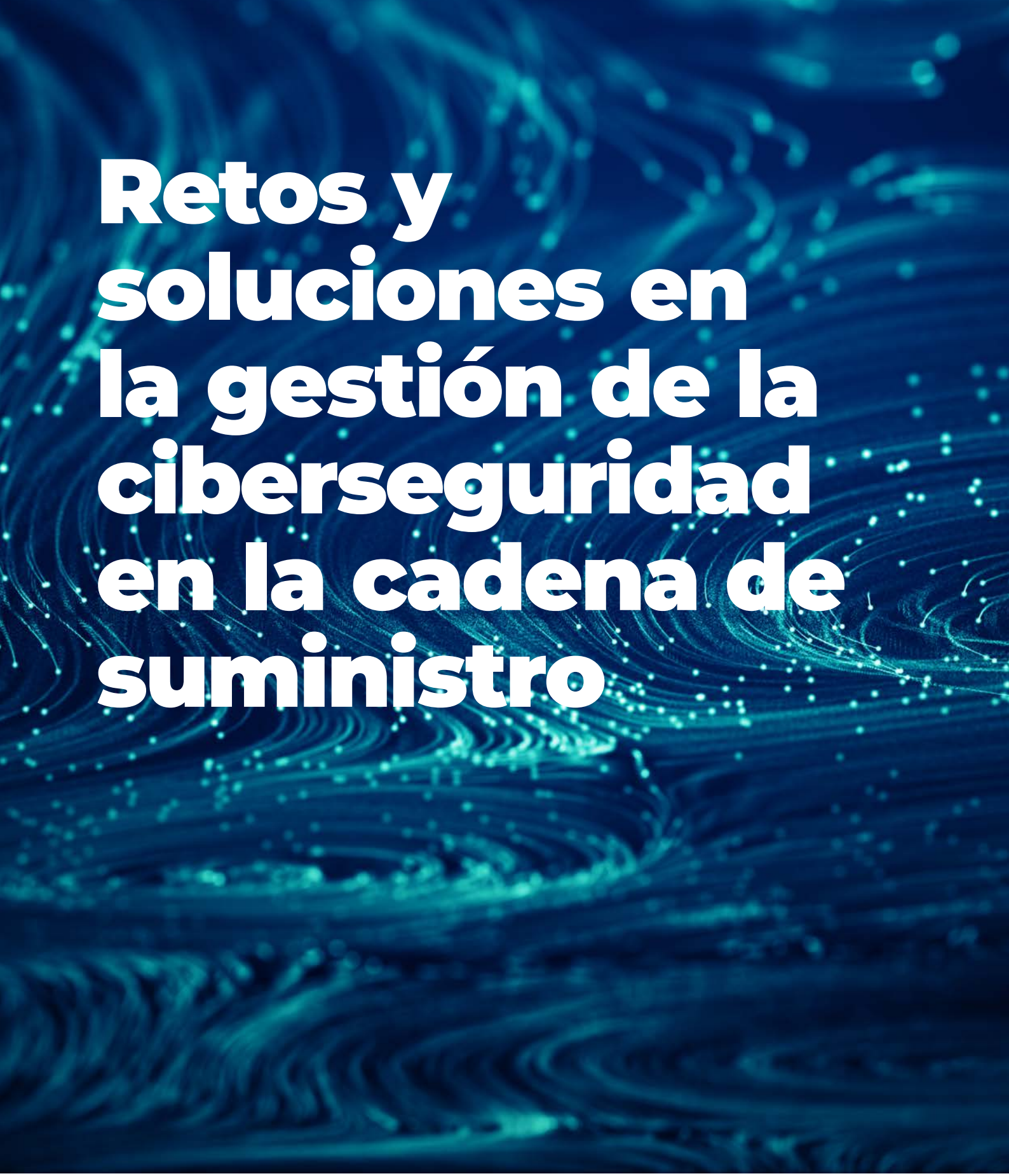
Retos y soluciones en la gestión de la ciberseguridad en la cadena de suministro



CSC CYBER SECURITY CENTRE

isms forum

isms EUSKADI

ZIUR INDUSTRIAL CYBER SECURITY CENTER-GIPUZKOA

COORDINADORES

Francisco Lázaro

Hugo Llanos

Izaskun Onandia

Kerman Arcelay

PARTICIPANTES

Alberto López

Alfonso Pastor

Carlos Asenjo Gutiérrez

Concepción Cordón

David Andrés Hurtado

Fran García Martínez

Iago Fortes Caramés

Jesús Abascal

Juan José Santos

Juan Manuel Valiente

María Penilla Azcuenaga

Noel Castillo

Pablo Ramírez García

COLABORACIONES

Ziur

GESTIÓN DEL PROYECTO

Beatriz García

DISEÑO Y MAQUETACIÓN

Susana Marín

CONTENIDO.

01.

RESUMEN EJECUTIVO

Importancia de la Ciberseguridad en la Cadena de Suministro

1. Los proveedores representan uno de los principales vectores de ataque para las organizaciones, ya sea por acceso directo a redes/sistemas o por el manejo de información sensible.
2. Incidentes recientes y estudios sectoriales muestran que un alto porcentaje de ciberataques se originan o afectan a través de la cadena de suministro, con impactos potencialmente catastróficos para la empresa contratante.
3. La gestión de riesgos de terceros (VRM/TPRM) es ya una exigencia regulatoria en sectores críticos, y su implantación requiere inversión en recursos humanos, tecnológicos y procesos de supervisión.

Requisitos legales y contractuales

1. Las organizaciones pueden y deben exigir a sus proveedores medidas de ciberseguridad tanto por interés propio como por cumplimiento normativo.
2. Normativas relevantes incluyen el RGPD, LOPDGDD, Directiva NIS2, ENS, DORA y la futura CRA, que establecen obligaciones de protección de datos, gestión de riesgos y notificación de incidentes, entre otras.
3. Es fundamental que las obligaciones de ciberseguridad se recojan explícitamente en los contratos, incluyendo cláusulas de responsabilidad, auditoría y mecanismos de supervisión.

Medidas de Seguridad Exigibles a Proveedores

1. Políticas de seguridad organizacional y designación de responsables.
2. Monitorización, gestión y notificación de incidentes.
3. Gestión de accesos con principio de mínimo privilegio y autenticación multifactor.
4. Cifrado de datos en tránsito y en reposo.
5. Evaluación y gestión periódica de riesgos y vulnerabilidades.
6. Pruebas de seguridad (pentesting, auditorías) y formación continua del personal.
7. Políticas de backup y recuperación ante desastres.

Supervisión y control de cumplimiento

1. Uso de cuestionarios normalizados y auditorías para evaluar el nivel de cumplimiento de los proveedores.
2. Herramientas de reputación digital y ratings de ciberseguridad como complemento.
3. La criticidad del proveedor determina la profundidad y frecuencia de los controles.

Certificaciones y estándares

1. Se recomienda exigir certificaciones como ISO/IEC 27001, ENS o TISAX (automoción), aunque se advierte que estas no garantizan por sí solas la madurez ni la idoneidad de los controles implantados.
2. Es necesario complementar las certificaciones con auditorías y evaluaciones específicas de riesgos.

Ciberseguridad por Diseño y Ciclo de Vida del Producto

1. Integrar la ciberseguridad desde las fases iniciales de diseño y desarrollo (Security by Design, SDLC).
2. Exigir documentación técnica, código fuente (o mecanismos de escrow), SBoM y manuales detallados para garantizar la trazabilidad y gestión de activos

Gestión de Servicios Remotos y Asistencia In-Situ

1. Establecer canales seguros (VPN, MFA), segmentación de redes, registro y aprobación de conexiones remotas.
2. Prohibir el uso de dispositivos personales y exigir controles estrictos sobre dispositivos externos en intervenciones presenciales.
3. Mantener registros de auditoría y monitorización en tiempo real de actividades de soporte.

Gestión de Vulnerabilidades y Ciberincidentes

1. Definir procesos de identificación, análisis y remediación de vulnerabilidades durante todo el ciclo de vida de los activos.
2. Preparar y ensayar procedimientos de respuesta a incidentes, involucrando tanto equipos de ciberseguridad como de operación.
3. Documentar incidentes y extraer lecciones aprendidas para mejorar la resiliencia organizacional.

Responsabilidades legales y sanciones

1. El incumplimiento de las obligaciones contractuales y legales en materia de ciberseguridad puede acarrear sanciones económicas severas y la rescisión de contratos.
2. Es esencial poder acreditar la diligencia en la selección y supervisión de proveedores, así como la implantación de medidas de seguridad adecuadas. La criticidad del proveedor determina la profundidad y frecuencia de los controles.

Conclusión

La gestión de la ciberseguridad en la cadena de suministro industrial es una responsabilidad estratégica y legal ineludible. Requiere la integración de controles técnicos, organizativos y legales, una supervisión continua y una cultura de prevención y mejora constante. Las organizaciones deben establecer relaciones contractuales claras, exigir y verificar el cumplimiento de requisitos de ciberseguridad, y apoyarse en marcos normativos y buenas prácticas para reducir su exposición a riesgos y garantizar la continuidad de sus operaciones.

02.

INTRO-DUCCIÓN.

2.1. OBJETO DE LA GUÍA

La gestión de la ciberseguridad en la cadena de suministro es una prioridad ineludible para las organizaciones.

La gestión de la ciberseguridad en la cadena de suministro es una prioridad ineludible para las organizaciones.

Muchas lo han identificado recientemente como requisito legal en las nuevas regulaciones, y se añaden a las que ya eran conscientes y por ello tienen implantados procesos y controles de seguridad específicos.

El objeto del presente documento es servir de guía a aquellas empresas que se planteen ejercer un control, en materia de ciberseguridad, sobre sus proveedores y más extensamente sobre la cadena de suministro; más concretamente, sobre aquellos productos, proyectos, o servicios, que les suministran terceros y en los que su nivel y estado de la ciberseguridad, tiene impacto para la empresa contratante.

