilizar privilegios administrativos, usar “runas” o “sudo”.
- No utilizar usuarios genéricos (los usuarios deben ser individuales).
- Limitar al máximo el uso de cuentas de servicio (y en caso de ser necesarias desactivar la opción de login interactivo).
- Es necesario realizar un adecuado ejercicio de segregación de funciones.
- Utilizar una política de contraseñas robusta (incluyendo claves de cifrado).
- Las herramientas de despliegue deben ser bastionadas adecuadamente previamente a su despliegue en producción.

- Utilizar buenas prácticas de seguridad del mercado (por ejemplo, CIS benchmark) para comprobar el estado de seguridad de las herramientas.
- Cambio de usuarios y contraseñas por defecto.
- Utilizar las capacidades integradas de seguridad de las propias herramientas.
- Actualización periódica de las herramientas de despliegue y aplicación de las últimas actualizaciones de seguridad.
- Validación de la seguridad previa al despliegue de cualquier biblioteca o add-on de terceros.
- No almacenar contraseñas o ficheros sensibles sin cifrado en las diferentes herramientas (cifrado en lado servidor es recomendable).
- Los entornos en desarrollo, preproducción y producción deben encontrarse adecuadamente aislados.
- Mantener una adecuada política de backups.
- Establecer controles suficientes para desplegar el código de forma segura (monitorización de la integridad de los ficheros).
- Establecer registros de auditoria y garantizar la preservación de los mismos.
- Identificar todos los flujos de componentes dentro de la infraestructura y pipeline.
- Establecer un entorno de trabajo fiable para los desarrolladores y un acceso seguro.
- Desarrollar los componentes de forma segura de acuerdo con las mejores prácticas del mercado.

Medida de ciberseguridad en las relaciones con terceros

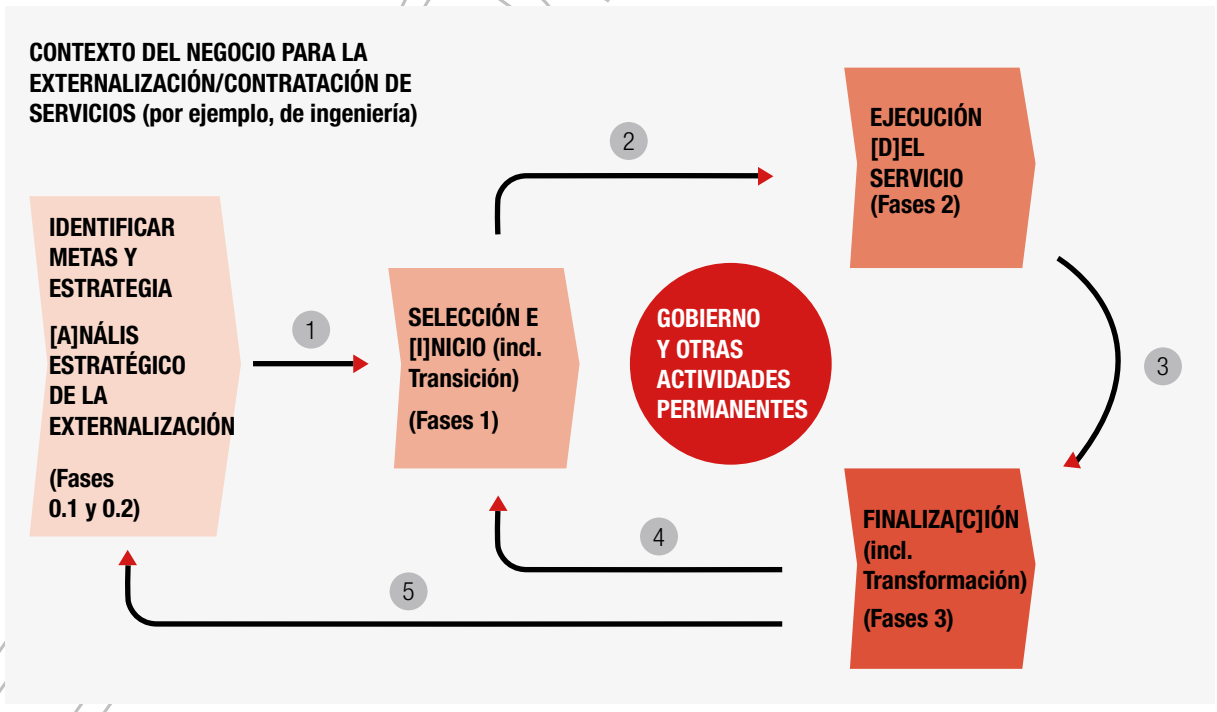
MEDIDA DE CIBERSEGURIDAD EN LAS RELACIONES CON TERCEROS

Los perfiles más relevantes en la relación operador-tercera parte, desde el punto de vista de la puesta en marcha y el mantenimiento de soluciones de automatización industrial, son, hoy en día, los siguientes:

› fabricantes
› integradores

Una medida de ciberseguridad que contemple los posibles problemas (riesgos) derivados de este tipo de relaciones habrá de contemplar la identificación de un conjunto de mínimos, que permita ofrecer una cierta capa normativa orientada a garantizar la ciberseguridad del proceso industrial objeto de implantación o mantenimiento a lo largo de todo el ciclo de vida de la relación cliente-proveedor.

La siguiente figura muestra las principales fases de ese ciclo:



Los números sobre las flechas indican secuencia. las fechas 2, 3 y 4 conforman el verdadero ciclo de la externalización.
Las prácticas Permanentes también podrían desarrollarse durante la Fase 0 (Análisis Estratégico) El contexto del Negocio envuelve por completo al ciclo de vida.

Fuente: iTTi

Figura 20: Ciclo de vida de la externalización de servicios

Como factor crítico de éxito en la salvaguarda de la seguridad (ciberseguridad) de los activos (equipamientos y procesos) de la actividad industrial concreta, ha de tenerse en cuenta que la responsabilidad sobre la rendición de cuentas recaerá, siempre, en el operador industrial y no en sus proveedores.

Sobre estos habrá de recaer la ejecución de las tareas objeto de la externalización; pero, en ningún caso, las labores de toma de decisiones, supervisión y control.

La figura, a continuación, refleja una serie de procesos típicos a ejecutar en el curso de una relación cliente-proveedor. Como puede apreciarse, las acciones de control/supervisión se encuentran asignadas en la vertiente del cliente.

Los nombres de los procesos coloreados a aquellos procesos que aparecen, como espejo, a ambos lados de la relación Cliente-Proveedor.
Fuente: iTTi

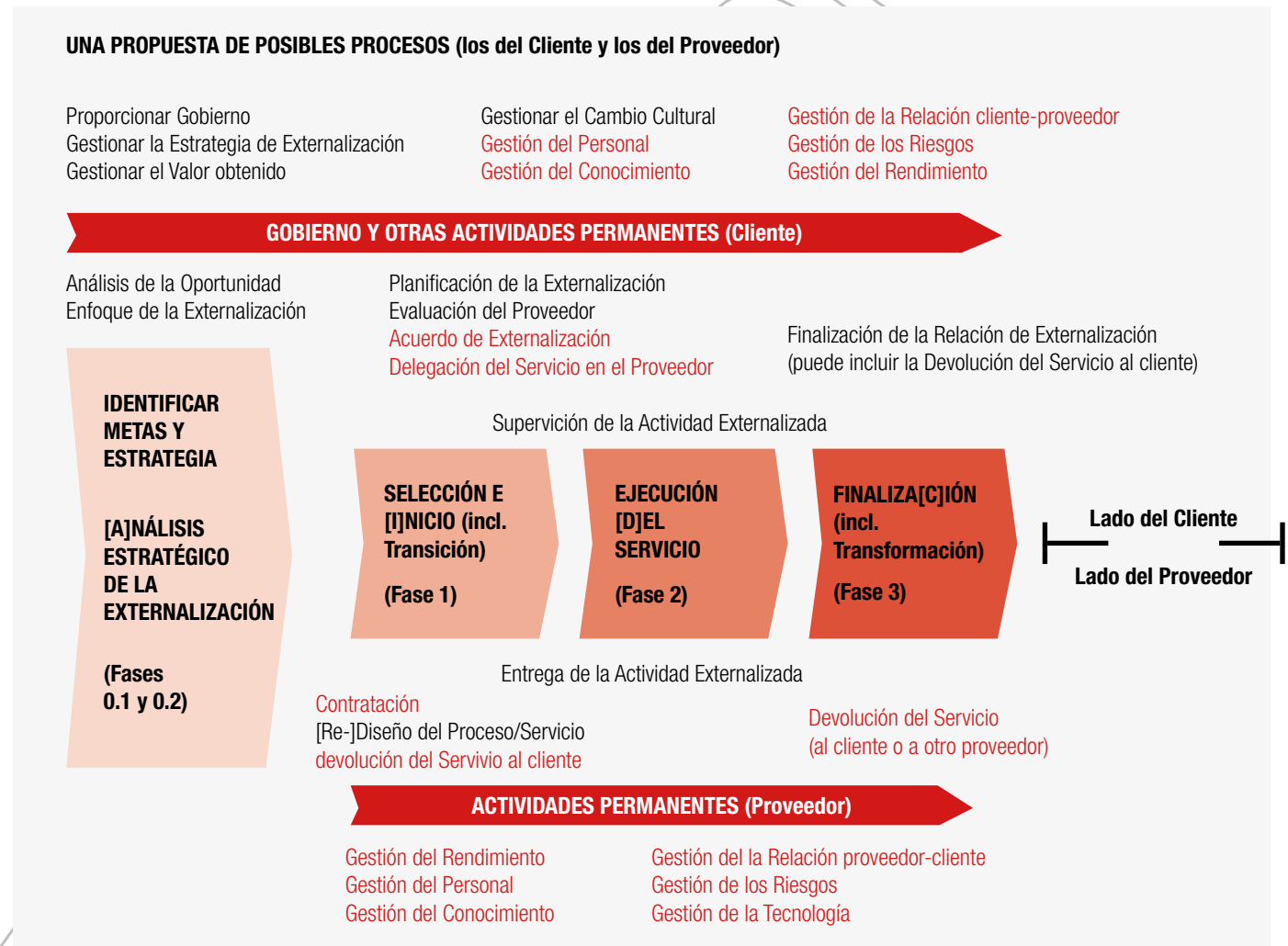


Figura 21: Propuesta de procesos en el ciclo de vida de la externalización de servicios

5

Dominio 5:
Garantía de Resiliencia y Continuidad de los Sistemas de Operación

DOMINIO 5: GARANTÍA DE RESILIENCIA Y CONTINUIDAD DE LOS SISTEMAS DE OPERACIÓN

CONTEXTO

COMPONENTES

ORGANIZACIÓN PARA LA RESILIENCIA Y LA CONTINUIDAD DE LOS SISTEMAS DE OPERACIÓN
ALCANCE Y POLÍTICA
OBJETIVOS Y MÉTRICAS
ESTABLECIMIENTO DE RESPONSABILIDADES
COMITÉ DE EXPERTOS

ANÁLISIS DE IMPACTO EN TECNOLOGÍAS DE OPERACIÓN Y SU EVALUACIÓN
ESTABLECER LOS ESCENARIOS DE RIESGO
ESTRUCTURA DE ESCENARIOS DE RIESGO
ESTRATEGIA DE RESILIENCIA Y CONTINUIDAD: ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)
DEFINIR LA ESTRATEGIA PARA LA RESILIENCIA Y LA CONTINUIDAD

PROCEDIMIENTOS DE RESILIENCIA Y CONTINUIDAD
PROCESO DE RESPUESTA A INCIDENTES
DEFINIR PLAN DE RESPUESTA A INCIDENTES
DEFINIR PLAN DE COMUNICACIÓN
DEFINIR PLAN DE FORMACIÓN Y CONCIENCIACIÓN
DEFINIR PLAN DE RECUPERACIÓN Y CONTINGENCIA
DEFINIR PLAN DE CONTINUIDAD
DEFINIR PLAN DE PRUEBAS

Dominio 5: Garantía de Resiliencia y Continuidad de los Sistemas de Operación

Contexto

CONTEXTO

El presente capítulo de esta guía describe el quinto de los dominios del marco de referencia del SGCI: **Garantía de Resiliencia y Continuidad de los Sistemas de Operación.**

Figura 22: Marco de referencia del SGCI. Dominio 5

Se ofrece aquí una serie de consideraciones generales que deberían contemplarse, como parte de la puesta en marcha de un SGCI, al objeto de garantizar la continuidad y, en última instancia, la resiliencia de las organizaciones industriales, particularmente dado el carácter crecientemente digital de sus sistemas de operación y control (así como de sus sistemas de información).

Se tratará, de ese modo, de establecer una serie de recomendaciones que permitan mejorar la resiliencia y continuidad de tales sistemas y, por extensión, la de la propia instalación u organización, de manera continuada en el tiempo.