03.

REQUISITOS GENERALES DE CIBERSEGURIDAD A PROVEEDORES

3.1. EL PROVEEDOR: VECTOR DE ATAQUE

Hoy en día nadie pone en duda que el concepto “ciberseguridad” para una empresa incluye la relación con sus proveedores. Los proveedores de productos y servicios de Tecnologías de la Información y Comunicaciones (TIC), así como aquellos que, sin pertenecer a la provisión de servicios de este sector, tienen acceso a nuestras redes y sistemas, pueden originar incidencias o incidentes (que en origen hay intencionalidad).

Existen ejemplos notorios de cómo la falta de calidad en las entregas afecta a las operaciones; por ejemplo, el fallo en la actualización de CrowdStrike, que provocó interrupciones severas en múltiples organizaciones. Sin embargo, este trabajo se centrará en los incidentes que surgen de servicios tercerizados y tienen impacto en la empresa contratante.

La significativa importancia y los efectos catastróficos que pueden derivarse de los ataques a la cadena de suministro han llevado a que ENISA lo haya considerado como la mayor de las amenazas, dedicando una publicación específica a *este tema*. Más aún, en su último informe sobre el *panorama de amenazas en 2023*, declara que numerosos estudios elevan hasta un 61% el número de compañías que declaran haber sido impactadas por algún ataque a su cadena de suministro, y el análisis realizado por *SecurityScorecard* indica que el 99% de las compañías en el índice Global 2000 están conectadas con algún proveedor que ha sufrido algún incidente durante los 15 meses de la muestra (correspondiéndose con que el 20% de los proveedores han sido afectados).

Uno de estos estudios es el realizado por LEET Security, enfocado a la ciberseguridad en la cadena de suministro. *El último publicado, correspondiente a 2022*, muestra que, para las organizaciones conscientes de haber sido impactadas por algún incidente, en casi la mitad de los casos, ha tenido su origen en alguno de sus proveedores, lo cual no es extraño teniendo en cuenta que en más de un 50% de los casos, estos proveedores están directamente conectados a las redes de sus clientes, y también en este porcentaje el proveedor dispone y procesa información de sus clientes en sus propios sistemas.

Los ataques a la cadena de suministro no son nada nuevo, y las casuísticas que se pueden encontrar son muy variadas. Como un primer ejemplo real, imagínese una gran cadena de distribución, con centenares o miles de establecimientos y millones de clientes. Todos los centros están diseñados en base a un mismo proyecto, en el que la ingeniería, monitorización y mantenimiento de la climatización es realizada por una empresa especializada. Este proveedor no dispone de medidas adecuadas de protección, y sus credenciales de acceso a la red de mantenimiento son sustraídas. Por su parte, la organización cliente no cuenta con una segmentación apropiada de sus redes, con lo que los atacantes logran instalar su software para robar los datos de tarjetas en varios TPVs, acabando por desplegarse en toda la organización. Resultado: robo de los datos de millones de tarjetas e inmensos costes directos y reputacionales soportados por la organización.

En este ejemplo, el objetivo es la organización finalmente alcanzada, para lo cual los atacantes realizan un análisis de su cadena de suministro a fin de encontrar la puerta de entrada más sencilla, la más débil, resultando esta ser a través del citado proveedor, que, dada su actividad, no parecería representar un riesgo relevante. Esto ocurre a menudo, y se corresponde con una percepción general de que los proveedores son menos resilientes que las propias organizaciones clientes.

Otra casuística muy diferente que se da con cierta frecuencia es la introducción de malware dentro de piezas de algún software que cuente con amplia implantación en organizaciones por todo el mundo, como pueden ser plataformas para la monitorización y gestión remota de servicios y activos IT (para cuya ejecución además se requieren privilegios administrativos).

La distribución de actualizaciones de dicho software conlleva como resultado la implantación del malware en miles de usuarios.

Efecto similar causa la inyección de código malicioso en librerías de código abierto, que son ampliamente utilizadas por numerosos desarrolladores, y así, las aplicaciones resultantes llevan consigo una puerta trasera a todas las organizaciones en que acaban instaladas. Este es un modelo que ofrece escasas barreras de entrada y cuenta con una amplia difusión. Además, su detección suele demorarse al encontrarse ofuscado y activarse solamente bajo ciertas condiciones.

En estos casos el objetivo de los cibercriminales no es una organización en particular, sino el efecto multiplicador que tiene el modelo, y que les permite obtener los beneficios buscados, normalmente rescates económicos, de una interminable lista afectados.

Tenemos pues dos tipos de objetivos de estos ataques a proveedores:

1. **Una organización en particular, alcanzada a través de proveedores con menores capacidades de ciberseguridad que la propia organización objetivo.**

2. **El proveedor, con maximización del número de organizaciones afectadas, mediante la “troyanización” de software de amplia difusión.**

No podemos olvidar un tercer y diferente ejemplo de proveedores con impacto potencial en sus clientes, que es el que viene determinado por los denominados como “no conectados”, pero que cuentan y procesan en sus sistemas con mucha información privada de sus clientes.

Como ejemplo de esta casuística puede considerarse un gran despacho de abogados entre cuyos clientes se encuentran numerosas empresas y particulares con todo tipo de operaciones mercantiles alrededor del mundo, y cuyos detalles pueden resultar altamente sensibles. No se trata del clásico proveedor tecnológico, pero si de una organización cuya operativa está soportada por sistemas y tecnología en la que se procesa información, en muchas ocasiones, comprometedora.

El caso puede originarse con un exempleado que se ha sentido tratado injustamente, por un cliente insatisfecho o por un hacker malicioso, y la puerta de entrada puede ser la falta de actualización de las aplicaciones utilizadas, que contienen vulnerabilidades conocidas…

El resultado será que la ingente cantidad de información que obra en los sistemas del despacho resulta capturada y cifrada o exfiltrada, para público conocimiento y con el espanto del despacho, que puede considerarse como el objetivo directo, pero también de los clientes de este, al ver airear sus más íntimos secretos por todo el mundo, con un clarísimo impacto reputacional (y legal, según el caso).

https://www.leetsecurity.com/es/documentacion/iv-estudio-empresas-ciberseguridad/dl/

Así pues, desde el punto de vista de los proveedores, también podemos considerar dos tipologías:

Proveedores conectados a las redes de las organizaciones, que son utilizados como vía de acceso no autorizado a las mismas

Proveedores no conectados, pero que disponen y/o procesan información de los clientes en sus propios sistemas

Cuando pensamos en proveedores como vector de ataque, la tendencia es a pensar en el primer tipo, que abarca principalmente fabricantes de hardware o software, integradores de sistemas, servicios gestionados y proveedores de servicios digitales/cloud, pero no debemos olvidarnos del segundo, que sin ofrecer esa vía de entrada, pueden llegar a causar severos perjuicios a sus clientes (reputacional, como hemos dicho antes, pero podría también ser robo o difusión de propiedad intelectual/industrial, etc.).

La causa de que un proveedor ofrezca mayores facilidades para el acceso puede ser debida a una menor diligencia del mismo a la hora de implantar y gestionar procedimientos y medidas de seguridad que sus propios clientes, pero también es necesario que las organizaciones, adicionalmente a la implantación y gestión de sus propias medidas de seguridad, lleven a cabo prácticas de gestión de riesgos de la cadena de suministro (conocidas habitualmente como VRM-Vendor Risk Management o TPRM-Third Party Risk Management).

En este sentido, un nuevo informe de ENISA sobre buenas prácticas en la gestión de la cadena de suministro5 (encuesta realizada sobre 1081 organizaciones de los 27 Estados Miembros de la UE) revela que el 53% de las organizaciones no cuenta con un presupuesto aprobado para este propósito, y que incluso en aquellas en las que se realizan este tipo de actividades (un 86% declaran disponer de políticas a este respecto), tampoco lo tiene un 41%, y sólo una pequeña proporción, el 24%, cuenta con personal dedicado a esta función.

Este es un aspecto fundamental que tener en consideración: una adecuada gestión de la cadena de suministro requiere invertir en recursos humanos y herramientas de gestión, tanto por las compañías como por sus suministradores. Pero como toda inversión, debe ser realizada a partir de un cuidadoso análisis, sopesando los costes y beneficios, y tomando decisiones basadas en una comprensión clara de las implicaciones y la exposición al riesgo.

En este contexto, la supervisión y gestión de los riesgos asociados a la cadena de suministro ha adquirido tal notoriedad, que ya ha llegado a ser incluido como obligatorio en diferentes regulaciones. El sector financiero ha sido pionero, con las directrices que la Autoridad Bancaria Europea (EBA) publicó en febrero de 2019, y que se han visto recogidas y ampliadas por el conocido reglamento DORA (Digital Operational Resilience Act), así como en la también conocida Directiva NIS 2, de aplicación a todas las organizaciones consideradas como Esenciales o Importantes, y que será tratado más adelante.

Finalmente debemos recalcar que hemos dejado al margen, por no ser deliberados, las situaciones en las que la seguridad de una empresa se ve comprometida por errores de su proveedor; por ejemplo, **como el que se dio en una actualización de software de CrowdStrike**, que afectó a millones de sistemas Windows, y provocó una interrupción masiva de operaciones en sus clientes a nivel global. El fallo generó la temida «pantalla azul de la muerte», bloqueando equipos y causando estragos en diversos sectores, por perdida de disponibilidad, incluyendo:

A

Transporte

Se retrasaron vuelos internacionales y se interrumpieron operaciones de transporte público.

B

Salud

Los sistemas de hospitales se vieron afectados, obligando a cancelar operaciones no urgentes.

C

Finanzas

Las operaciones bancarias y de pago se vieron ralentizadas o interrumpidas.