Una resiliencia que puede interpretarse como la capacidad de la organización para resistir, dar respuesta y superar, cualquier perturbación sobrevenida de forma imprevista -de manera especial las más graves- que afecte a su actividad productiva normal.

No obstante, ha de advertirse que en el contexto industrial se dan ciertas diferencias significativas respecto a la resiliencia orientada a otros entornos:

- Habitualmente los incidentes en el entorno industrial -particularmente los más graves, que alcanzan la consideración de desastres- tienen, o pueden tener, **un impacto muy elevado** para las personas, el patrimonio y el medioambiente. Piénsese, por ejemplo, en el caso de los escapes de gas, vertidos de fluidos contaminantes, etc.
- Las operaciones y, por tanto, las consecuencias de cualquier perturbación en estos entornos tienen un **gran componente físico**. Los principales escenarios de desastre hacen referencia a amenazas de naturaleza física como incendios, inundaciones, sabotajes o destrucción de equipamiento/instalaciones.
- Los **tradicionales enfoques** para la contención y recuperación, tras una perturbación, propios de otros sectores a menudo **resultan no ser de aplicación** en el ámbito industrial. Por ejemplo, en muchas ocasiones resultará inviable disponer de una localización alternativa donde ubicar el proceso industrial durante el periodo de recuperación, lo cual es una práctica habitual, institucionalizada, en los entornos corporativos.

Dominio 5: Garantía de Resiliencia y Continuidad de los Sistemas de Operación

Componentes

COMPONENTES

Organización para la resiliencia y la continuidad de los sistemas de operación

Alcance y política

El logro de la resiliencia y la continuidad de los sistemas de operación y control de una organización industrial debe pasar por la adopción de una perspectiva amplia, holística, que facilite la puesta en marcha de un conjunto de capacidades para la protección permanente de las operaciones de dicha organización.

Dichas capacidades habrán de tener como foco principal las infraestructuras y el resto de recursos clave que se encuentren al servicio del proceso productivo particular.

Asimismo, cabe recordar que, en determinadas jurisdicciones, la ley define los servicios esenciales que se desarrollan dentro de distintos sectores estratégicos. Las empresas de sectores estratégicos deben disponer de cierta capacidad de ciberresiliencia ante distintos ataques, amenazas o incidentes que puedan sufrir.

Es preciso respaldar la estrategia de resiliencia y continuidad con una política, y sus normas y procedimientos de desarrollo, bien definida. Un conjunto documentado de las mismas es importante para:

- Lograr que las actividades orientadas a garantizar la resiliencia se encuentren alineadas con la misión de la organización;
- establecer expectativas correctas;
- establecer las condiciones necesarias para el ejercicio de la mejora continua;
- proporcionar asesoramiento sobre necesidades operativas; y,
- mantener la consistencia, la fiabilidad y la continuidad de las operaciones de producción.

La falta de una política adecuada obstaculiza las capacidades de la gestión de la resiliencia y la continuidad.

Esta política deberá incluir el propósito, alcance y audiencia objetivo ante incidentes de naturaleza cibernética que afecten los sistemas de operación y control industrial de la organización. La política deberá contener una declaración de responsabilidades y estructura organizativa que garantice la puesta en marcha de las medidas adecuadas para lograr la resiliencia de los procesos industriales de la compañía ante ciberincidentes. Medidas que habrán de ser compatibles con las capacidades de continuidad del negocio y de respuesta a incidentes de la empresa.

En el Anexo XIV se proporciona una plantilla para ayudar a la confección de la política de Resiliencia y Continuidad.

Objetivos y métricas

El objetivo de un enfoque que busque la resiliencia de la empresa consistirá en desarrollar una visión compartida y común de la habilidad de la organización para hacer frente a los riesgos que puedan afectar a la operativa normal de sus servicios críticos, deteriorándolos, hasta llevar a la organización a una situación de crisis.

Uno de los principios fundamentales en la búsqueda de la resiliencia es el hecho de considerar que una organización despliega sus activos (personal, información, tecnología, instalaciones) a fin de hacer posible su misión específica (por ejemplo, ofrecer u operar servicios críticos para la Sociedad). Bajo este principio se entenderán las necesidades de la organización para planificar, definir, desarrollar, gestionar y medir las oportunas prácticas y comportamientos que conduzcan hacia la resiliencia corporativa.

Las métricas, medidas e indicadores de la gestión de incidentes son los criterios que se utilizan para medir la eficacia y la eficiencia de la función de gestión de incidentes. Las métricas basadas en indicadores clave de desempeño (KPI, Key Performance Indicator) y las metas del programa establecidas para la gestión de incidentes deben presentarse a la alta dirección como una base para justificar el soporte y funcionamiento continuos. Permiten a la alta dirección entender la capacidad de la gestión de incidentes de su organización y las áreas de riesgo que es necesario atender.

Las medidas y los informes obtenidos sobre la resiliencia resultan de utilidad a fin de llevar a cabo una autoevaluación y saber lo que se ha hecho satisfactoriamente y las mejoras que es necesario abordar.

Algunos criterios comunes que se utilizan como parte de las métricas de la gestión de incidentes y las de

desastres se mencionan a continuación:

- Número total de incidentes reportados
- Número total de incidentes detectados
- Tiempo promedio para responder a un incidente
- Tiempo promedio para resolver un incidente
- Número total de incidentes resueltos satisfactoriamente
- Medidas proactivas y preventivas tomadas
- Medidas compensatorias
- Número total de empleados que reciben cursos de concienciación sobre seguridad
- Daño total ocasionado por incidentes reportados y detectados
- Ahorros totales de los posibles daños que se hubieran generado por incidentes resueltos oportunamente
- Disponibilidad de planes de contingencia específica
- Número de escenarios contemplados
- Infraesrucuturas críticas de la organización cubiertas en la gestión de la continuidad
- Tiempos de respuesta en la gestión de la contingencia
- Pruebas realizadas
- Éxito o desviaciones en las pruebas
- Actualización de procedimientos de recuperación

Por su parte, las mediciones del desempeño se centrarán en alcanzar los objetivos definidos y en optimizar la eficacia. Las partes interesadas deben definir y acordar los indicadores clave de meta (KGI, Key Goal Indicator) y los KPI de la actividad, los cuales deberán ser ratificados por la alta dirección. El rango típico de los KGI abarca el manejo exitoso de los incidentes, ya sea mediante pruebas en vivo, o en condiciones reales. Las medidas de desempeño clave pueden identificarse mediante el cumplimiento de los tiempos objetivo de recuperación o mediante el manejo exitoso de incidentes que amenacen las operaciones del negocio.

Establecimiento de responsabilidades

La organización de la resiliencia en cualquier entidad requiere disponer de una estructura que asuma desde funciones de dirección y control hasta la realización de tareas de respuesta y seguimiento de incidentes, incluyendo las tareas proactivas de mantenimiento habitual de los sistemas. Esta estructura deberá estar formada por personal interno (responsable del negocio y su operación); pudiendo integrarla, también, personal externo (especialistas que no existan en la organización).

A continuación, presentamos una guía que podría servir para identificar los roles y responsabilidades necesarios en su organización:

Posición	Roles	Responsabilidades
Miembros del Comité de expertos (CRC)	Estructura más alta de las funciones relativas a la reliciencia y continuidad de las operaciones	1. Asume responsabilidad en dirección y control de las actividades de resiliencia y continuidad 2. Organo asesor de la alta dirección 3. Supervisión y gestión de las actividades de resiliencia 4. Responsabilidad corporativa en resiliencia y continuidad"
Gerente de Seguridad de Operación Tecnológica	Lider e interfaz principal del SGCI	1. Desarrolla y mantiene la capacidad de gestión y respuesta a incidentes 2. Gestiona de manera efectiva los riesgos OT e incidentes 3. Adopta medidas proactivas y reactivas para controlar el nivel de riesgo de la operación tecnológica
Gerente de respuesta a incidentes	Lider del equipo de respuesta a incidentes	1. Supervisa las tareas de respuesta a incidentes 2. Coordina los recursos internos y externos para llevar a cabo de manera efectiva la respuesta a incidentes 3. Asume la responsabilidad de la ejecución exitosa del plan de respuesta a incidentes 4. Presenta un informe sobre la respuesta a los incidentes y las lecciones aprendidas a los miembros del CRC
Administrador de incidentes	Miembro del equipo de respuesta a incidentes	1. Realiza las tareas de respuesta a incidentes para contener la exposición derivada de un incidente 2. Documenta los pasos adoptados al ejecutar el plan de respuesta 3. Mantiene la cadena de custodia y observa los procedimientos de gestión de incidentes con fines procesales 4. Redacta un informe sobre los hallazgos de la investigación
Investigador	Miembro del equipo de respuesta a incidentes	1. Realizar las tareas de investigación sobre un incidente específico 2. Determina el origen de la causa de un incidente 3. Redacta un informe sobre los hallazgos de la investigación
Especialista en seguridad IT	Miembro del equipo de respuesta a incidentes experto en materia de seguridad IT	1. Realizar las tareas complejas y exhaustivas relativas a la seguridad IT como parte del plan de respuestas a incidentes 2. Realiza la evaluación/auditoría de seguridad IT como medida proactiva y parte de la gestión de vulnerabilidades
Especialista en seguridad OT	Miembro del equipo de respuesta a incidentes experto en materia de seguridad OT	1. Realizar las tareas complejas y exhaustivas relativas a la seguridad OT como parte del plan de respuestas a incidentes 2. Realiza la evaluación/auditoría de seguridad OT como medida proactiva y parte de la gestión de vulnerabilidades
Gerente de negocio	Propietario de la función del negocio; propietarios de los activos IT/OT	1. Toma decisiones sobre los asuntos relacionados con los activos/sistemas de operación cuando ocurre un incidente, según las recomendaciones del CRC 2. Ofece un entendimiento claro sobre el impacto para el negocio
Especialistas/ representantes IT	Experto en materia de servicios IT	1. Proporcionar apoyo en la resolución de incidentes 2. Mantienen los sistemas de información en buenas condiciones de acuerdo con la política de la compañía y las mejores práctivas
Especialistas/ representantes OT	Experto en materia de automatización industrial	1. Proporcionar apoyo en la resolución de incidentes 2. Mantienen los sistemas de operación en buenas condiciones de acuerdo con la política de la compañía y las mejores práctivas
Representante legal	Experto en materia legal	1. Proporciona asistencia en la gestión/respuesta de incidentes cuado sea necesario debido a una demanda legal
RRHH	Experto en el área de RR.HH	1. Proporciona asistencia en la gestión/respuesta a incidentes cuando sea necesario investigar a un empleado sospechoso de causar un incidente 2. Integrar la política de RR.HH para apoyar la gestión/respuesta de incidentes (sanciones a empleados cuando se determine que se haya violado el uso aceptable de la política o esten involucrados en un incidente
Representante de relaciones públicas	Experto del área de comunicación	1. Ofrece una comunicación controlada a las partes interesadas tanto internas como externas para minimizar el impacto adverso de las actividades de respuesta a incidentes 2. Proporciona asistencia en los asuntos de comunicación
Especialista en gestión de riesgos	Experto en materia de gestión de riesgos corporativos	1. Travaja de forma estrecha con los gerentes del negocio y la gerencia ejecutiva para determinar y manejar el riesgo 2. Proporciona información

Tabla 14: Roles y responsabilidades para la resiliencia y la continuidad

Resultará altamente recomendable que cada perfil disponga de su correspondiente respaldo para el caso en que el individuo asignado no se encuentre disponible (baja, vacaciones, permiso, etc.).

En esta guía se facilita una plantilla para definir una matriz de responsabilidades en materia de resiliencia y continuidad en el Anexo XV.

Comité de expertos

La responsabilidad sobre la protección de la organización y su proceso productivo es, ante todo, una responsabilidad compartida. Por ese motivo la participación "transversal" de los diferentes interesados en la capacidad resiliente de la organización resulta un factor crítico de éxito.

Llevado a la práctica, ello aconseja la conformación de un equipo formado por representantes de las diferentes "partes" de la organización, desde miembros de las áreas estrictamente de negocio, hasta representantes de operaciones, ingeniería, mantenimiento, seguridad, informática, etc. Dichos representantes podrían atender, a su vez, a perfiles relacionados con actividades como:

- producción, esto es, operaciones de negocio (como el Director de Producción o, incluso, el Director de Planta);
- análisis de riesgo corporativo, o de las operaciones (como los analistas de riesgos);
- planificación de la recuperación ante desastres y continuidad de negocio;
- operaciones (como los responsables de turno, del lado de los operadores);
- administracion y mantenimiento de las infraestructuras de TO (como los responsables de ingeniería o los jefes de turno, del lado de mantenimiento);
- elaboración de políticas y procedimientos de TO (respectivamente de TI);
- planificación y gestión de la seguridad de TO (respectivamente, de TI);

entre otros.

En el **Anexo XVII** se proporciona una plantilla para ayudar a la confección del reglamento interno del comité de expertos.

Análisis de impacto en tecnologías de operación y su evaluación

Establecer los escenarios de riesgo

Existe una evolución del enfoque tradicional de **mitigación de los riesgos** a un enfoque de **optimización de los riesgo**s, la principal razón de este cambio se debe a que hoy en día, y cada vez más, el mercado en el que se desenvuelven las organizaciones industriales es más global, competitivo y dinámico, con nuevos actores en la cadena de suministro y una constante redefinición del modelo de negocio. Se tiende por tanto a evitar los controles que alejan a la organización de su **"nivel óptimo de riesgo aceptable"**.

La **optimización de los riesgos** es parte fundamental de cualquier sistema de gobierno y debe contemplar todos los riesgos del negocio en su conjunto, al tiempo que busca la eficiencia en el uso de los recursos.

En seguridad de la información es práctica generalizada llegar a un nivel detallado de análisis de riesgos basado en activos, amenazas y vulnerabilidades. Estos análisis emplean un lenguaje demasiado técnico que, en ocasiones, no conecta con otras áreas de la empresa y provoca una definición de umbrales de tratamiento del riesgo compleja, mal comprendida y con consecuencias que no responden a la realidad del problema que se pretende atajar. Es necesario, por tanto, un análisis de riesgos basado en escenarios que permitan una comprensión de alto nivel para que desde la dirección de la compañía sean capaces de proporcionar el apoyo necesario para su gestión y su alineación con los objetivos corporativos. Para ello se establecerán criterios usables, homogéneos y rigurosos de estimación del riesgo en el marco de toda la organización.

El riesgo tecnológico de operación -se adopta aquí una interpretación clásica del riesgo, entendido como incertidumbre de consecuencias negativas- podría definirse como la probabilidad de pérdidas derivadas de un suceso relacionado con el acceso o uso de la tecnología, que afecta al desarrollo de los procesos del negocio y la gestión de riesgos de la organización, al comprometer o degradar las dimensiones críticas de disponibilidad, integridad y confidencialidad.

Además, en el caso particular de aquellos servicios considerados por ley como esenciales, que comprenderían instalaciones, redes, servicios, equipos

físicos o tecnología de la información, una gestión de riesgos de TO incorrecta, no solo tiene un impacto económico, sino que puede tener un grave impacto en la salud, la seguridad o el bienestar social o económico de los ciudadanos, o en el eficaz funcionamiento de las instituciones y los servicios públicos o privados.

Una gestión de los riesgos TO incorrecta, puede reducir el valor del negocio creando pérdidas económicas, afectando a la calidad del producto o servicio, afectando al medio ambiente o la salud de las personas, desperdiciando nuevas oportunidades y por lo tanto, dañando la reputación corporativa.

Un **escenario de riesgo**, es una descripción de un posible suceso, que cuando se produce tiene un impacto potencial sobre el logro de los objetivos de la organización. Un solo suceso puede tener una o varias consecuencias, positivas o negativas, sobre los objetivos.

Para poder **establecer los escenarios de riesg**o, es fundamental identificar primero las unidades de negocio de alto riesgo y sus procesos y/o servicios críticos que dan soporte a los objetivos del negocio, para los cuales se deben definir aquellos sucesos que pueden afectar a la disponibilidad e integridad de dichos procesos, e incluso a la confidencialidad de la información que gestionan. Para ello se tendrán en cuenta los activos y los actores que intervienen en el proceso, así como el conjunto de las amenazas a las que se exponen. Esta sería la forma de establecer los escenarios de riesgo de arriba a abajo, desde los objetivos a los escenarios.

Una segunda forma de establecer escenarios es de abajo a arriba, es decir, partiendo de escenarios genéricos o escenarios de ocurrencia común en su sector o área de producto, también podrían considerarse escenarios que representan cumplimiento de requisitos de cliente o regulatorios. En esta segunda forma de establecer los escenarios debería llevarse a cabo una validación contra los objetivos del negocio.

Ambas formas de establecer escenarios son complementarias y deberían emplearse simultáneamente para limitar la incertidumbre.

Existen aspectos fundamentales que deben tenerse en cuenta a la hora de establecer los escenarios de riesgo:

- El número de escenarios de riesgo deberían reflejar la realidad y complejidad de la organización.
- Una vez identificados el conjunto de escenarios de ocurrencia, deberían reducirse estos a un número manejable en línea con la criticidad para cada una de las unidades de negocio.
- Cada escenario debe ser realista y adecuado para permitir tomar decisiones.
- La revisión periódica de los escenarios de riesgo para contemplar y reflejar los cambios que se puedan haber producido.

Estructura de escenarios de riesgo

La estructura de cada escenario de riesgo deberá contener al menos los siguientes elementos:

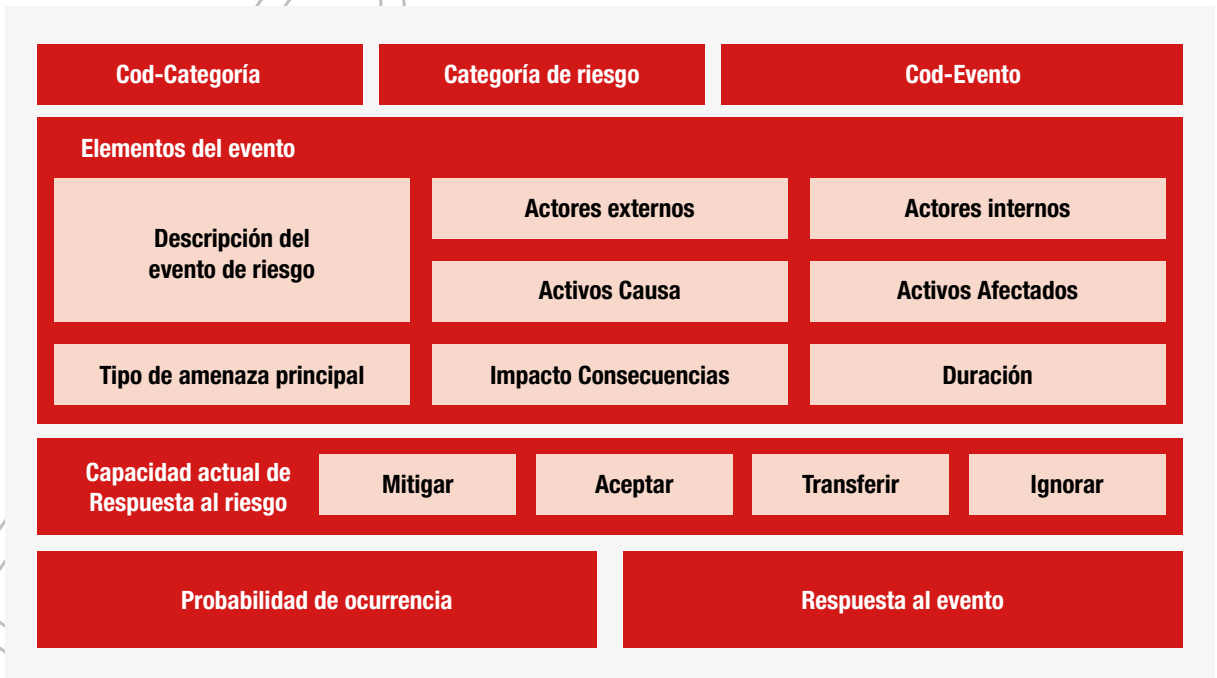


Figura 23: Atributos para la caracterización de un escenario de riesgo

Cod-Categoría: Identificador único de la categoría del riesgo.

Categoría del riesgo: Es la clasificación de los escenarios de riesgo en función del área donde podría materializarse el incidente que desencadena el evento. Se han identificado 9 categorías que son:

› Diseño y Arquitectura
› Infraestructura (Software y hardware)
› Operación del Personal TI y TO
› Dirección de la organización
› Cadena de suministro
› Cumplimiento normativo
› Medioambiente y Seguridad Industrial
› Ciberataques y Malware
› Geopolítico

Descripción del evento: Describe la situación del evento del escenario de riesgo.

Tipo de amenaza: Identifica el tipo de amenaza que podría dañar los activos afectados por el evento. Algunos ejemplos de tipos de amenazas posibles son:

› Acciones no autorizadas
› Compromiso de funciones
› Daño físico
› Fallo de servicio de soporte
› Fallo técnico
› Información

Activos causa: Son los activos susceptibles de causar el evento al ser explotadas sus debilidades.

Activos afectados: Son los activos que sufrirían los daños del evento y que dependerá de cada tipo de sistema/aplicación afectado por el evento.

Actores internos: Identifica los actores internos de cuya dependencia se pueden aprovechar las debilidades que podrían llegar a desencadenar el evento. Algunos ejemplos de actores internos que pueden encontrarse:

› Auditores internos
› Gerente de seguridad industrial
› Responsable de sistemas de información
› Responsable de seguridad de la información
› Responsables de proyectos
› Responsable de comunicación
› Comité de gobierno
› Operador TI
› Operador TO
› Compras (tecnología)
› Recursos Humanos
› Propietario del servicio
› Usuario del servicio
› Comercial y marketing

Actores externos o terceras partes: Identifica a los actores externos o terceras partes cuyas debilidades podrían ser aprovechadas para desencadenar el evento. Entre los que pueden encontrarse:

› Reguladores
› Auditores externos
› Proveedores de tecnología
› Consultores
› Integradores

Impacto/Consecuencias: Corresponde al grado de impacto que tendrían los activos afectados si se materializara el evento del escenario de riesgo. Este impacto corresponde al valor de las dimensiones afectadas (Disponibilidad, Integridad y/o Confidencialidad) de la seguridad que se obtiene de la valoración CID de los aspectos de protección.

Duración: Identifica la posible duración del incidente basado en las consecuencias y las capacidades de resistencia y recuperación actuales.

Capacidad: Es la capacidad actual de resistir y recuperarse frente al evento, es decir, las medidas que se han adoptado actualmente para proteger los activos.

Respuesta al evento: Es el grado de capacidad para resistir y recuperarse del evento que afectará a los activos que soportan el servicio.

Probabilidad de ocurrencia: Es el valor porcentual de la posibilidad de que un evento suceda, en función de sus antecedentes, la duración de dichas situaciones anteriores y la capacidad de respuesta actual del operador ante dicho evento.

Es importante tener en cuenta la naturaleza imprevisible y poco estática de los riesgos en este entorno. En general los riesgos industriales clásicos tienden a tener un valor estable en el tiempo, de forma que la probabilidad de ocurrencia en 5 años puede

extrapolarse fácilmente si se conoce la probabilidad en un año. En el caso de la ciberseguridad, la agresividad, complejidad y sofisticación de las amenazas crecen de manera exponencial con el tiempo de exposición y por ello es importante hacer una evaluación de posibles pérdidas a cinco años. Un método puede ser considerar varios casos dentro de cada escenario de diferentes probabilidad e impacto (al menos 4), asignarles una probabilidad de ocurrencia a cinco años con un SGCI estático (el actual) y calcular la envolvente de la curva con métodos de estadística clásica de riesgos. De esta forma se puede mostrar a la Dirección qué podría ocurrir si no existiera una actualización y adaptación permanente del sistema SGCI y de sus recursos asignados a la agresividad creciente de estas amenazas.

Grado del Riesgo: Es un valor que se calculará automáticamente y que corresponde al producto del valor de impacto por el valor de probabilidad de ocurrencia del evento del escenario.

En el **Anexo XVIII** se proporciona una plantilla para ayudar a la confección escenarios de alto riesgo, incluye tres ejemplos de escenarios.

Estrategia de Resiliencia y Continuidad: análisis de impacto en el negocio (BIA)

Un análisis de impacto en el negocio (BIA, Business Impact Analysis) debe permitir a una organización establecer una estrategia de continuidad y resiliencia del negocio eficiente, y tiene como objetivo principal identificar las necesidades del negocio en términos de resistencia y recuperación.

Cuando, según la jurisdicción, se trate de servicios legalmente considerados esenciales, se deberán analizar las consecuencias que supondría una interrupción del mismo, con el fin de identificar cuáles son las áreas de impacto, y asegurar que los riesgos se priorizan de acuerdo con la importancia para la organización, y se mitigan en consecuencia.

El propósito de un BIA es identificar primero qué unidades de negocio, departamentos y procesos o actividades son críticas para la supervivencia del negocio; para, después, estimar los impactos operativos y financieros de cada unidad de negocio, asumiendo siempre el peor de los casos; y para identificar, finalmente, el tiempo asumible de recuperación si se interrumpiesen los procesos críticos para cada unidad de negocio después de haberse producido un desastre, así como los recursos necesarios para reanudar las operaciones en el tiempo establecido.