D

Empresas

Innumerables empresas de todo tipo experimentaron fallos en sus sistemas informáticos.

3.2. REQUERIMIENTOS DE CIBERSEGURIDAD LEGALES

LAS ORGANIZACIONES TIENEN LA CAPACIDAD DE EXIGIR MEDIDAS DE CIBERSEGURIDAD A SUS PROVEEDORES POR DOS MOTIVOS PRINCIPALES: LA PROTECCIÓN DE SUS PROPIOS INTERESES Y EL CUMPLIMIENTO DE OBLIGACIONES LEGALES.

En primer lugar, una organización puede, en interés propio, demandar que sus proveedores apliquen medidas de ciberseguridad adecuadas para proteger sus datos, sistemas y operaciones. Los proveedores que manejan información sensible o acceden a los sistemas de la organización pueden convertirse en un vector de ataque. Si el proveedor no cuenta con un nivel de seguridad apropiado, los riesgos de sufrir ciberataques aumentan, lo que podría ocasionar impactos operativos, regulatorios, financieros y reputacionales para la organización.

Por otro lado, existen marcos regulatorios que exigen a las organizaciones asegurarse de que sus proveedores cumplan con determinados requisitos de seguridad. **El Reglamento General de Protección de Datos (en adelante, "RGPD"),** por ejemplo, establece la responsabilidad compartida entre el controlador de los datos (la organización contratante) y el encargado del tratamiento; el procesador (el proveedor).

Esto implica que ambas partes deben implementar medidas técnicas y organizativas adecuadas para proteger los datos personales. Normativas como la **Directiva de Seguridad de Redes y Sistemas de Información (en adelante, "NIS2") o la Ley de Resiliencia Operativa Digital (en adelante, "DORA")** obligan a las organizaciones de sectores críticos y esenciales o del sector bancario a gestionar correctamente los riesgos en su cadena de suministro.

Es muy importante entender, cuando una ley establece obligaciones a los proveedores, si estos están en el alcance subjetivo o no, de esa norma.

El ámbito subjetivo de una ley se refiere a las personas o entidades a las que dicha ley se aplica. Es decir, determina quiénes están obligados a cumplir con lo establecido en la ley y a quiénes se les reconocen ciertos derechos o beneficios.

La gran diferencia de una legislación en la que se habla de que las entidades obligadas (bajo el alcance subjetivo) deben gestionar la cadena de suministro y aquellas otras, dónde la cadena de suministro está directamente en el alcance subjetivo, es radical.

En el primer supuesto, en la que el proveedor no está expresamente identificado como sujeto obligado, entendemos que es un brindis al sol, ya que las entidades no pueden hacerse responsables de una forma eficaz de sus proveedores, al carecer lógicamente de capacidad real de gestión de los medios de este.

En el segundo, en el que el proveedor está en el alcance subjetivo, él es directamente un sujeto obligado y, por tanto, responsable directo de cumplir con esa ley. En España, a través de leyes nacionales o trasposiciones de Directivas distintas normativas proporcionan un marco legal para exigir ciberseguridad a los proveedores:

LOPDGDD

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales

Establece que la organización y el proveedor comparten la responsabilidad de proteger los datos personales. Los proveedores están incluidos en el alcance subjetivo. En caso de una brecha de seguridad en el proveedor, la organización puede ser sancionada por las autoridades de protección de datos.

DIRECTIVA NIS2

Aplicable a sectores esenciales y críticos

Obliga a las organizaciones a implementar medidas adecuadas para gestionar los riesgos de la cadena de suministro. En esta Directiva, y en su trasposición los proveedores tienen obligaciones, pero le son dadas de forma indirecta, pues no están en el alcance subjetivo de la Directiva.

ENS

Esquema Nacional de Seguridad

El RD 311/2022 impone a las organizaciones del sector público el cumplimiento de medidas de seguridad para proteger la información. Estas medidas también aplican a los proveedores que gestionan datos o sistemas relacionados con dicho sector. La cadena de suministro está incluida en el alcance subjetivo. Esta ley, exige, por ejemplo, la designación de un Punto de contacto de Seguridad del proveedor para el producto o servicio que presta a la entidad pública.

La Ley de Protección de Infraestructuras Críticas (en adelante, “LPIC”), una vez se actualice con la trasposición de la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo, deberá recoger lo que se dice en esta y en relación a la cadena de suministro e idealmente, mejorar los requerimientos sobre la misma.

La Directiva, presenta una muy somera referencia a la cadena de suministro, ya sea bajo esa denominación o bajo el término “proveedores de servicios externos”. Encontraremos esas referencias en el artículo 13.1. en los apartados d y f. En el apartado d) se dice con relación a las medidas que deben adoptar las entidades críticas: recuperarse de incidentes, considerando con la debida atención medidas de continuidad de las actividades y la identificación de cadenas de suministro alternativas, a fin de retomar la prestación del servicio esencial.

ADICIONALMENTE, DESDE UN PUNTO DE VISTA LEGAL, UNA ORGANIZACIÓN PUEDE EXIGIR A UN PROVEEDOR QUE CUMPLA CON LOS REQUISITOS QUE JUZGUE NECESARIO ESTABLECER, LOS CUALES DEBEN PLASMARSE EN EL CONTRATO.

Por un lado, se pueden exigir los requisitos mínimos de ciberseguridad que impongan las normativas o que, por interés legítimo, se establezcan en función de la criticidad del proveedor. Generalmente, los detalles sobre las condiciones y medidas de ciberseguridad se recogen en el anexo de ciberseguridad del contrato general con el proveedor. Adicionalmente, se puede requerir la auditoría del proveedor para validar que cumple con lo acordado en dicho anexo o que comunique sus informes de vulnerabilidades.

De esta manera, por ejemplo, encontramos que, conforme al ENS, los pliegos de contratación de las entidades públicas deben incluir los requisitos necesarios para asegurar que los sistemas de información de los proveedores cumplan con el ENS. Así los proveedores deberían presentar las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS. Esta cautela se extiende también a la cadena de suministro de los proveedores.

Estas leyes, tomadas en su conjunto, establecen directamente un conjunto de obligaciones; tales como los análisis de riesgos o notificaciones de incidentes y/o brechas de seguridad, o como antes indicamos un punto de contacto de seguridad.

A modo de ejemplo, señalaremos que las obligaciones de los proveedores conforme al Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) se centran en las responsabilidades que asumen como encargados del tratamiento de datos personales. A continuación, se detallan dichas obligaciones:

1. **Tratamiento conforme a instrucciones**

Los proveedores deben tratar los datos personales únicamente siguiendo las instrucciones documentadas del responsable del tratamiento (cliente), incluyendo en materia de transferencias internacionales de datos.

2. **Confidencialidad**

Garantizar que las personas autorizadas para tratar datos personales se comprometan a respetar la confidencialidad o estén sujetas a una obligación legal de confidencialidad.

3. **Medidas de seguridad**

Implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo asociado al tratamiento de datos personales.

4. **Subcontratación**

No recurrir a otro encargado del tratamiento (subencargado) sin la autorización previa y por escrito del responsable del tratamiento. Si se subcontrata, deben imponerse al subencargado las mismas obligaciones de protección de datos.

5. **Asistencia al responsable**

Ayudar al responsable del tratamiento a cumplir con sus obligaciones en materia de seguridad, notificación de brechas de seguridad, evaluaciones de impacto y consultas previas a la autoridad de control.

6. **Gestión de violaciones de seguridad**

Notificar al responsable del tratamiento sin dilación indebida cualquier violación de seguridad de los datos personales de la que tenga conocimiento.

7. **Supresión o devolución de datos**

Al finalizar la prestación de servicios, suprimir o devolver todos los datos personales al responsable, a elección de este, y suprimir las copias existentes salvo que se requiera su conservación por ley.

8. **Información y auditorías**

Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones y permitir y contribuir a las auditorías o inspecciones realizadas por el responsable o un auditor autorizado. En concreto, el artículo 28 del RGPD, en su apartado 3 letra h establece que: “el encargado pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable”.

9. **Registro de actividades de tratamiento**

Mantener un registro de todas las categorías de actividades de tratamiento realizadas por cuenta del responsable, que incluya detalles como:

- ✔ *Nombre y datos de contacto del encargado y del responsable.*
- ✔ *Las categorías de tratamientos realizados*
- ✔ *Transferencias de datos personales a terceros países u organizaciones internacionales.*
- ✔ *Descripción general de las medidas de seguridad técnicas y organizativas.*

10.

Designación de un delegado de protección de datos (DPO)

Cuando sea requerido, designar un DPO y facilitar sus datos de contacto al responsable del tratamiento.

11.

Tranferencias internacionales

No transferir datos personales a un tercer país u organización internacional sin las garantías adecuadas y sin informar al responsable del tratamiento.

12.

Cumplimiento de principios de protección de datos

Respetar los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad.

13.

Protección de datos desde el diseño y por defecto

Aplicar, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas destinadas a aplicar de forma efectiva los principios de protección de datos.

14.

Cooperación con las autoridades de control

Colaborar con la Agencia Española de Protección de Datos (AEPD) u otras autoridades de control en el desempeño de sus funciones.

15.

Responsabilidad proactiva

Ser capaz de demostrar el cumplimiento de todas estas obligaciones, lo que implica una actitud proactiva en la gestión y protección de los datos personales.

Formalización mediante contrato o acto jurídico:

Es imprescindible que el tratamiento por parte del proveedor esté regulado mediante un contrato o acto jurídico que vincule al encargado respecto al responsable y que establezca:

- *El objeto, la duración, la naturaleza y la finalidad del tratamiento.*
- *El tipo de datos personales y las categorías de interesados.*
- *Las obligaciones y derechos del responsable.*
- *Las condiciones específicas para el tratamiento, incluyendo las relativas a la subcontratación y transferencias internacionales.*

Todas estas exigencias deben ser recogidas contractualmente entre la parte contratante y la parte contratada. La protección de los intereses de la organización y el cumplimiento de las normativas vigentes hacen no solo posible, sino necesario, exigir medidas de ciberseguridad a los proveedores. Al establecer medidas claras, realizar en la medida de lo posible la supervisión o exigir auditorías y asegurar el cumplimiento de normativas, las organizaciones pueden reducir considerablemente los riesgos en su cadena de suministro.

3.3. MEDIDAS DE SEGURIDAD EXIGIBLES A PROVEEDORES

Más allá de los requerimientos legales que debemos exigir a un proveedor, la organización puede exigir o sugerir medidas de seguridad adicionales que van a facilitar la confianza entre la organización y su proveedor. Estas prácticas requeridas por la organización a su proveedor pueden variar en función del contexto, el sector y el nivel de exigencia en cuanto a ciberseguridad. En este capítulo enumeramos un conjunto de medidas que podrán ser adaptadas en función de cada contexto.

ORGANIZACIÓN Y CUERPO FORMATIVO

Una correcta práctica de ciberseguridad requiere de al menos una persona que dirija la misma, sin esa dirección no puedo existir el cumplimiento en materia de ciberseguridad. Esa persona o comité (el ENS lo permite) puede ser un trabajador de la empresa o externa al mismo. El cuerpo normativo acredita una cultura organizacional que valora la seguridad, involucrando a todos los empleados en la protección de la empresa, sirviendo de guía y principios a todos ellos.

MONITORIZACIÓN, GESTIÓN DE INCIDENTES Y NOTIFICACIÓN

Un plan de respuesta bien definido, comienza detectando los incidentes en su fase más temprana y para ello es necesario implantar y desarrollar el proceso de monitorización y que mediante su gestión especifique cómo la organización debe actuar ante incidentes de seguridad. También es fundamental la capacidad de notificar al cliente en tiempo real, con toda la información que requiere para sus propios procesos y para elevar a las autoridades de control y colaborar en la remediación.

GESTIÓN DE ACCESOS Y AUTENTIFI-CACIÓN

Requiere políticas de “least privilege” (mínimo privilegio)yautenticación multifactor (MFA) para accesos críticos. Los proveedores deben segmentar accesos y gestionar derechos de acceso de forma centralizada y segura.

CIFRADO DE DATOS

Tanto en tránsito como en reposo, los datos deben estar cifrados. Esto protege la confidencialidad y ayuda a cumplir con normativas como el RGPD y el ENS.

EVOLUCIÓN Y GESTIÓN DE RIESGOS

Los proveedores deben realizar evaluaciones regulares de riesgos de ciberseguridad y actualizaciones de su infraestructura para mitigar vulnerabilidades conocidas.

GESTIÓN DE VULNERABI-LIDADES Y REMEDIACIÓN

Obtener información detallada y actualizada sobre vulnerabilidades con el objetivo de priorizar de las vulnerabilidades y las acciones de parcheo regular para asegurar que el proveedor mantenga la mayoría de sus sistemas actualizados con los últimos parches de seguridad y/o actualizaciones funcionales.

PRUEBAS DE SEGURIDAD Y AUDITORÍAS

Pruebas periódicas, como “pen-testing” y auditorías de cumplimiento, ayudan a garantizar que las medidas de seguridad son efectivas.

CONCIENCIA Y FORMACIÓN EN SEGURIDAD

La formación continua de los empleados en ciberseguridad es clave para reducir el riesgo de ataques de ingeniería social.

BACKUP Y RECUPERACIÓN ANTE DESASTRES

Políticas de respaldo y recuperación de datos probadas para garantizar la continuidad del negocio ante una brecha o desastre.

3.4. RESPONSABILIDADES LEGALES FRENTE A INCUMPLIMIENTOS

La normativa vigente en materia de ciberseguridad ***(ver epígrafe 3.2 de la presente Guía)*** *i*mpone obligaciones a las organizaciones en la materia, cuyo incumplimiento puede acarrear sanciones económicas significativas, pérdida de reputación y asunción de responsabilidades con los clientes. Algunas de estas obligaciones están vinculadas a la implementación y control de medidas de seguridad en la cadena de suministro. Por lo tanto, la asignación de responsabilidades en materia de ciberseguridad dirigidas a proveedores adquiere una importancia esencial.

En el presente epígrafe se analizan las responsabilidades legales frente a incumplimientos contractuales sin que se haya producido un incidente de seguridad en la cadena de suministro. Las responsabilidades legales que pueden derivarse por un incidente de seguridad en la cadena de suministro se analizan en el epígrafe 5.6 de la presente Guía.

En primer lugar, como se ha indicado en los apartados precedentes, es necesario que el contrato entre la organización y sus proveedores establezcan obligaciones relacionadas con la ciberseguridad, así como cláusulas específicas de responsabilidad como consecuencia de un incumplimiento contractual, incluidos incumplimientos relacionados con las obligaciones de implantación de medidas de seguridad adecuadas.

Una vez definidas contractualmente las obligaciones en materia de ciberseguridad impuestas al proveedor, la organización debe llevar a cabo un control continuo y planificado donde se evalúe el nivel de cumplimiento de las mencionadas obligaciones por parte de sus proveedores. Estas actuaciones de control continuo tienen como finalidad el aseguramiento del cumplimiento de las obligaciones contractuales asumidas por el proveedor, así como evaluar la idoneidad de este para seguir prestando servicios a la organización.

Estas actuaciones de control de proveedores se llevan a la práctica a través, principalmente, de dos acciones:

Cuestionarios

Los cuestionarios de ciberseguridad son herramientas que permiten evaluar el nivel de cumplimiento de requisitos de ciberseguridad de la cadena de suministro, tanto de manera previa con la finalidad de decidir su un proveedor es idóneo para su contratación, como una vez iniciada la relación contractual con la finalidad de evaluar si el proveedor cumple con las obligaciones asumidas contractualmente. Una vez iniciada la relación contractual, estos cuestionarios, como mínimo, deben contener información sobre las obligaciones de ciberseguridad específicas asumidas por el proveedor (políticas y procedimientos de seguridad, gestión de accesos, gestión de vulnerabilidades, gestión de incidentes, planes de recuperación, etc.).

Auditorías

Las auditorías de cumplimiento de requisitos de ciberseguridad tienen la misma finalidad que el control de la cadena de suministro a través de cuestionarios. No obstante, las auditorías suelen tener una mayor profundidad de análisis de cumplimiento del proveedor, incluso a través de visitas presenciales a las instalaciones de este en caso necesario.

Un tercer método, complementario a los dos anteriores, pues en modo alguno puede ser sustitutivo de alguno de ellos, es la utilización de webs de reputación en materia de ciberseguridad; como son, por ejemplo, las que representan empresas de “raiting” como BitSight o SecurityScoreCard.

La decisión entre utilizar un método de control u otro radica principalmente en lo crítico que sea el proveedor para la organización, las sospechas de incumplimiento de los requisitos de ciberseguridad asumidos por parte de este y por qué no decirlo: las capacidades de la entidad/empresa y/o las ganas de involucrase en su obligación de control que la ha contratado.

Derivado de dicho análisis, la organización podrá identificar posibles riesgos, incumplimientos contractuales, la necesidad de implantar medidas de seguridad adicionales a las inicialmente previstas y, en último término decidir si el proveedor es confiable.

En el supuesto de que el análisis realizado tenga como conclusión que el proveedor no está cumpliendo con las obligaciones contractuales asumidas, la organización podrá establecer un plazo para que el proveedor cumpla con estas o, en el supuesto de que los incumplimientos sean graves, tomar la decisión de rescindir el contrato. Adicionalmente, si el incumplimiento de las medidas de seguridad pactadas contractualmente, incluso sin que haya mediado un incidente de seguridad, hayan causado daños y perjuicios a la organización, se deberá valorar la posibilidad de exigir una indemnización por los daños y perjuicios causados.

En este punto, es importante destacar el trabajo que, en el ISMS, un nutrido grupo de CISOs ha apostado por un modelo de declaración responsable único y compartido. Este grupo de trabajo ha participado en la identificación del contenido y formato que debería tener este modelo único para que sea realmente útil, eficaz y eficiente sin perder rigor y sin olvidar ningún control de seguridad necesario (ver este informe).

Este cuestionario normalizado, permite evitar el escenario actual de cuestionarios personalizados por cada empresa que quiere conocer la situación de ciberseguridad de cada empresa proveedora y del servicio que cada una de ellas le presta. En su lugar, cada organización (proveedora) completa una única declaración estandarizada, que queda lista para enviarse a los clientes que la precisan, junto con las evidencias correspondientes. Por otra parte, el cliente puede analizar con rapidez esta información y determinar su idoneidad. Además, este modelo compartido simplifica la integración de la información de los diversos proveedores de Tier2 (proveedores de proveedores) en un único cuestionario cuando el Tier1 (proveedor) debe facilitar información a un cliente sobre su organización y la de sus proveedores.

Se agiliza así el proceso, reduciendo los esfuerzos necesarios y proporcionando un enfoque más eficiente y transparente para toda la red de suministro.

3.5. EXIGENCIA DE CERTIFICACIONES A PROVEEDORES

Hemos visto anteriormente el efecto de los proveedores, incrementando la superficie de ataque de las organizaciones, hasta el punto de que ha llevado a la Unión Europea a la publicación de regulaciones que incorporan la gestión de los riesgos derivados de la cadena de suministro como un componente fundamental para el aseguramiento de unas condiciones que permitan alcanzar un adecuado nivel de ciberseguridad y mejorar el funcionamiento de los mercados.