Para la elaboración de un BIA es fundamental identificar una serie de parámetros temporales. En concreto, es necesario identificar los siguientes:

- **RTO (Recovery Time Objective):** Tiempo de recuperación de las actividades que hemos identificado bajo unas condiciones mínimas aceptables. Por ejemplo, supongamos que el Responsable de operaciones nos indica que, en caso de que fallara la plataforma que soporta las aplicaciones para la generación de energía, se deberían recuperar el proceso en un plazo máximo de 2h. En este caso, estableceríamos que el RTO asociado a dicho proceso es de 2h.
- **MTD (Maximum Tolerable Downtime):** Tiempo máximo tolerable de caída, el cual nos determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio. Volviendo al caso anterior, supongamos que el proceso de monitorización en tiempo real de un proceso crítico no debe estar interrumpido por un periodo superior a 6h. En este caso, estableceríamos que el MTD asociado a dicho proceso es de 6h.
- **RPO (Recovery Point Objective):** Es el periodo máximo del que se pueden perder los datos a consecuencia de un incidente antes de tener consecuencias inaceptables, formando parte de las políticas de respaldo definidas por la organización. En este sentido, imaginemos que el Responsable del centro de control nos indica que podrían tolerar una pérdida de datos siempre y cuando no se perdieran los datos generados en más de un día completo. Por lo tanto, estableceríamos que el RPO es de 24h.
- **CTO (Containment Time Objetive):** Tiempo máximo tolerable para la contención de un fallo, o ataque, que podría provocar la pérdida de un servicio crítico para el negocio.

La ejecución del BIA comenzará con una serie de reuniones con las unidades de negocio dentro del alcance del análisis, a fin de recabar la información necesaria. El personal entrevistado (responsables de área, coordinadores, personal técnico, etc.) nos facilitará la información de los procesos, y requisitos de contención y recuperación, así como las posibles

dependencias con los proveedores, clientes, etc. Deberemos intentar contemplar todas estas cuestiones y dejar constancia de ello en el BIA.

Como resultado de los trabajos de análisis se dispondrá de un conjunto de procesos o actividades para los cuales se habrán definido el RTO, MTD, RPO y CTO. Con esta información podrá crearse la lista ordenada por prioridad y obtener las actividades críticas y si profundizamos en el análisis podemos deducir cuales son los activos críticos de TI y TO.

La elaboración y puesta en marcha de un análisis de impacto o BIA para el negocio consiste en conocer las necesidades de negocio expresándolas en términos de contención y recuperación, atendiendo a los resultados del análisis, e implantando los planes de contención y recuperación que permitan restablecer los servicios o infraestructuras, entre otros, cubriendo las necesidades y el cumplimiento de los objetivos de negocio marcados por la compañía.

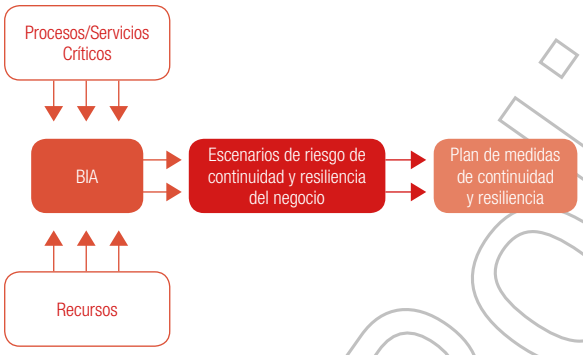


Figura 24: Análisis de impacto en el negocio en el marco de la garantía de la resiliencia y la continuidad

Proteger sistemas de control industrial requiere crear una cultura de seguridad continua en el tiempo. Se trata de un proceso que requiere constante actualización, no de una acción puntual; máxime, dado que los vectores de ataque cambian constantemente, en la medida que son descubiertas nuevas vulnerabilidades de forma permanente.

Definir la estrategia para la resiliencia y la continuidad

La resiliencia del negocio constituye una de las más notables prioridades en las que debería reparar el consejo de administración. El mercado está cada vez más interconectado y provoca que cualquier organización, en algún momento, sea vulnerable a determinados riesgos que están fuera de su control.

Algunos de estos factores de riesgo, en cualquiera de los niveles de la cadena de suministro podría llegar a afectar a la organización y a su reputación, ahora más global y con “visibilidad instantánea” en las redes sociales.

Para dar respuesta al nuevo entorno empresarial es vital para el negocio que la infraestructura, los datos y las personas que componen la empresa sean fiables, rápidos, seguros y resilientes.

Debido al aumento constante del número y tipo de riesgos, es fundamental una estrategia de resiliencia de negocio robusta que pueda garantizar el éxito futuro de la organización, de forma que sea capaz de recuperarse de forma eficaz de un amplio conjunto de riesgos multidimensionales.

A la hora de establecer la estrategia de resiliencia se deberá considerar que la resiliencia es una cualidad inherente a una organización para enfrentarse a una crisis sin que se vea afectada su actividad, por ello será necesario realizar modificaciones en la misma naturaleza de la organización, y diseñar una infraestructura tecnológica segura. Se puede conseguir un determinado nivel de seguridad con políticas a corto plazo, pero para alcanzar una autentica resiliencia es necesario aplicar medidas estructurales a largo plazo.

El origen de una crisis grave que afecte a una organización industrial puede ser de origen interno. Centrar la estrategia en resistir ataques externos, subrayando la palabra ataques, es enfocar el problema de forma errónea. Una crisis interna puede generarse por la influencia de agentes externos o tener carácter mixto. Puede ser el caso de la crisis que se genera debido a una prolongada situación de estrés, condicionada por factores ambientales, que desgasta los recursos propios. En ese caso, los recursos más críticos son fundamentalmente humanos, sensibles a los fenómenos sociales.

Para cada dependencia externa, la organización debería haber establecido y documentado un conjunto detallado de las especificaciones que la entidad externa debe cumplir con el fin de apoyar y ampliar la capacidad de recuperación de las operaciones de la organización, incluyendo estos requisitos de ciberresiliencia en las especificaciones de los acuerdos con dichas entidades. El cumplimiento de estos acuerdos debe ser monitorizado regularmente, comprobando que se solucionan los problemas de operación encontrados. Asimismo, se deberían

identificar las dependencias externas respecto de los servicios públicos que pueden ser vitales para el funcionamiento continuo del servicio durante una interrupción (servicios de respuesta a incendios y salvamento, fuerzas y cuerpos de seguridad, servicios de gestión de emergencias, etc.).

En el **Anexo XX** se proporciona una plantilla para ayudar a la definición de un acuerdo de nivel de servicio.

El primer paso antes de definir la estrategia de resiliencia es alcanzar un conocimiento real y profundo de la organización y su entorno. La documentación interna de operación de una organización ofrece una visión idealizada de su funcionamiento, y posiblemente alejada del modo real de trabajo, no reflejando relaciones y canales que constituyen las operaciones del día a día. Para conseguir una visión crítica de la organización no solo es necesario obtener la visión desde dentro, sino que es fundamental obtener información de cómo es vista la misma desde el exterior. Esa visión la proporcionan aquellos que tienen que interaccionar con ella, ya sean clientes de sus servicios, proveedores o competidores.

Procedimientos de resiliencia y continuidad

Abordar la resiliencia y continuidad de los sistemas de operación requiere de una amplia gama de actividades destinadas a mantener y recuperar los servicios críticos del sistema después de un evento. Además, planificar las contingencias de los sistemas de operación deber formar parte de un esfuerzo de la seguridad y la gestión de incidentes mucho más amplio que incluye la continuidad del proceso organizativo y de negocio, la planificación de recuperación de desastres y la gestión de incidencias.

En última instancia, una organización podría utilizar un conjunto de planes para preparar adecuadamente la respuesta, recuperación y continuidad de las actividades de las perturbaciones que afectan a los sistemas de operación de la organización, procesos de negocio, de personal y las instalaciones. Debido a que existe una relación inherente entre un sistema de operación y los procesos de negocio al que dan soporte, debe existir coordinación entre cada plan durante su desarrollo y cambios para asegurar que las estrategias de recuperación están alineadas y no se duplicarán esfuerzos.

La continuidad y la planificación de contingencias son componentes críticos de la gestión de emergencias y la resiliencia organizacional, pero a menudo se confunden en su uso. Planificación de la continuidad se aplica normalmente al negocio en sí mismo; se refiere a la capacidad para continuar las funciones y los procesos críticos durante y después de un evento. Los planes de contingencia normalmente se aplican a los sistemas de operación o a los sistemas de información, y proporcionan los pasos necesarios para recuperar -de forma manual o automatizada- el funcionamiento de la totalidad, o de parte, de los sistemas de operación o información de una determinada ubicación. La planificación de respuesta a incidentes es un tipo de plan que normalmente se centra en la detección, respuesta y recuperación ante un incidente o evento de seguridad tecnológica.

Proceso de respuesta a incidentes

El proceso de respuesta a incidentes tiene cuatro fases.

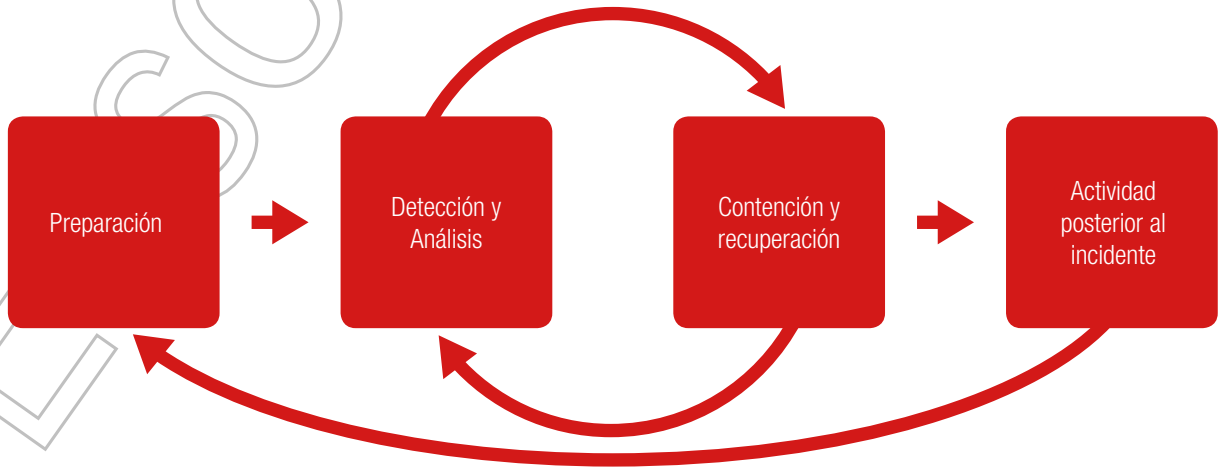


Figura 25: Fases de la respuesta ante incidentes

(por ejemplo, apagar un sistema, desconectarlo de la red, desactivar ciertas funciones). Estas decisiones son mucho más fáciles de adoptar si hay estrategias y procedimientos predeterminados para contener el incidente.

Las estrategias de contención (y, respectivamente, de contingencia) varían en función del tipo de incidente. Por ejemplo, la estrategia para contener una infección de malware es bastante diferente de la de un ataque DDoS en la red o un desastre natural. La organización debe crear estrategias de contingencia (y, respectivamente, de contingencia) para cada tipo principal de incidente, con criterios claramente documentados para facilitar la toma de decisiones. Como parte de esos criterios para determinar la estrategia apropiada cabría citar:

- Posibles daños de los recursos
- Necesidad de preservar pruebas
- Disponibilidad del servicio (por ejemplo, la conectividad de red, servicios prestados a las partes externas)
- Tiempo y recursos necesarios para aplicar la estrategia
- Eficacia de la estrategia (por ejemplo, la contención parcial, contención completa)
- Duración de la solución (por ejemplo, solución de emergencia de cuatro horas, solución temporal de dos semanas, solución permanente).

Como cuarta fase de gestión del incidente, se deberá elaborar un informe detallando la causa y el coste del incidente, así como las medidas que la organización debe adoptar para prevenir futuros incidentes.

Adicionalmente, habrá que analizar las lecciones aprendidas y modificar los procedimientos, de acuerdo a aquellas.

Definir plan de respuesta a incidentes

La organización deberá disponer de un enfoque formal, bien definido y coordinado para responder a los incidentes, incluyendo una hoja de ruta de capacidades de respuesta a incidentes. Cada organización necesita un plan que satisfaga sus necesidades específicas, que se contemple la misión, el tamaño, la estructura y funciones de la organización. El plan debe establecer los recursos necesarios para su gestión. El plan de respuesta a incidentes debe incluir los siguientes elementos:

- Misión
- Estrategias y objetivos
- Aprobación de la dirección
- Estructura organizacional de respuesta a incidentes
- Comunicación con el resto de la organización y con otras organizaciones
- Métricas para medir la capacidad de respuesta a incidentes y su eficacia
- Mapa de ruta con la madurez en las capacidades de respuesta a incidentes
- Programa general para su adopción por la organización

Los procedimientos operativos a desarrollar deberán estar basados en las directrices de la política y el plan de respuesta a incidentes. Estos procedimientos deberán ser razonablemente extensos y detallados para asegurar que las prioridades de la organización se reflejan en las operaciones de respuesta. Además, a raíz de las respuestas estandarizadas debe minimizar los errores, en particular aquellos que puedan ser causados por situaciones de manejo de incidentes complejos. Todos los procedimientos operativos deberán ser probados por el Comité de Expertos para validar su exactitud y utilidad, y posterior distribución a todos los miembros del equipo. Se deberá capacitar a los usuarios de los procedimientos; utilizando los documentos de procedimientos como una herramienta de instrucción.