En concreto, la directiva europea NIS2 en el artículo 21 obliga a las compañías a prestar especial atención a los riesgos relacionados con los proveedores o prestadores de servicios directos. Por otro lado, en el artículo 24, permite que los países de la UE (Estados miembros) exijan a las entidades afectadas que utilicen productos o servicios de TIC que estén certificados. Esos productos y servicios de TIC deberán estar certificados de acuerdo con el esquema europeo de certificación de la ciberseguridad (Reglamento UE 2019/881).

Artículo 21 NIS2

Artículo 24 NIS2

Reglamento UE 2019/881

La trasposición española de esta Directiva debe dirimir un aspecto crucial. La NIS2 habla de esquemas de certificación Europeos de Ciberseguridad, que no existen aún, por lo que deberá decantarse por estándares ISO o del Esquema Nacional de Seguridad o por ambas.

Con independencia de que sea una obligación legal o contractual, solicitar certificaciones a proveedores se es una buena práctica para garantizar un nivel adecuado de seguridad en toda la cadena de suministro. Estas certificaciones no solo apoyan, e incluso en ocasiones, aseguran el cumplimiento normativo, sino que también ayudan a las organizaciones a mitigar los riesgos inherentes a la externalización y a fortalecer la confianza en las relaciones con terceros. La adopción de estas certificaciones también responde a requisitos contractuales.

También hemos comentado (ver apartado 3.1) que una proporción sustancial de las organizaciones dice tener implantada alguna política para la gestión de ciberseguridad en la cadena de suministro, pero ya es menor la proporción que cuenta con presupuesto asociado, y solo una pequeña parte dispone de personal dedicado a esta función.

La carencia de presupuestos y personal dedicado conduce a que la modalidad de mayor implantación para gestionar los riesgos asociado sea la solicitud de certificaciones, fundamentalmente ISO 27001, seguida del uso de los llamados “ratings” digitales (evaluaciones no intrusivas que analizan configuraciones e información visible desde el exterior, asignando un nivel de riesgo a los activos observables de la organización).

La certificación ISO/IEC 27001:2022 ***“especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización.”*** Para ello, se basa en la norma ISO/IEC 27002:2022, que conforma el repositorio o marco de controles que contienen o modifican los riesgos determinados en el preceptivo análisis previo.

Estos controles están clasificados en cuatro grandes epígrafes: **Organización, Controles de personas, Controles físicos y Controles tecnológicos**, y abarcan todos los aspectos a considerar para dotarse de un completo programa de seguridad.

En relación a la gestión de la cadena de suministro, nos parece relevante señalar los siguientes apartados:

Una organización con dependencias de sus proveedores hará bien en implantar estos procesos dentro de su sistema de gestión. Ahora bien, la certificación de este sistema no supone que todos estos controles estén implantados con un elevado grado de madurez, ya que cada organización **“puede diseñar los controles según sus propias necesidades”.**

Y esto mismo ocurre con todo el contenido de la norma. Es decir, la certificación ISO 27001 por sí misma visibiliza que se ha implantado un sistema de gestión que trata sobre todos los aspectos con relevancia en la ciberseguridad, pero no evidencia el grado madurez o robustez en su implementación.

Una organización conoce las medidas y controles de seguridad que tiene implantados, pero cuando se exige esta certificación a un proveedor, lo único que sabemos es que el mismo dispone de unos procesos que dan cobertura a todos estos controles, pero no sabemos si el diseño de los mismos, que corresponde a sus necesidades, es el apropiado y se corresponde con las nuestras, derivadas de nuestro análisis de riesgos, para la contratación de sus servicios. Así pues, podemos decir que es una base mínima de confianza.

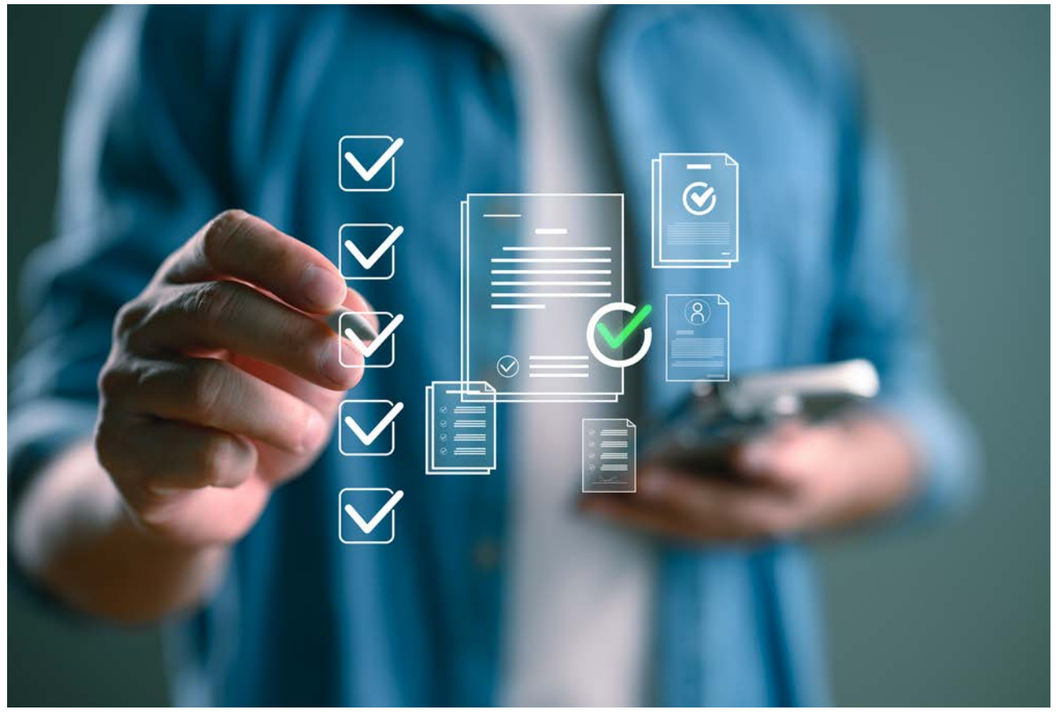
El uso de una base mínima para estos propósitos, puede resultar preocupante cuando se conjugan los datos de escasos recursos para la gestión de riesgos en la cadena de suministro junto al importante porcentaje de incidentes relacionados con los proveedores.

Otras certificaciones, como es el ENS (Esquema Nacional de Seguridad) aportan algo más de información, puesto que ya dispone de una estructura en tres categorías: Básica, Media y Alta, que se corresponden con distintos requisitos para cada una de las medidas de seguridad que lo componen.

El ENS surgió en 2010, enfocando su aplicación a las Sedes Electrónicas de las diferentes entidades del Sector Público, y planteando la extensión de ser requerido a proveedores. Con su actualización en 2022, se ha dotado de un mayor alcance en cuanto a las tipologías de sistemas y servicios sobre los que debe ser aplicado, y enfatizado como un requisito para los proveedores de este sector.

No obstante, las medidas de seguridad contenidas en el mismo mantienen la orientación a los servicios de Administración Electrónica, por lo que su encaje en otro tipo de servicios no resulta totalmente adecuado, especialmente si hablamos de sistema de gestión de ciberseguridad industrial, donde encajaría mejor una norma como la ISA/IEC 62443, si bien esta norma cuenta con poca implantación en nuestro país, lo que hace que no pueda ser exigida a proveedores de forma generalizada.

Llegados a este punto hay una diferenciación entre ambas certificaciones que nos parce muy relevante: ISO 27001 se certifica en base al estándar ISO 17021 de certificación de sistemas de gestión, mientras que el ENS lo hace en base a ISO 17065, de certificación de producto. El primero es lo que permite que el diseño de los controles sea flexible acorde al criterio del evaluado, mientras que la certificación de producto requiere el cumplimiento de los controles establecidos en el estándar, por lo que su resultado es mucho más objetivo.



Por último, cabe mencionar que en automoción existe una certificación requerida por los grandes fabricantes alemanes **(grupo VDA: Verband Der Automobilindustrie – Asociación de la Industria del Automóvil alemana)**, conocida como **TISAX** y que utiliza la norma **VDA-ISA (Information Security Assesment)**. TISAX (Trusted Information Security Assessment Exchange): Es un esquema de certificación específico de la industria de automoción diseñado para asegurar que los proveedores de la cadena de suministro cumplan con los requisitos de seguridad de la información.

Solicitar únicamente una certificación de seguridad de la información a un proveedor, como ISO/IEC 27001, puede parecer un paso sólido para garantizar la seguridad, pero no es suficiente por sí solo para mitigar todos los riesgos relevantes. Existen varios riesgos y limitaciones asociados con depender exclusivamente de la certificación:

1. Cumplimiento superficial o puntual

Las certificaciones suelen basarse en auditorías periódicas, pero esto no garantiza que el proveedor mantenga el nivel de seguridad de manera constante. Un proveedor podría haber cumplido los requisitos solo en el momento de la auditoría, pero no mantener las buenas prácticas de forma continua.

2. Limitaciones del alcance de la certificación

No todas las certificaciones cubren el mismo alcance. Por ejemplo, una certificación ISO/IEC 27001 puede cubrir solo partes específicas de una organización, dejando otras áreas críticas fuera de la evaluación. Es importante asegurarse de que la certificación cubra específicamente los procesos y sistemas relevantes para los servicios que el proveedor nos proporciona.

3. Ausencia de evaluación específica de riesgos

Una certificación es una indicación general de que un proveedor sigue buenas prácticas, pero no sustituye una evaluación específica de riesgos para la organización cliente. Cada empresa tiene necesidades y vulnerabilidades particulares que no siempre se reflejan en las auditorías estándar de certificación.

4. Posibles irregularidades o falta de rigor y calidad

Aunque la certificación esté vigente, podría haber riesgos de fraude o de obtener certificaciones de organismos poco rigurosos. La simple existencia de un certificado no garantiza que el proveedor siga todas las mejores prácticas de manera consistente. En general, la auditoría es solicitada y pagada por la entidad certificada y podría no haber la suficiente independencia y rigurosidad al existir ese vínculo cliente-proveedor.

5. Riesgos de la cadena de suministro extendida

Incluso si un proveedor tiene una certificación válida, puede depender de otros subcontratistas o proveedores externos que no tienen certificaciones adecuadas o que presentan vulnerabilidades. Es necesario asegurar que todo el ecosistema en la cadena de suministro cumpla con los requisitos de seguridad.

6. Auditorías internas y revisiones continuas

La certificación no reemplaza la necesidad de realizar auditorías periódicas internas y externas. Es fundamental llevar a cabo revisiones periódicas de los controles de seguridad y monitorizarlos cuando sea posible, para asegurarse de que se sigan aplicando de forma efectiva en el tiempo.

Con todo lo anterior, no podemos dejar de mencionar otros modelos distintos de las certificaciones y que están concebidos para dotar de mayor visibilidad al nivel real y efectivo de seguridad aportado por las organizaciones en la prestación de servicios, como lo es la calificación de ciberseguridad, que evalúa la implementación y operatividad de procedimientos y medidas técnicas, y ofrece como resultado una valoración del grado de madurez y robustez real ofrecido en el servicio evaluado, siendo el cliente usuario del mismo quien decide si ello resulta adecuado a sus propias necesidades y riesgo inherente.

04.

CIBERSEGURIDAD EN LAS ETAPAS DE INGENIERÍA Y DESARROLLO

4.1. CIBERSEGURIDAD POR DISEÑO

El concepto de seguridad por diseño conocido como Security by Design, (SbD, surge de la necesidad de proteger de manera integral desde las etapas iniciales los componentes que forman la arquitectura de seguridad de un producto o servicio.

Es precisamente en las etapas de diseño y planificación del producto, y en particular de los elementos que lo conforman, donde debe llevarse a cabo un exhaustivo análisis de riesgos de las posibles vulnerabilidades o amenazas a las que puede verse sometido el componente en cuestión, de tal forma que se añadan los elementos necesarios para mitigar todos o la mayoría de los riegos identificados.

El enfoque SbD, es, por tanto, una estrategia eficaz para hacer un producto más sostenible, competitivo y rentable, ya que implica incorporar la seguridad desde el inicio no sólo del componente en sí, sino en cada etapa siguiente del ciclo de vida. Son varios los estudios que indican cómo la metodología de SbD, permite un ahorro significativo de costes en la fabricación de soluciones y productos, al detectar y abordar posibles amenazas en las etapas iniciales de la fabricación o desarrollo. Esto facilita la incorporación de los elementos necesarios para que realmente sea una solución segura. En cambio, si las deficiencias en las medidas mitigadoras de amenazas se identifican al final de la fabricación, es posible que ya no se pueda modificar la ingeniería ni la arquitectura, siendo inviable en el peor de los casos, su uso y comercialización.

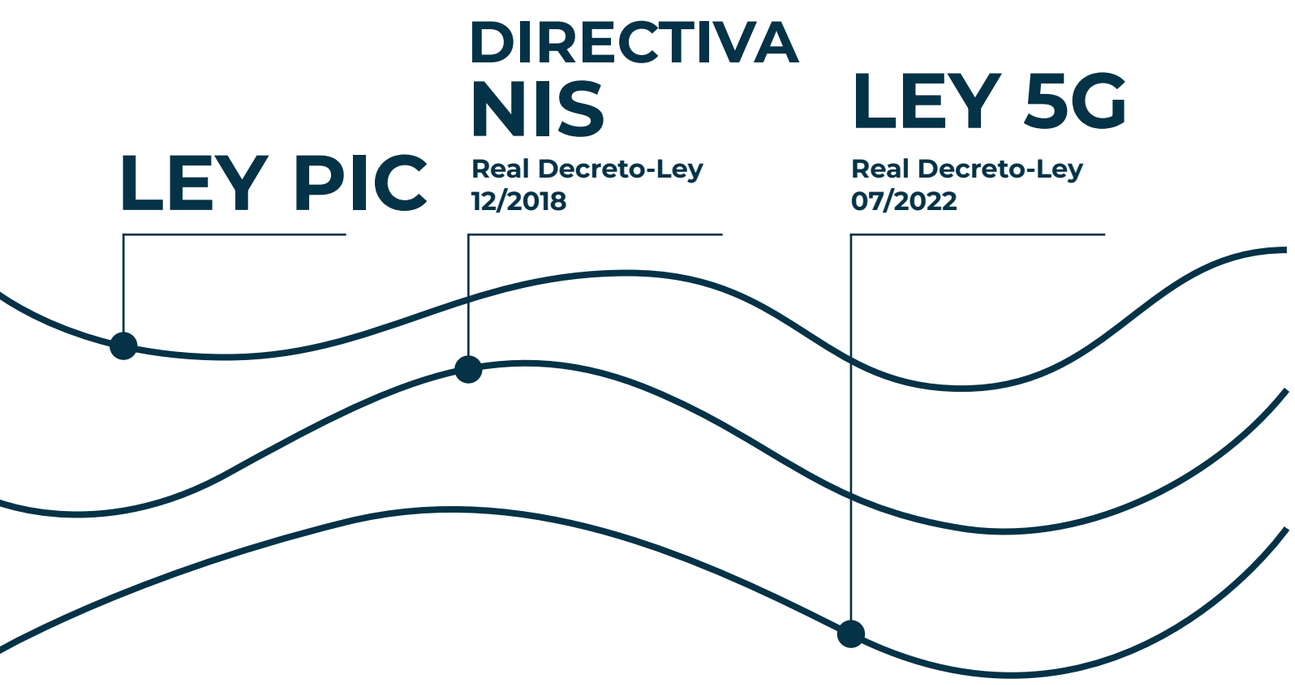
Por otra parte, para abordar la seguridad de una manera integral nace el ciclo del desarrollo de software del producto, conocido como (SDLC), ello permite abordar con seguridad el desarrollo de software y de productos evitando los problemas detectados en el modelo tradicional, donde se detectaban carencias insalvables de seguridad una vez terminado el producto. Los requisitos del ciclo de vida del desarrollo seguro de productos para los sistemas de automatización y control industrial vienen definidos en la norma UNE-EN IEC 62443-4-1.

Para diseñar y entregar productos seguros, el mundo de la industria debe invertir especialmente en las primeras etapas del SDLC, siendo la seguridad un pilar fundamental mediante la aplicación de Security by design(SbD) en cada fase del proceso. Este enfoque se complementa con la metodología del Ciclo Deming (PDCA), cuyas etapas - Plan, Do, Check, Act (Planifica, Haz, Comprueba y Actúa) - establecen los controles necesarios para gestionar y mitigar los riesgos detectados.

El SDLC se puede abordar en distintos momentos del desarrollo del software, recibiendo distintos nombres según el momento de aplicar las fases del PDCA, así se pueden denominar en cascada, iterativo, en espiral, ágil, entre otras, todas tienen su ventajas e inconvenientes, pudiendo no ser excluyentes. Cada organización deberá implementar la que mejor se adapte a la idiosincrasia de funcionamiento global.

4.2. NORMATIVA: LA QUE ESTÁ Y LA QUE VIENE

La preocupación de la UE en el ámbito de la ciberseguridad, especialmente de la ciberseguridad de las infraestructuras y servicios más críticos para la sociedad, ha aumentado en los últimos años con motivo del ascenso de los ciberataques sufridos por las organizaciones. **Con la finalidad de prevenir y saber responder a las preocupantes consecuencias de estos ciberataques, la legislación en materia de ciberseguridad ha crecido exponencialmente en los últimos años en el ámbito europeo.**



En la siguiente tabla se muestra la legislación vigente en materia de ciberseguridad más relevante para entornos industriales, así como su ámbito de aplicación y requerimientos:

NORMA	ÁMBITO DE APLICACIÓN	REQUERIMIENTOS DE CIBERSEGURIDAD
Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC)	Infraestructuras críticas vinculadas a sectores estratégicos	Implantación de medidas de seguridad por infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (norma de transposición Directiva NIS)	Operadores de servicios esenciales y proveedores de servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en la nube	Implantación de medidas de seguridad en las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, así como el establecimiento de un sistema de notificación de incidentes.
Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (Ley 5G)	Proveedores de equipamiento 5G	Implantación de un marco de gestión de riesgos de ciberseguridad, excluyendo a actores de la cadena de suministro categorizados de alto riesgo.

Como se ha indicado al inicio del presente epígrafe, la legislación en materia de ciberseguridad ha crecido exponencialmente en los últimos años y, actualmente, se encuentran sobre la mesa **dos nuevos textos legales** de especial relevancia que afectan al sector industrial.

El primero de ellos es la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión; comúnmente conocida como **Directiva NIS 2.**

La Directiva NIS, su predecesora, ha ayudado a alcanzar considerables progresos en el nivel de ciberresiliencia en la UE, preparando el camino para un cambio significativo de mentalidad. Entre otros, se ha logrado la realización de marcos nacionales de seguridad de los sistemas y redes de información a través de estrategias nacionales de seguridad, la creación de organismos encargados de su supervisión a nivel nacional y europeo, así como la aplicación de medidas por parte de entidades e infraestructuras más críticas. No obstante, desde la aprobación y puesta en marcha de la Directiva NIS, se han identificado algunas deficiencias que impiden afrontar los retos actuales y una falta de homogeneidad en su cumplimiento por parte de cada uno de los Estados miembros de la UE. Consecuencia de ello, se aprueba la Directiva NIS 2.