En el **Anexo XIX** se proporciona una plantilla para ayudar a la gestión de incidentes.

La resiliencia y continuidad de una organización se fundamentará en la madurez de las capacidades de preparación de respuesta a incidentes, dichas capacidades de preparación serían:

Detección de Intrusiones

Primer nivel de un equipo de respuesta a incidentes que permitirá estar preparado para analizar los incidentes de forma más rápida y precisa, basándose en el conocimiento que se obtiene de las tecnologías de detección de intrusos.

Gestión de Notificación de Vulnerabilidades

La gestión de notificaciones o comunicaciones, dentro de la organización, con respecto a las nuevas vulnerabilidades y amenazas (por ejemplo, la aparición

de nuevas tácticas o casos de ingeniería social, en el sector o en el mercado, en general). Utilizando métodos automatizados siempre que sea posible y pertinente. Es recomendable la existencia de una gestión unificada de notificaciones dentro de la organización para evitar la duplicación de esfuerzos y la información contradictoria.

Educación y Concienciación

La educación y la concienciación son cruciales, y deberá formar parte de las actividades de gestión de incidentes la elaboración de comunicados a través de múltiples medios: talleres, intranet, boletines y carteles entre otros.

Es deseable disponer de un plan de formación para promover el conocimiento y el desarrollo de habilidades y conocimientos, tanto de los usuarios técnicos como del resto de personal, en apoyo de sus funciones para la consecución y el mantenimiento de la resiliencia. El plan de formación, por tanto, comprenderá cualquier iniciativa de formación en ciberseguridad, incluyendo la participación en ciberejercicios.

Intercambio de Información

Se deberá definir el intercambio de información con organismos públicos y privados, como los CERT. La respuesta ante incidentes, a menudo, es un esfuerzo compartido, en el que el equipo de respuesta a incidentes de la organización agrega información relacionada con, o derivada de, otros incidentes; y, al mismo tiempo, la comparte de forma eficaz con otras organizaciones.

Definir plan de comunicación

La organización debe documentar los procedimientos estándar para las comunicaciones internas y externas en el caso de una interrupción mediante un plan de comunicación de crisis. Un plan de comunicación de crisis deberá ser desarrollado por la organización responsable de la difusión pública. El plan deberá ofrecer varios formatos para cada uno de los canales de comunicación adecuados. El plan de comunicación de crisis normalmente deberá designar a individuos específicos que tendrán la autoridad para responder a las preguntas o proporcionar información al público con respecto a la respuesta de emergencia. También deberá incluir procedimientos para la difusión de informes al personal sobre el estado del incidente y las plantillas para comunicados de prensa públicas.

Los procedimientos de comunicación de crisis del plan deben ser comunicados a los responsables del plan de continuidad y de recuperación de la organización para asegurar que los planes incluyen una dirección clara.

Una comunicación eficaz es un componente crucial para garantizar que se obtendrá y proporcionará la información que se precise en cada momento; y para que puedan ponerse a disposición detalles sobre el incidente que se esté atajando.

Asimismo, será básico mantener el control de estas comunicaciones para determinar de la manera más eficaz lo que está sucediendo, los hechos que son importantes y la asistencia que se necesita.

Puede ser preciso establecer comunicación con los siguientes grupos de interés:

- Miembros internos del equipo
- Personal de TO (respectivamente, de TI)
- Dueños de los sistemas de operación y control
- Operadores de dichos sistemas
- Expertos técnicos, como el personal de ingeniería y mantenimiento
- Personal de Dirección u otro personal administrativo como, por ejemplo, RRHH, Prevención de Riesgos Laborales, Asesoría Jurídica, etc.
- Personal de medios de comunicación/relaciones publicas
- Proveedores

Es fundamental establecer de forma adecuada la comunicación con terceras partes en relación con un incidente, comunicaciones tales como ponerse en contacto con la policía, medios de comunicación, o expertos externos. También la comunicación con los proveedores de servicios de Internet (ISP), el proveedor de software vulnerable, u otros equipos de respuesta a incidentes. Incluso la comunicación con otras áreas de la organización con las cuales puede ser necesario informar de manera proactiva de un incidente relevante con el objetivo de mejorar la detección y análisis de incidentes.

El equipo de respuesta a incidentes deberá establecer de forma conjunta con los departamentos legal y de comunicación antes de que ocurra un incidente para definir políticas y procedimientos relacionados con el intercambio de información. De lo contrario, la información confidencial relativa a los incidentes puede ser proporcionada a terceros no autorizados,

lo cual puede conducir a una pérdida de imagen y financiera. El equipo debe documentar todos los contactos y comunicaciones con terceros con fines probatorios de responsabilidad.

En el **Anexo XVI** se define una plantilla de contactos clave.

La comunicación puede adoptar muchas formas, entre otras:

- Respuestas por correo electrónico relativas a incidentes
- Documentación de informes de eventos o incidentes, vulnerabilidades y otra información técnica
- Notificaciones y/o directrices que se proporcionan a la comunidad de usuarios
- Políticas y procedimientos de desarrollo interno
- Otros comunicados externos al personal, la gerencia u otras partes interesadas

Definir plan de formación y concienciación

En el supuesto de que una organización no pueda encontrar expertos internos, ni contratar/capacitar al personal para proporcionar las habilidades especializadas que se requieren, podría desarrollar relaciones con expertos en este campo para aportar las habilidades necesarias. Cuando surgen situaciones en las cuales el conocimiento interno no es suficiente, se puede recurrir a especialistas técnicos para cubrir esos vacíos de conocimientos especializados.

Cuando se reportan incidentes más complejos, la organización puede necesitar complementar o ampliar las habilidades básicas del personal para incluir un conocimiento más profundo, de tal forma que el personal pueda entender, analizar e identificar respuestas eficaces a los incidentes reportados.

Las organizaciones requieren de personas que cuenten con unas determinadas habilidades y conocimientos técnicos especializados, con habilidades que les permitan responder a incidentes, llevar a cabo tareas de análisis y comunicarse de forma eficaz con la comunidad de usuarios y otros actores internos y externos.

También deben ser capaces de solucionar problemas de manera competente, adaptarse al cambio rápidamente y ser eficientes en el desempeño de sus actividades diarias.

El conjunto de estas habilidades básicas se puede clasificar en dos grandes grupos:

- Habilidades personales
  - Habilidades de liderazgo
  - Habilidades de presentación
  - Habilidad para alinearse con las políticas y los procedimientos establecidos
  - Habilidades de equipo
  - Integridad
  - Conocimiento de sí mismos
  - Capacidad de superar las tensiones (resiliencia personal)
  - Capacidad para la resolución de problemas
  - Capacidad para una buena gestión del tiempo
  - Capacidades de pensamiento sistémico y complejo
- Habilidades técnicas
  - Habilidades de base técnica, propiamente dichas
  - Habilidades para el tratamiento de la contingencia y la recuperación

Definir plan de recuperación y contingencia

Un plan de contingencia deberá proporcionar procedimientos para la evaluación y la recuperación de un sistema después de su interrupción; o para el establecimiento de medidas alternativas, temporales, que permitan que el proceso de negocio continúe. Este plan proporcionará información clave necesaria para la recuperación del sistema, incluidas las funciones y responsabilidades, información del inventario, procedimientos de evaluación, procedimientos detallados de recuperación, y las pruebas del sistema.

Conviene tener en cuenta que los planes de recuperación en entornos industriales son de muy difícil diseño y peor ensayo, puesto que los dispositivos afectados por el plan no suelen tener alternativa de producción. Por ello es muy importante considerar un plan de continuidad que incluya como alternativa subfases cuyas pruebas sean de tipo virtual o que se hayan realizado en otros momentos (paradas de mantenimiento, rearranques por cambio de producto, etc.).

Un plan de contingencia puede ser activado en la ubicación actual del sistema o en un sitio alternativo. En contraste, un plan de recuperación de desastres

es un plan para un sitio específico que desarrolla procedimientos para trasladar las operaciones de uno o más sistemas de operación, desde una ubicación dañada o inhabitable a una ubicación alternativa temporal. Una vez que el plan de recuperación ha transferido el servicio con éxito a un sitio alternativo, cada sistema afectado entonces utilizará el plan de contingencia para restaurar, recuperar y probar los sistemas, para ponerlos en funcionamiento.

El tiempo y los recursos que deben destinarse a la recuperación de un incidente son proporcionales a la magnitud del mismo. Incluso en algunos casos no será posible recuperarse de un incidente; y en otros, un incidente puede requerir muchos más recursos de los que tiene disponibles una organización. Por todo ello la recuperación frente a un incidente deberá estar basada en una valoración del esfuerzo de su recuperación y los requisitos relacionados con la gestión de incidentes.

Los planes de continuidad deben ser actualizados de forma continua a medida que se encuentran nuevos riesgos o el entorno operacional cambia. Dichos planes deben incluir los tiempos objetivos de recuperación (RTO) para cada servicio esencial de la organización.

La capacidad de recuperación del incidente determina las posibles respuestas que el equipo puede tomar al gestionar el incidente. Un incidente con un alto impacto funcional y con un bajo esfuerzo para su recuperación es un candidato ideal para una acción inmediata. Sin embargo, algunos incidentes de difícil recuperación hacen necesario transferir parte de la responsabilidad en la gestión del incidente, e incluso crear un plan de difusión para alertar a personas u organizaciones. Deberá establecerse prioridad de respuesta a cada incidente basándose en la estimación del impacto en el negocio causado por el incidente y los esfuerzos estimados necesarios para recuperarse del mismo, para lo cual es recomendable establecer calificaciones de incidentes que permitan priorizar los recursos limitados.

El proceso para desarrollar y mantener un plan de contingencia de sistemas de operación requiere de varios pasos:

1. Desarrollar la política de planificación de contingencia;
2. Análisis de impacto en el negocio (**BIA**, Business Impact Analysis);
3. Identificar los controles preventivos;
4. Crear estrategias de contingencia;
5. Desarrollar un plan de contingencia;
6. Desarrollar un plan de pruebas, capacitación y ejercicios;
7. Garantizar el mantenimiento del plan.

Estos siete pasos representan los elementos clave para dotar a la organización de una capacidad completa de contingencia de los sistemas de operación.
El desarrollo de la política de planificación de contingencia y la realización del ejercicio BIA se lleva a cabo siguiendo los principios del Ciclo de Vida de Desarrollo de Sistemas (**SDLC**, Systems Development Life Cycle).

Definir plan de continuidad

El plan de continuidad de negocio (**BCP**, Business Continuity Plan) se centra en el mantenimiento de los procesos de negocio de una organización durante y después de una interrupción. Un ejemplo de un proceso de negocio puede ser el proceso de embotellado. Un BCP puede abarcar los procesos críticos de una sola unidad de negocio o puede abordar procesos de toda la organización. El BCP también puede contemplar solamente las funciones que se consideren prioritarias. Debido a que los procesos de negocio utilizan los sistemas de operación y/o información, el plan de continuidad del negocio debe estar coordinado con los propietarios de los sistemas de operación y de información para asegurarse de que las expectativas y capacidades del BCP coinciden.

Como parte del BCP, cabría, además, contemplar los conceptos de:

- Plan de Continuidad de las Operaciones (**CoOP**, Continuity of Operations Plan). Plan para continuar realizando las operaciones del negocio [en modo degradado] hasta que se recupere la infraestructura tecnológica que las sustenta en condiciones normales.
- Plan de Recuperación ante el Desastre (**DRP**, Disaster Recovery Plan). Plan de recuperación tras un desastre que haya afectado a las TI (respectivamente, a las TO). El plan buscará devolver la insfraestructura de TI (respectivamente, de TO) a un estado operativo.
- Plan de Reanudación del Negocio (**BRP**, Business Resumption Plan). Plan para desplazarse desde el centro de respaldo, de nuevo, a las instalaciones habituales desde las que se realizan las operaciones del negocio.

Definir plan de pruebas

El objetivo fundamental del plan de pruebas es llevar a cabo todos los pasos documentados en un plan de contingencia. El plan de pruebas permite adaptarse a las pruebas sin necesidad de modificar el plan de recuperación real.

Además, este plan de pruebas ayuda en el análisis de realización de la prueba mediante la calificación del resultado de las actividades realizadas durante la prueba identificando lo que se hizo bien y las áreas que requieren atención.

El propósito de las pruebas es verificar que la solución de resiliencia y continuidad de negocio satisface los requisitos de recuperación (de resiliencia) de la organización. Los planes pueden dejar de cumplir con las expectativas debido a los requisitos de recuperación insuficientes o inexactos, defectos de diseño solución, o errores de implementación solución. Las pruebas pueden incluir:

- Comprobación de llamadas al equipo de crisis
- Comprobación de los lugares de trabajo secundarios
- Verificación de soluciones técnicas (distribución de parches y aplicaciones de seguridad)
- Operatividad hardware y software
- Prueba de recuperación de aplicaciones
- Prueba de procesos de negocio
- Prueba de los medios de respaldo
- Pruebas de los mecanismos de contingencia

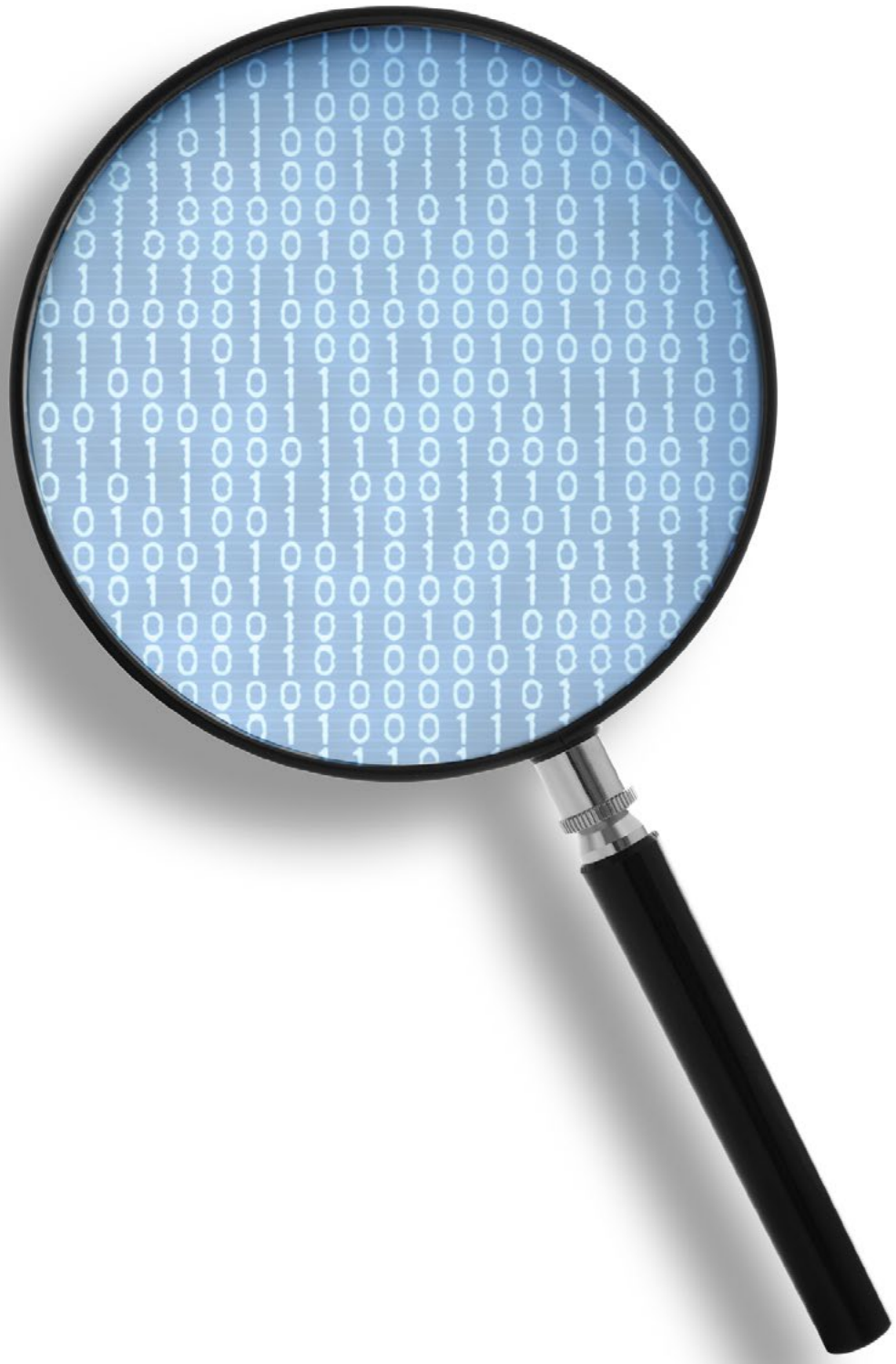
Consideraciones de un plan de pruebas

Un plan de pruebas integral y multidimensional considerará los siguientes elementos:

- El tipo de pruebas a realizar deberán validar los objetivos de recuperación definidos
- Diseñar un programa de pruebas de largo alcance con, métricas de gestión claras
- Preparar escenarios significativos de la prueba, definir los objetivos de aprendizaje y criterios de éxito.
- Gestionar la puesta en escena y la ejecución de las pruebas programadas
- Las herramientas utilizadas deben ser auditables en cuanto a las acciones del equipo, detalles de comunicación, mejoras y las lecciones aprendidas durante la prueba
- Desarrollar acciones pre-, y post-, prueba que permitan identificar vacíos
- Priorizar cuestiones de organización y plan de mejoras del programa de continuidad del negocio.
- Los participantes de la prueba deben recibir formación y sensibilización
- Revisar/ Analizar la integración de mantenimiento y pruebas del plan
- Desarrollar programas de capacitación para futuras pruebas

En la realización de tales pruebas, intervendrán diferentes perfiles, en función de la madurez de la organización, sus recursos, y del nivel de implantación del BCP en la misma:

- El coordinador del BCP y los responsables de las unidades de negocio intervendrán en la verificación (checklist) de las pruebas
- Representantes de las unidades de negocio y otro personal clave en el proceso de BCP, realizarán la ejecución estructurada (structured walkthrough) de las pruebas
- Todo el personal de operación y otro personal de apoyo será responsable de la aplicación (simulation) de los procedimientos del BCP
- Todos los empleados de la organización participarán en la convivencia en paralelo (parallel) de los sistemas de respaldo y de operación normal, previa a la activación definitiva de éstos; y,
- Todos los empleados de la organización, y las dependencias externas intervendrán ante una interrupción plena (full interruption)



6

Dominio 6:
Gestión, Revisión, Mejora y Sostenibilidad del SGCI

DOMINIO 6: GESTIÓN, REVISIÓN, MEJORA Y SOSTENIBILIDAD DEL SGCI

CONTEXTO

REQUISITOS

REQUISITOS PARA EL DESARROLLO Y MANTENIMIENTO DEL SGCI

REQUISITOS PARA LA DEFINICIÓN DOCUMENTAL

REQUISITOS DE EVALUACIÓN Y SEGUIMIENTO

REQUISITOS DE AUDITORÍA INTERNA

FASES DE LA AUDITORÍA INTERNA

REQUISITOS DE SUPERVISIÓN Y MEJORA

PLAN DE MEJORA: EL CAMINO HACIA LA SOSTENIBILIDAD

REQUISITOS PARA LA REVISIÓN POR LA DIRECCIÓN

REQUISITOS PARA LA COMUNICACIÓN

REQUISITOS PARA LA INTEGRACIÓN CON OTROS SISTEMAS DE GESTIÓN

MÉTODO BÁSICO

MÉTODO AVANZADO

MÉTODO EXPERTO

Dominio 6: Gestión, revisión, mejora y sostenibilidad del SGCI
Contexto

CONTEXTO

El presente capítulo de esta guía describe el último -el sexto- de los dominios del marco de referencia del SGCI: **Gestión, Revisión, Mejora y Sostenibilidad del SGCI.**

Figura 26: Marco de referencia del SGCI. Dominio 6

Este dominio ofrece una serie de directrices que deberían contemplarse, como parte fundamental del SGCI, al objeto de garantizar la sostenibilidad del SGCI, proporcionando los recursos precisos para establecer, implementar, mantener, y mejorar de forma continua dicho sistema de gestión. Para lograr dicho objetivo se requiere la medición, análisis y evaluación del desempeño en la gestión de los riesgos de ciberseguridad, para mejorar su efectividad, así como facilitar la integración con otros sistemas de gestión, que normalmente están implantados ya en las organizaciones industriales, como son: el sistema de gestión de calidad, medio ambiente, riesgos laborales o el de seguridad de la información.

Se tratará, por tanto, de establecer una serie de recomendaciones que permitan garantizar y mejorar el SGCI y, por extensión, la ciberseguridad de la propia instalación u organización.

Estos son los aspectos sobre los que deberían establecerse los requisitos:

- El **desarrollo y mantenimiento del SGCI** de forma sostenible.
- La **definición documenta**l de los requisitos y procedimientos de aprobación, revisión y modificación de cuantos recursos formen parte del repositorio documental del SGCI.
- Los requisitos de las **evaluaciones y auditorías** internas y su planificación.
- Los proceso para la **revisión del SGCI por parte de la Dirección** de la organización.
- Los procedimientos de **supervisión y mejora** del SGCI.
- las medidas oportunas que den **respuesta a los incidentes** propios de la operativa del SGCI.
- La **integración con otros sistemas de gestión**.

Dominio 6: Gestión, revisión, mejora y sostenibilidad del SGCI
Contexto

REQUISITOS

Requisitos para el desarrollo y mantenimiento del SGCI

Para garantizar el desarrollo y mantenimiento del SGCI será preciso el soporte de la organización, que estará basado en dotar de capacidad en cuanto a recursos humanos, documentales, así como de comunicación interna y externa, los cuales permitirán el establecimiento, implementación y mantenimiento del Sistema de Gestión.

Dichas capacidades deberán ser adecuadas para dar soporte al desarrollo y mantenimiento del SGCI, identificándose como requisitos fundamentales:

- Requisitos de competencia para recursos humanos:
  - Identificar qué competencia personal es la necesaria para realizar cada actividad necesaria para el desempeño de la ciberseguridad industrial.
  - Asegurar que el personal es competente, fundamentándose en la educación, formación o experiencia.
  - Tomar acciones, cuando sea necesario, para adquirir la competencia necesaria y evaluar la eficacia de las mismas.
  - Como pruebas de esta competencia, conservar la información documentada pertinente.
  - Todas las personas que trabajan bajo el control de la organización deben tomar conciencia de la política de ciberseguridad, su contribución personal en la eficacia del SGCI y las consecuencias de las no conformidades con el SGCI.
- Requisitos de creación, actualización y control de recursos documentales:
  - Incluirá toda la documentación que la organización estime relevante para el SGCI.
- Requisitos de comunicación interna y externa del SGCI:
  - Definición del contenido a comunicar y de sus responsables.
  - Planificación de las comunicaciones.
  - Establecer procesos de comunicación.

Requisitos para la definición documental

Aunque el alcance de la documentación para el SGCI puede variar en función de del tipo de organización por motivos como:

- Su tamaño, el tipo de actividad o las características de los procesos automatizados.
- Los productos y/o servicios.
- La complejidad de los procesos automatizados y sus interacciones.

A la hora de crear la documentación o actualizarla, la organización deberá asegurarse de lo siguiente:

- Quedará identificada y descrita, incluyendo título, fecha, autor o número de referencia.
- Se definirá el formato, indicando idioma, versión, etc.; y sus medios de soporte, como puede ser el papel o un medio electrónico.
- Será revisada y aprobada con respecto a su idoneidad y emitida al personal indicando su ubicación adecuación.

El SGCI requiere de una documentación que pueda ser controlada para garantizar que:

- Esté disponible y sea adecuada para usarla cuando y donde sea necesaria.
- Esté convenientemente protegida contra pérdida de confidencialidad, uso inadecuado o pérdida de integridad entre otras amenazas.

Para el control de esta información, la organización debería definir:

- La distribución, recuperación, acceso y uso adecuado.
- El almacenamiento y su preservación.
- El control de cambios.
- La retención y disposición.

El responsable de la información del SGCI, según la organización, deberá determinar los permisos de acceso a la información, quien podrá consultar dicha información y quien tendrá autoridad para consultar y modificar.

Requisitos de evaluación y seguimiento

La organización debe evaluar el desempeño en la gestión de riesgos de ciberseguridad industrial y la eficacia del SGCI. Para ello es necesario determinar:

- Sobre que procesos y controles debemos hacer seguimiento, es decir, qué se requiere medir.
- Cuáles serán las técnicas de seguimiento, medición, análisis y evaluación requeridas para garantizar que los resultados son válidos.
- Cuándo se ejecutará tanto el seguimiento como la medición.
- Quién es el responsable de la ejecución del seguimiento y medición.
- Cuándo es necesario analizar y evaluar los resultados de seguimiento y medición.
- Quién será el responsable de analizar y evaluar dichos resultados.
- Retener y mantener la información de la evaluación documentada.