La Directiva NIS 2 establece obligaciones tanto para los propios Estados miembros de la UE, como para determinadas entidades públicas y privadas. En relación con las obligaciones de los Estados miembros, la Directiva NIS 2 obliga a estos, a grandes rasgos, a crear una estrategia nacional de ciberseguridad en la que se contemple una adecuada evaluación de riesgos de ciberseguridad, a designar las partes interesadas y autoridades nacionales competentes en materia de ciberseguridad, a crear un marco nacional de gestión de crisis de ciberseguridad y a crear una autoridad encargada de su gestión de la ciberseguridad en coordinación con el resto de organismos de otros estados miembros.

ENERGÍA	**TRANSPORTE**	**BANCA**
SECTOR SANITARIO	**AGUAS POTABLES Y RESIDUALES**	**INFRAESTRUCTURA DIGITAL**
ADMINISTRACIÓN PÚBLICA	**ESPACIO**	**SERVICIOS POSTALES Y DE MENSAJERÍA**
QUÍMICA	**ALIMENTACIÓN**	**FABRICACIÓN**
INVESTIGACIÓN	**INFRAESTRUCTURA DE MERCADOS FINANCIEROS**	**GESTIÓN DE SERVICIOS TIC**
GESTIÓN DE RECURSOS	**PROVEEDORES DIGITALES DE MERCADOS EN LÍNEA Y SIMILARES**	

No obstante, no todas las entidades que se dedican a alguno de los sectores indicados anteriormente deben cumplir con la Directiva NIS 2, sino que es necesario realizar un análisis caso por caso para determinar si la mencionada Directiva es aplicable a una organización.

En primer lugar, se debe analizar si la organización es considerada mediana o gran empresa; o si la organización se encuentra en alguno de los supuestos de aplicación específicos en los que no existen requisitos de tamaño (prestadores de servicios de confianza, entidades críticas, etc.). Si la organización cumple alguno de los requisitos anteriores, es necesario analizar si se encuentra en alguno de los sectores indicados en el gráfico superior que, a su vez, establece requisitos específicos de aplicación en función de la legislación aplicable a cada subsector. En consecuencia, el análisis sobre la aplicabilidad de la Directiva NIS 2 no es nada sencillo y deberá realizarse en base a un estudio detallado.

Las entidades obligadas por la Directiva NIS2 deberán cumplir, a grandes rasgos, con las siguientes obligaciones:

Cabe mencionar que la Directiva NIS 2, debido a su carácter de Directiva, no es aplicable a las entidades de los Estados miembros hasta la aprobación de una norma de transposición al ordenamiento jurídico nacional. En este sentido, España no ha transpuesto la Directiva NIS 2 a fecha de publicación de la presente Guía.

El segundo texto legal se corresponde con el conocido como **“Ley de ciberresiliencia de la UE”, “Reglamento de ciberresiliencia de la UE” o “CRA” (Cyber Resilience Act).**

CRA tiene un gran alcance en el sector industrial, debido a que, aplica a todos los fabricantes de productos con elementos digitales cuyo uso previsto y razonablemente previsible incluya una conexión de datos, directa o indirecta, lógica o física, a un dispositivo o red.

La propuesta de Reglamento define “producto con elementos digitales” como cualquier producto consistente en programas o equipos informáticos, y sus soluciones de tratamiento a distancia, incluidos los componentes de programas o equipos informáticos que se introduzcan en el mercado por separado.

Es importante resaltar que, a diferencia del resto de legislación a la que estamos acostumbrados en la que se regula la ciberseguridad a nivel organización o sistemas, **CRA se centra en la ciberseguridad del producto desde su diseño,** con la finalidad de que el producto no salga al mercado hasta que cumpla unos determinados requisitos de ciberseguridad. A grandes rasgos, CRA obligará a:

Gestión de riesgos

- Realización de evaluación de riesgos de ciberseguridad asociados al producto.

- Implantación de medidas de seguridad con objeto de minimizar los riesgos de ciberseguridad, prevenir incidentes y reducir las repercusiones de dichos incidentes.

Documentación técnica

Deberá incluir la evaluación de riesgos y los detalles de cómo cumple el producto con los Anexos que obligan a la realización de pruebas de ciberseguridad del producto establecidos en el reglamento.

Nortificación de incidentes

- Comunicar a ENISA los incidentes de seguridad en el plazo de 24 horas.

- Comunicar a los usuarios del producto los incidentes de seguridad sin demora indebida.

Evaluación de conformidad

Realización de evaluación de conformidad del producto y emisión del certificado de conformidad. En determinados casos la evaluación de conformidad debe ser emitida por un tercero.

En definitiva, nos encontramos en un escenario donde confluyen una gran variedad de textos legales asociados a la ciberseguridad con ámbitos de aplicación diversos, siendo necesario por parte de cada organización realizar un análisis de qué normativa le es aplicable y de esta manera poder elaborar un plan de acción.

4.3. EXIGENCIA DE REQUISITOS DE CIBERSEGURIDAD DESDE LA RFP

En el entorno digital actual, la ciberseguridad se ha convertido en una prioridad crítica para las empresas de todos los tamaños y sectores. En las empresas se están viendo muchas brechas de ciberseguridad, y como estas pueden tener consecuencias devastadoras para una organización. El entorno de exposición de las empresas puede ser muy extenso, y variar mucho según la arquitectura de sistemas, la cultura de la empresa, la exposición pública, empleados, etc. Para preservar la información, los sistemas, las máquinas y/o los servicios prestados a nuestros clientes, uno de los factores más importantes a tener en cuenta son los proveedores y terceros. En concreto los proveedores pueden jugar un papel clave en los procesos de negocio.

Por esta razón, es imprescindible que las empresas incluyan requisitos de ciberseguridad en sus acuerdos con proveedores. Esta afirmación se centra en los siguientes pilares:

PROTECCIÓN DE LOS SISTEMAS

Los proveedores según el servicio prestado pueden tener mayor o menor acceso a los sistemas y datos.

Se deben establecer medidas de seguridad adecuadas para proteger los diferentes sistemas y la información de accesos no autorizados. Es fundamental que la organización exija a cualquier proveedor con acceso a la compañía la adopción de medidas para proteger estas conexiones dan accesos malintencionados y posibles ciberincidentes. Las medidas solicitadas dependerán del tipo de acceso que se le requiera a dicho proveedor y del tipo de información de la compañía que maneje, estas medidas pueden ir de más exhaustivas como puede para un proveedor de infraestructura o más simples un consultor externo, según la valoración del riesgo que se haga de dichas compañías.

CUMPLIMIENTO NORMATIVO

Dependiendo del tipo de empresa, el servicio que presta y el sector, puede haber variedad de proveedores. Estos deben cumplir con las regulaciones del entorno en el que intervienen dado que el incumplimiento de estas regulaciones puede tener afectaciones económicas y de negocio significativas. Es por lo tanto imprescindible que las empresas se aseguren de que sus proveedores también cumplan con estas regulaciones para minimizar el riesgo de incumplimiento y proteger su imagen corporativa.

Los proveedores deben ser conscientes de que el servicio que ofrecen determina las regulaciones que deben cumplir, según el lugar en el que operen. Muchas industrias están sujetas a regulaciones estrictas en materia de ciberseguridad y protección de datos. Para poder cumplir con esto se han de establecer requisitos de ciberseguridad en los contratos con proveedores, las empresas pueden asegurarse de que cumplen con estas normativas, evitando sanciones y daños a su reputación.

REDUCCIÓN DE RIESGOS

Los proveedores pueden ser un punto de entrada para los ciberataques, amenazando las tres dimensiones de la seguridad de la información: confidencialidad, integridad y disponibilidad. Un ciberataque que comprometa a un proveedor puede extenderse a una empresa cliente. Por lo tanto, como empresa cliente, se debe prestar mucha atención a los controles exigidos a los proveedores, ya que, si estos se ven comprometidos, pueden poner en riesgo a la empresa cliente según el tipo de servicio.

Para ello se ha de medir el riesgo de proveedores, y realizar auditorías si se intuyese que no cumple los estándares exigidos de seguridad. El eslabón más débil de la cadena determina el nivel general de madurez en ciberseguridad.

Por este motivo, es importante definir requisitos de ciberseguridad desde el inicio de la relación con el proveedor, ayudando a identificar y mitigar estos riesgos y fortaleciendo la postura de seguridad general de la empresa.

CONFIANZA Y TRANSPARENCIA

Establecer requisitos de ciberseguridad claros y específicos demuestra el compromiso de la empresa con la protección de la información. Esto no solo genera confianza entre los clientes y socios comerciales, sino que también establece una relación de transparencia y responsabilidad con los proveedores.

Al definir estos requisitos, la empresa muestra su dedicación a mantener altos estándares de seguridad, lo que refuerza la confianza de todas las partes involucradas. Los clientes y socios estarán seguros de que sus datos están protegidos, mientras que los proveedores entienden claramente las expectativas y responsabilidades que deben cumplir.

La transparencia en los requisitos de ciberseguridad también facilita una comunicación abierta y honesta con los proveedores que permite identificar y abordar cualquier posible vulnerabilidad de manera conjunta, fortaleciendo la relación y asegurando que todos trabajen hacia un objetivo común de seguridad. Además, al establecer y comunicar estos requisitos, la empresa demuestra su compromiso con la mejora continua y la adaptación a nuevas amenazas cibernéticas. Esto no solo protege la información, sino que también crea un entorno de confianza y colaboración, donde todos los involucrados se sienten seguros y respaldados.

Si tenemos que hacer mención a aquellos aspectos que sintetizan mejor, por qué debemos solicitar requisitos de seguridad en una RFP a proveedores:

Proteger nuestra información.

Asegurar la continuidad del servicio prestado a nuestros clientes.

Asegurar que el proveedor no se convierte en el eslabón más débil de la cadena y nuestro punto débil de compromiso.

Transmitir confianza a nuestros clientes.

Promover las mejores prácticas de seguridad de la información.