Para realizar el seguimiento es necesario establecer una serie de indicadores que permitan determinar el estado del sistema. El análisis de estos indicadores requiere que cada uno de las medidas implantadas esté asociada a una serie de registros que recopilen la información necesaria para la evaluación de la medida.

Por ejemplo, si disponemos de un indicador cuyo objetivo es que el número de incidencias graves de ciberseguridad no sea superior a dos al año. Para poder medir el número de incidentes de este tipo, deberá crearse un registro en el que se recojan las incidencias en el sistema y su nivel de gravedad. La revisión de estos registros permitirá comprobar si el sistema está funcionando tal y como se determinó en los objetivos.

En el **Anexo XXI** se proporciona una plantilla para ayudar a la gestión de indicadores del sistema.

El sistema de gestión contendrá multitud de entradas y salidas que deberán ser revisadas, alguna de ellas por la dirección.

Requisitos de auditoría interna

Las auditorías internas son una herramienta que debe llevar a cabo la organización a intervalos planificados para aportar información que asegure que los objetivos, los controles, los procesos y los procedimientos del sistema de gestión de la ciberseguridad industrial son adecuados y están conformes con los requisitos de la propia organización para su SGCI, así como con los requisitos establecidos.

El programa de auditoría se planificará en base al nivel de importancia de los procesos y de las áreas que van a ser auditadas, además se deberá contar con los resultados obtenidos de auditorías previas. Los auditores elegidos para llevar a cabo la auditoría deben garantizar que se realicen de forma objetiva e imparcial, por esto los auditores no deberán auditar su propio trabajo.

La auditoría permitirá comprobar que el SGCI está implementado y se mantiene de forma eficaz, para lo cual la organización deberá:

- Planificar, establecer, implementar y mantener una serie de programas de auditoría en los que estén incluidos los métodos, la frecuencia.
- Definir un procedimiento documentado en el que se especifiquen las responsabilidades, los requisitos y la dirección de las auditorías, además se debe emitir un informe con los resultados obtenidos.
- Precisar los criterios y el alcance de la auditoría.
- Ejecutar auditorías objetivas e imparciales.
- Garantizar la comunicación de los resultados de la auditoría a la alta dirección.
- Retener y mantener la información de las evidencias de la implementación de estos programas documentada.

Las responsabilidades en torno a las auditorías internas deben estar perfectamente establecidas, es decir, se debe conocer quiénes son las personas encargadas de planificarlas, los requisitos con los que cuentan, la manera de informar sobre los resultados, el lugar donde deben guardarse los registros, etc.

La alta dirección de la organización es la responsable de que el área auditada lleve a cabo las acciones necesarias para eliminar las no conformidades que se hayan detectado durante la auditoría interna, y presente los motivos que causaron la no conformidad lo antes posible.

Durante el seguimiento de las actividades realizadas se tiene que incluir una verificación de las acciones que se han llevado a cabo, además de un informe que indique la verificación de los resultados obtenidos.

Fases de la auditoría interna

1. Preparación de la auditoría.

La persona encargada de llevar a cabo la auditoría, el auditor, conforme a las fechas previstas en el Plan de Auditorías, tiene que comunicar por medio del programa de auditorías a los diferentes departamentos de la organización la fecha en la que tendrá lugar la misma.

En el **Anexo XXII** se proporciona una plantilla para ayudar a la confección del programa de auditoria interna.

2. Realización de la auditoría.

La auditoría estará basada en cuatros aspectos básicos dentro de cada uno de los departamentos de la organización, los cuales deberán verificar:

- La disposición adecuada de la estructura del documento, la actualización, codificación, etc.
- La eficacia de las medidas descritas en los documentos.
- Los documentos cumplen con los requisitos exigidos por el SGCI.
- Se aplica realmente lo descrito en los documentos.

Las comprobaciones se llevarán a cabo durante las reuniones que se realicen entre el auditor interno y las personas que integran el departamento auditado. Durante dichas reuniones, el auditor deberá disponer de las pruebas necesarias que demuestran el cumplimiento de lo indicado en los procedimientos que afectan al departamento auditado.

3. Conclusiones de la auditoría

Una vez realizada la auditoría, el auditor líder encargado de realizarla debe cumplimentar el Informe de Auditoría. Con dicho Informe se establecen las "no conformidades" detectadas para posteriormente proceder a abrir la no conformidad oportuna, y si es necesario realizar la apertura de las acciones correctivas o preventivas que se derivan de la auditoría. Las no conformidades y las acciones correctivas o preventivas que se abran se deben registrar y se hace entrega de una copia a cada responsable de los departamentos afectados.

4. Seguimiento de la auditoría.

Si durante la auditoría se han detectado desviaciones, el auditor será el responsable de realizar las comprobaciones necesarias para corroborar que se están aplicando las acciones propuestas y dentro del plazo de tiempo estimado para cada una de ellas.

Será decisión del auditor interno la aprobación o la no aprobación de las acciones que se han llevado a cabo en cada una de las desviaciones detectadas durante la auditoría, y quedarán reflejadas en el apartado de cierre de la misma.

Si no se aprueba, se deben indicar los motivos por los que se ha llegado a esa conclusión en el correspondiente apartado, y el auditor junto con el responsable de corregir dicha desviación deberá proponer una nueva medida, que bien puede ser una medida correctiva o preventiva. Si por algún motivo persisten las desviaciones, el auditor interno deberá informar a la alta dirección de la organización.

Se originará la apertura de Acciones Correctoras Preventivas siempre y cuando, el Auditor perciba que se reiteran las deviaciones y estas afectan gravemente al buen funcionamiento del Sistema de Gestión.

Requisitos de supervisión y mejora

La organización debe mejorar continuamente la eficacia de su Sistema de Gestión mediante la utilización de la política de ciberseguridad, los objetivos de gestión de los riesgos de ciberseguridad, de los resultados obtenidos tras la realización de la auditoría, mediante el análisis de los eventos monitorizados, o gracias a las acciones correctivas o preventivas y la gestión de la revisión.

Se deberán adoptar las acciones necesarias para eliminar las causas de las "**no conformidades**", teniendo en cuenta los requisitos del Sistema de Gestión. La mejor forma de prevenir que vuelva a surgir una "**no conformidad**" es utilizando acciones correctivas, y se deberá determinar cuáles fueron las causas por las que se dieron las no conformidades. Para prevenir las "**no conformidades**" se deben utilizar medidas preventivas.

La organización deberá identificar los posibles cambios en los riesgos y asociarles acciones preventivas para evitar, en la medida de lo posible, que sucedan. La prioridad para utilizar una acción preventiva vendrá determinada por el resultado obtenido al valorar el riesgo. Las acciones preventivas que se utilicen deberán ser adecuadas al impacto que puedan generar

los posibles problemas, es decir, intentar evitar que la solución sea peor que el impacto generado. La opción de utilizar medidas preventivas para evitar las no conformidades es, a menudo, mucho más rentable que tomar acciones correctivas.

Plan de Mejora: el camino hacia la sostenibilidad

El Plan de Mejora (normalmente con periodicidad anual) es una herramienta que se utiliza durante la mejora continua. Dicho plan es un documento vivo que tiene la finalidad de recopilar todas las acciones implicadas en la mejora continua SGCI y de sus procesos. Se establece en dicho procedimiento el análisis de datos, para cada uno de los diferentes procesos que la organización ha definido para cada uno de los indicadores, a los cuales se les realizará un seguimiento cada cierto tiempo, como ya se ha indicado.

Cuando comienza el año se realiza la apertura del Plan Anual de Mejora, el cual se encuentra formado por todas las acciones de mejora en las que se detallará:

- La fecha de apertura de la acción preventiva o correctiva.
- Número de acción de mejora (se utilizará un número correlativo).
- El origen de la acción (sugerencia, revisión de sistemas, etc.). En el caso de acciones correctivas, preventivas y sugerencias se llevarán al Plan Anual de Mejora cuando se necesita realizar una planificación y seguimiento en el tiempo.
- Descripción de la acción de mejora.
- Planificación de la acción de mejora: se desglosará en acciones mucho más pequeñas y detalladas, y se asignarán plazos de ejecución y los responsables de llevarlas a cabo.
- Seguimiento: lo normal es que el seguimiento se realice trimestralmente, aunque pueden existir excepciones por las cuales se realice el seguimiento antes de la fecha prevista, será el Responsable del SGCI el que determine este aspecto.

Las acciones de mejora se deberán aprobar por parte de la alta dirección de la organización. El Plan Anual de Mejora se irá completando a medida que vayan surgiendo necesidades de planificación en alguna mejora, esto se produce o bien en las reuniones de Comité o en reuniones de algunos de los miembros de este. Si se realiza una reunión en la que no están todos los miembros del comité es necesario que el Responsable del SGCI asista y lo realice con:

- Las acciones de mejora propuestas por cualquier persona que asista a la reunión, entre los que se encuentran los responsables de todos los procesos que se realizan en la organización.
- Las sugerencias propuestas por cualquier trabajador de la organización.
- Las acciones preventivas y correctivas que requieran de una planificación y seguimiento en el tiempo.
- Cualquier otro origen.

En el **Anexo XXIII** se proporciona una plantilla para ayudar a la confección del plan de mejora.

Requisitos para la revisión por la Dirección

La alta dirección de la organización deberá revisar el SGCI dentro de unos intervalos de tiempo planificados, al menos una vez al año, asegurando que se encuentra dicho SGCI implementado adecuadamente y de forma eficaz.

El principal motivo por el que surge la necesidad de realizar una Revisión por la Dirección es conseguir que el Sistema de Gestión cumpla con la conveniencia, la adecuación y la eficacia continua.

La revisión deberá incluir la evaluación de las oportunidades de mejora y la necesidad de realizar cambios en el SGCI, se debe incluir en la revisión la política de ciberseguridad y sus objetivos.

Los requisitos mínimos que debería incluir esta actividad son:

- El estado en que se encuentran las acciones relacionadas con otras revisiones por la dirección.
- Los cambios ocurridos en cuestiones externas e internas que afecten al Sistema de Gestión.
- Retroalimentación del desempeño de dicho sistema, incluyendo:
    - La tendencia de las no conformidades y las acciones correctivas.
    - El seguimiento y los resultados de las mediciones.

- Los resultados obtenidos de la auditoría.
- El cumplimiento de cada uno de los objetivos de la gestión de ciberseguridad.

› Retroalimentación de todas las partes interesadas e involucradas.

› Los resultados obtenidos de la evaluación de riesgos y el estado en el que se encuentra el plan de tratamiento de riesgos.

› Oportunidades de mejora continua.

En concreto la dirección de la organización debe revisar los siguientes documentos:

› El informe de las auditorías internas que recoge el estado del sistema y de las incidencias detectadas.

› Los informes que el comité de gestión dirige al comité de dirección. Estos documentos son una fuente muy valiosa para el seguimiento, ya que reflejan el estado del sistema y los puntos que requieren la supervisión por parte de la dirección.

› El informe sobre las acciones previstas por parte de los diferentes actores involucrados en el sistema según el plan anual de mejora.

› El resumen sobre el estado de las incidencias reportadas y la solución a las mismas.

› La revisión de los objetivos propuestos en cada una de las fases así como el grado de cumplimiento de los mismos.

› Y el resumen sobre los cambios sufridos en la organización.

Los resultados obtenidos de las revisiones deberán quedar perfectamente documentados y registrados, para futuras consultas, y se deberán mantener en perfectas condiciones.

En el **Anexo XXIV** se proporciona una plantilla para ayudar a la confección del documento de revisión por la dirección.

Requisitos para la comunicación

Es importante formalizar las vías de comunicación dentro del SGCI y determinar que es necesario identificar las necesidades internas y externas en materia de comunicación sobre la ciberseguridad estableciendo:

› Qué debe comunicarse.

› Cuándo debe hacerse.

› A quién debe hacerse.

› Quién comunicará.

› Cómo la comunicación será transportada o que medios se utilizarán.

Estos aspectos son extremadamente relevantes cuando ocurren incidentes de seguridad donde la agilidad de los procesos de notificación puede minimizar el tiempo de respuesta y reducir los posibles daños.

Requisitos para la integración con otros sistemas de gestión

En todos los sistemas de gestión hay ciertos elementos comunes que se pueden gestionar de forma integrada. La integración de los sistemas de gestión de una organización supone múltiples ventajas entre las que destacan:

› La reducción del volumen de documentación necesaria para gestionar los sistemas, así como las duplicidades.

› Se reduce el número de registros necesarios para demostrar la correcta implantación de los sistemas.

› Si las auditorías de certificación son conjuntas, se simplifica el proceso de auditoría externa y se reducen los días de auditoría. Si las auditorías no son conjuntas, esta ventaja se convierte en un inconveniente.

› Si los responsables de los sistemas de gestión coinciden en una misma persona se evita duplicidad de algunas actividades.

› Se reducen los costes, gracias a la optimización de recursos en todas sus fases y a un aumento de la eficiencia de los procesos, cuyos aspectos (calidad, medio ambiente, seguridad y salud, seguridad de la información y de operación) dejan de gestionarse independientemente.

El proceso de integración de sistemas de gestión requiere un **Plan de Integración** enfocado a crear un SIG (Sistema Integrado de Gestión) que deberá ajustarse al contexto organizativo. La implantación del Plan de Integración requiere de un cambio cultural en la organización, es decir, un suficiente desarrollo de su nivel de madurez o de experiencia en la gestión.

La aplicación de la gestión por procesos requiere cambios organizativos en el organigrama, la definición

de responsabilidades, entre otros, derivados de la necesidad de dotar a los "propietarios de procesos" de la responsabilidad, autoridad y capacidad necesaria para su gestión, así como para la gestión unificada de los requisitos y factores de los diferentes sistemas que se encuentran en cada proceso.

Es importante destacar que la gestión por procesos se puede aplicar paulatinamente limitando su aplicación a ciertos procesos, áreas o sistemas, o aplicarla a la totalidad de los procesos de la organización.

Según *UNE 66177:2005. Sistemas de gestión. Guía para la integración de los sistemas de gestión*, los tres métodos de integración a utilizar según el nivel de madurez de la gestión por procesos son los siguientes:

Método Básico

Es un método muy rentable ya que requiere una inversión pequeña y se obtienen resultados importantes a corto plazo, debido a la optimización de los recursos destinados a la gestión de la documentación y a la gestión integrada de algunos procesos.

Este método no requiere experiencia en la gestión por procesos, y es abordable por todo tipo de organizaciones.

Entre las acciones que pueden llevarse a cabo en este método se encuentran las siguientes:

- Integrar las políticas de cada sistema de gestión en una política única de sistema integrado de gestión.
- Integrar en un único Manual de Gestión la documentación de los sistemas de gestión que se aplican.
- Definir las responsabilidades y funciones del personal relacionado con los procesos críticos para la gestión de todos los aspectos que cubre el sistema integrado (calidad, medio ambiente, salud y seguridad ocupacional, etc.).
- Integrar la gestión de algunos procesos organizativos comunes a los sistemas teniendo en cuenta los requisitos de cada uno. Por ejemplo, elaboración y gestión de los documentos y registros, auditoría interna.
- Integrar también la documentación de estos procesos.

Método Avanzado

Este método supone la continuación natural del método "Básico", y su rentabilidad se consigue normalmente a medio plazo, ya que se requiere cierta experiencia para implantar eficazmente la gestión por procesos.

Para aplicar este método se necesita un nivel de medio de madurez en la gestión por procesos. Por ello, intentar aplicar este método sin la necesaria experiencia en la gestión por procesos puede suponer la aparición de problemas durante la integración.

Las acciones que, a modo de ejemplo, pueden ser abordadas en este estadio son las siguientes:

- Desarrollo de un mapa de procesos que integre para los diferentes sistemas de gestión, los procesos gestión o estratégicos, los procesos operativos o clave y los procesos de soporte, y sus interrelaciones.
- Definir y gestionar los procesos que contemplan entre otros los siguientes factores: definición de responsables, objetivos, indicadores, elementos de entrada y salida de los procesos, instrucciones que aplican a requisitos de varios sistemas, formación, planificación, procesos relacionados con el cliente, compras, producción y prestación del servicio, mantenimiento, equipos de seguimiento y medición, etc.
- Revisar y mejorar sistemáticamente los procesos teniendo en cuenta los requisitos de cada sistema.

Método Experto

Este método supone la continuación natural del método "Avanzado", y es un método muy rentable, ya que supone extender la integración a corto plazo del sistema de gestión por procesos existente a otras áreas o aspectos no contemplados hasta ahora, sin inversión adicional. Se pueden conseguir grandes resultados si se logra alinear los procesos con las estrategias de la organización.

Se requiere una gran experiencia en la gestión por procesos para aplicar este método. Las acciones que, a modo de ejemplo, pueden ser abordadas en este estadio son las siguientes:

- Establecer objetivos y metas, e indicadores integrados, así como "desplegar" los objetivos e indicadores a los procesos y subprocesos.
- Incluir la "voz del cliente", a los proveedores y otras partes interesadas en el diseño de todos los

procesos.

- Extender la gestión por procesos a las actividades administrativas y económicas.
- Involucrar a los proveedores en la mejora de los procesos.

GLOSARIO

CCI	Centro de Ciberseguridad Industrial
DCS	Distributed control system (Sistema de control distribuido)
HMI	Human-machine interface (Interfaz hombre-máquina)
IACS	Industrial Automation and Control System (Sistema de Automatización y Control Industrial) Véase SCI.
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
ISA	International Society of Automation (Sociedad Internacional de Automatización)
ISO	International Standardization Organization (Organización Internacional de Normalización)
MES	Manufacturing execution system (Sistema de Ejecución de la Fabricación)
PLC	Programmable logic controller (Controlador lógico programable)
SCADA	Supervisory control and data acquisition (Adquisición de datos y control de supervisión)
SCI	Sistema de Control Industrial
SGCI	Sistema de Gestión de la Ciberseguridad Industrial
Sistema de Gestión	Estructura operativa de trabajo, bien documentada e integrada con los procedimientos técnicos y de dirección, cuyo objeto es guiar las acciones de empleados, maquinaria o equipos, así como la información de la organización, de una manera práctica y coordinada que asegure la satisfacción de los diferentes grupos de interés y la eficiencia.
Sistema de Gobierno	En una organización, aquel por el que ésta es dirigida y controlada. En relación a la ciberseguridad industrial, aquel por el que las actividades, presentes y futuras, relativas a la ciberprotección de la organización son dirigidas y controladas.

BIBLIOGRAFÍA

International Electrotechnical Commission. "IEC 62264-1:2013. Enterprise-control system integration. Part 1: Models and terminology". IEC/ISO, 28 de mayo de 2013.
URL: http://www.iso.org/iso/catalogue_detail.htm?csnumber=57308.

International Electrotechnical Commission. "IEC 62443-2-1:2010. Industrial communication networks. Network and system security. Part 2-1: Establishing an industrial automation and control system security program". IEC, 10 de noviembre de 2010.
URL: https://webstore.iec.ch/publication/7030.

International Electrotechnical Commission. "IEC 62443-2-2 Ed. 1.0. Network and system security. Part 2-2: Operating a manufacturing and control systems security program" (PWI). IEC, 5 de marzo de 2009.
URL: http://www.iec.ch/dyn/www/f?p=103:38:0::::FSP_LANG_ID,FSP_APEX_PAGE,FSP_ORG_ID,FSP_PROJECT:25,20,1250,IEC%2062443-2-2%20Ed.%201.0.

Buenas prácticas para el Diagnóstico de Ciberseguridad en Entornos Industriales. Noviembre de 2014.
URL: https://www.cci-es.org/informes-y-analisis-estategicos

Ciberseguridad en el Ciclo de Vida en un Proyecto de Automatización Industrial. Mayo de 2016.
URL: https://www.cci-es.org/informes-y-analisis-estategicos

Buenas Prácticas en el Análisis Forense de Sistemas de Automatización y Control Industrial. Septiembre de 2016.
URL: https://www.cci-es.org/informes-y-analisis-estategicos

Desarrollo y despliegue seguro de software industrial [4.0]. Diciembre de 2017.
URL: https://www.cci-es.org/informes-y-analisis-estategicos

National Institute of Standards and Technology. "NIST Special Publication 800-82. Revision 2. Guide to Industrial Control Systems (ICS) Security". NIST, mayo de 2015.
URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

Idaho National Laboratory. "Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments. Version 1. Draft Recommended Practice". INL Critical Infrastructure Protection Center, febrero de 2007.
URL: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/OpSec_Recommended_Practice.pdf.

International Standardization Organization. "ISO 31000:2009. Risk Management. Principles and guidelines". ISO, 15 de noviembre de 2009.
URL: http://www.iso.org/iso/catalogue_detail?csnumber=43170.

International Standardization Organization/International Electrotechnical Commission. "ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements". ISO/IEC, 1 de octubre de 2013.
URL: http://www.iso.org/iso/catalogue_detail?csnumber=54534.

International Standardization Organization/International Electrotechnical Commission. "ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls". ISO/IEC, 1 de octubre de 2013.
URL: http://www.iso.org/iso/catalogue_detail?csnumber=54533.

ANEXOS: Plantillas de Apoyo a la Construcción de un SGCI

Dominio 1: Definición de una Estrategia de Ciberseguridad Industrial

Anexo I Fundamentos del Negocio
Anexo II Organización del SGCI
Anexo III Alcance del SGCI
Anexo IV Política de Ciberseguridad Industrial

Dominio 2: Gestión de los Riesgos para la Ciberseguridad Industrial

Anexo V Inventario de Activos
Anexo VI Caracterización de Sistemas de Control Industrial
Anexo VII Amenazas y Vulnerabilidades en el Ámbito Industrial - Selección de Controles
Anexo VIII Hoja de Trabajo - Análisis de Riesgos

Dominio 3: Promoción de una Cultura de la Ciberseguridad Industrial

Anexo IX Normativa de Personal
Anexo X Formación y Concienciación

Dominio 4: Establecimiento de Normativas de Ciberprotección en Instalaciones Industriales

Anexo XI Procedimiento de Administración de Cuentas de Usuario
Anexo XII Normativa de Segmentación de Redes
Anexo XIII Plan de Direccionamiento

Dominio 5: Garantía de Resiliencia y Continuidad de los Sistemas de Operación

Anexo XIV Normativa de Ciberresiliencia y Continuidad
Anexo XV Funciones y Responsabilidades
Anexo XVI Identificación de Contactos Clave
Anexo XVII Reglamento de Régimen Interno del Comité de Expertos
Anexo XVIII Escenarios de Riesgo
Anexo XIX Procedimiento de Gestión de Incidentes
Anexo XX Acuerdo de Nivel de Servicio

Dominio 6: Gestión, Revisión, Mejora y Sostenibilidad del SGCI

Anexo XXI Gestión de Indicadores
Anexo XXII Plan de Auditoría
Anexo XXIII Plan de Mejora
Anexo XIV Revisión por la Dirección

AUTORES Y COLABORADORES

Nombre	Compañía	Autor	Colaborador	Revisor
Susana Asensio	CCI	●		
Samuel Linares	CCI	●		
Ignacio Paredes	CCI	●		
José Valiente	CCI	●		
Eduardo Sainz	INDRA	●		
Carlos Asún	Initec	●		
Miguel García-Menéndez	iTTi	●		
Beatriz Martínez	Accenture	●		
Javier Calmuntia	3M			●
Covadonga Villacorta	Accenture		●	
Antonio Rodríguez	Air Liquide		●	
Silvia Villanueva	AXA		●	
Rafael Hernández	Cepsa			●
Eutimio Fernández	Cisco			●
Jose Valdelvira	CLH			●
Rafael Picazo	CLH			●
Miguel Ángel Abad	CNPIC		●	
Arturo Trujillo	DEKRA		●	
Gustavo Bermejo	DKTI			●
Antonio Santana	Endesa			●
Joaquín Álvarez	Endesa		●	
Manel Medina	ENISA			●
Ricardo Cañizares	Eulen Seguridad		●	
María Pilar Torres	Everis			●
Jose Luis Laguna	Fortinet		●	
Pablo Barreiro	Gas Natural Fenosa			●
Javier Zubieta	GMV		●	
Ricardo González	Grupo TSK			●
María José Aniorte	Iberdrola			●
Eusebio García	Iberdrola			●
Marcos Gómez	InCibe		●	
Juana Higuera	Initec			●
Susana Suárez	Intermark		●	
Javier Lorrio	Internet Security Auditors		●	
Raquel Mateos	ISA España			●
Claudio Caracholo	ISSA Argentina		●	

Nombre	Compañía	Autor	Colaborador	Revisor
David Corral	Repsol			●
Erik de Pablo	Rutilus		●	
Elyoenai Egozcue	S21Sec			●
Andrés Núñez	S2Grupo			●
José Rosell	S2Grupo			●
Hector Puyosa	Sabic			●
Jesús Friginal	SCASSI		●	
Mariano del Rio	SecureTech		●	
Elena Ortuondo	Sener			●
Jose María Rivera	Sener		●	
David del Pozo	Siemens			●
Juan Carlos Pozas	Siemens			●
David Marco	Técnicas Reunidas			●
Jesús Mérida	Técnicas Reunidas			●
Manuel Muñiz	Telefónica			●
Ignacio García	Telefónica			●
Rodolfo Rodríguez	Tragsa		●	
Amor Domínguez	TÜV IT		●	

C/ Maiquez, 18 · 28009 MADRID
Tel.: +34 910 910 751
e-mail: info@CCI-es.org
www.CCI-es.org
Blog: blog.CCI-es.org
Twitter: @info_CCI