En resumen, la inclusión de requisitos de ciberseguridad en los acuerdos con proveedores no es solo una medida preventiva, sino una estrategia esencial para proteger la integridad y la continuidad del negocio. **En un mundo donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, asegurar que todos los socios comerciales cumplan con altos estándares de seguridad es una responsabilidad que ninguna empresa puede permitirse ignorar.**

4.4. MEDIDAS DE SEGURIDAD DE PRODUCTO EXIGIBLES A PROVEEDORES

LAS MEDIDAS DE SEGURIDAD PRESENTADAS EN LA SIGUIENTE TABLA SE CENTRAN EN LOS ASPECTOS TÉCNICOS DE SEGURIDAD QUE DEBEN ESTAR PRESENTES EN LOS COMPONENTES DEL PRODUCTO DE TERCEROS (YA SEA HARDWARE O SOFTWARE) PARA GARANTIZAR SU SEGURIDAD EN ENTORNOS INDUSTRIALES. SE TRATA DE MEDIDAS ORIENTATIVAS QUE HABRÁ QUE CADA ORGANIZACIÓN DEBERÁ ADOPTAR EN FUNCIÓN DEL SECTOR EN EL QUE SE ENCUENTRE, ASÍ COMO EN EL OBJETO DE LOS SISTEMAS A ADQUIRIR.

Se incluyen también requisitos para la gestión de la ciberseguridad a lo largo de todo el ciclo de vida del desarrollo del producto.

Control de acceso, autenticación y autorización

1. Incluir **mecanismos de control de acceso** para asegurar que solo los usuarios y/o componentes autorizados pueden interactuar con el producto.
2. **Habilitar diferentes roles o niveles de** acceso para permitir que cada identidad que interaccione con el producto lo haga de acorde al principio de mínimos permisos necesarios para cumplir su función.
3. Implementar medidas seguras de **autenticación de identidades.**
4. **Requerir el uso de contraseñas seguras,** no permitiendo usar contraseñas por defecto de los componentes.
5. Idealmente, requerir el uso de un **doble factor de autenticación.**

Seguridad de almacenamiento de datos

Incluir **mecanismos de control de acceso** para asegurar que solo los usuarios y/o componentes autorizados pueden interactuar con el producto.

Protección de la comunicación

1. Cifrar la transmisión de los datos entre componentes del producto, así como a otros dispositivos, componentes o proveedores externos. Debe usarse, al menos, el estándar de cifrado de TLS1.2
2. Validar los datos de entrada en las interfaces externas para comprobar que las entradas de usuarios u otros dispositivos son benignas.

Resilencia y disponibilidad

1

Permitir la realización de copias de seguridad o backups, y proporcionar mecanismos de recuperación de datos basado en backups en caso de fallo o ataque del sistema.

2

Implementar mecanismos de filtrado o de failover para garantizar la resiliencia del producto en caso de ataques de denegación de servicio.

Configuración segura

1

Deshabilitar la conexión a Internet de los componentes, salvo en caso necesario.

2

De presentar interfaces externas, requerir que todas ellas estén protegidas mediante mecanismos de autenticación, cifrado y filtrado.

3

Deshabilitar cualquier componente del producto que no sea necesario para cumplir con sus funciones específicas, tales como puertos de red, APIs, conexiones hardware, etc.

Integridad del producto

Proteger la identidad de los datos mediante el uso de hashing, firmas digitales u otros mecanismos de identificación.

Gestión segura de vulnerabilidades

Asegurar que el dispositivo o producto del proveedor cuenta con un mecanismo seguro para la distribución de actualizaciones y/o parches de seguridad, de tal manera que se garantice la autenticidad de los parches antes de su aplicación.

Registro y auditoría

1

Todos los componentes del producto deben registrar cualquier evento de acceso o de cambio de configuración de forma segura. Debe asegurarse que dichos registros de logs no pueden ser eliminados ni alterados. Esto permitirá facilitar la investigación de incidentes.

2

En caso de que el componente sea hardware, debe contar con medidas para detectar y mitigar manipulaciones físicas, como sensores de intrusión, sellos de seguridad o protecciones contra el acceso no autorizado.

Ciclo de vida de desarrollo seguro

1

Definir un proceso formal de desarrollo seguro del producto que garantice que el producto ha sido desarrollado con medidas de seguridad desde la fase de especificación de requisitos hasta el despliegue a producción.

2

Implementar políticas, procedimientos y metodologías en dicho proceso que guíen en el desarrollo seguro del producto.

3

Incluir los requisitos de ciberseguridad desde la especificación del producto como parte integral del diseño y desarrollo.

4

Durante las fases de desarrollo y pruebas, incluir prácticas de seguridad como revisiones de código, tanto manuales como automáticas, y pruebas de seguridad. Asegurar que dichos controles de seguridad no pueden ser evitados fácilmente.

5

Durante el ciclo de vida continuo del producto debe existir y ponerse en práctica una política de gestión y corrección de vulnerabilidades. Esto significa que el producto comercializado por los proveedores no es algo estático, sino en continua actualización para remediar los riesgos que puedan surgir de la aparición de vulnerabilidades en el software del producto.

4.5. EXIGENCIAS DE LOS PROVEEDORES HACIA LOS CLIENTES

Generalidades

Aunque un fabricante o proveedor industrial no puede imponer unilateralmente requisitos de ciberseguridad a sus clientes, sí puede proponer u obligar a cumplir ciertas condiciones y requisitos cuando los clientes hacen uso de la infraestructura del proveedor. Esta clase de condiciones pudieran ser pertinentes en casos en los que se proporciona software como servicio o alquiler de equipamiento.

De exigirse o proponerse dichas condiciones, deberán de observarse en las cláusulas contractuales de prestación. En ellas, el proveedor solicitaría al cliente el alineamiento de su postura de ciberseguridad con la del proveedor.

Este alineamiento deberá de ser **idóneo, necesario y proporcional** en la medida que permita al proveedor mantener su propia postura de seguridad:

Necesariedad

El proveedor no puede establecer controles o medidas adicionales para que el "no alineamiento" del cliente le afecte. Dicho de otra forma, si el cliente decide no implementar un marco de gobernanza y gestión de la seguridad, la empresa del proveedor, los activos del proveedor pudieran verse comprometidos. Ejemplo: un cliente decide dejar en un descampado sin controles de seguridad física material que gestiona tecnologías operativas, alquilado al proveedor.

Idoneidad

El alineamiento de postura de seguridad del cliente es efectivo con relación al objetivo de permitirle mantener al proveedor mantener su propia postura de seguridad. Ejemplo: Mi cliente podría ser corresponsable en el tratamiento de datos según la GDPR si resulta que su sistema cuenta con datos de mis empleados. El cumplimiento de la GDPR es la norma idónea para aplicar

Proporcionalidad

El alineamiento de posturas dependerá del grado de integración de sistemas (esto se suele traducir en cómo de dependientes son los sistemas del proveedor respecto a los del cliente). Ejemplo: Modelo de prestación B2B será más exigente que el modelo B2C.

Por último, hay que señalar que, aunque la persona última responsable de mantener el sistema de gestión de la seguridad de la información del proveedor sería el proveedor, así como los controles dependientes; subsidiariamente se podría hacer responsable al cliente de apreciarse daño o deterioro sucedido por su acción, inacción o negligencia.

05.

CIBERSEGURIDAD EN EL COMMISSIONING

5.1. EVALUACIÓN DE LA CIBERSEGURIDAD EN PRUEBAS FAT Y SAT

Entendiendo que es necesario ejecutar pruebas de funcionalidad en los sistemas entregados, la forma de ejecutar tales pruebas es, al menos, subsistema a subsistema en el entorno controlado de la factoría para las pruebas FAT. Y posteriormente, en conjunto, tras la puesta en marcha, como una parte del todo.

Recomendamos hacer los test de implementación de la siguiente forma:

1. FAT subsistema a subsistema.
2. FAT al sistema completo.
3. SAT al sistema completo.

Recomendamos hacer los test de decomisión de la siguiente forma:

1. FAT al sistema completo.
2. FAT subsistema a subsistema (si fuese necesario).

Los test de seguridad deberían de aprobarse y gestionarse como cualquier otra funcionalidad, dentro del propio proceso de aprobación que la factoría tenga establecido para estas pruebas.

En referencia a los test y controles, ***el documento ISA/IEC 62443-4-2*** contiene una batería de controles de seguridad a implementar en función de los niveles de seguridad (4) en los que un producto pueda estar. En este documento se describe el control y proporciona una guía sobre como testear los controles requeridos.

¿Cómo se evalúan estas pruebas?

Configuración segura

Se verifica que los sistemas estén configurados de acuerdo con las mejores prácticas de seguridad y que se hayan aplicado los parches de seguridad necesarios.

Vulnerabilidades

Se identifican y evalúan las vulnerabilidades en el hardware, software y configuración del sistema.

Fortaleza de las contraseñas

Se verifica la fortaleza de las contraseñas utilizadas y se evalúa la implementación de la autenticación multifactor.

Permisos y accesos

Se evalúa la gestión de los permisos y accesos para garantizar que solo el personal autorizado tenga acceso a los sistemas y datos.

Protección contra malware

Se evalúa la protección contra malware y otras amenazas, como ransomware y virus.

Planes de respuesta a incidentes

Se verifica la existencia y eficacia de los planes de respuesta a incidentes.

Confidencialidad de datos

Restricción de flujos de datos entre partes del subsistema y entre subsistemas

Respuesta a tiempo sobre eventos

Cumplimiento normativo

Se evalúa el cumplimiento de las normativas de seguridad aplicables, como **IEC 62443, NIST CSF, etc.**

5.2. ¿LA CIBERSEGURIDAD COMO ASPECTO A CONSIDERAR EN LA VALIDACIÓN Y ACEPTACIÓN DE UN SUMINISTRO?

Como anteriormente indicamos, **el proveedor es integrador de subsistemas, proveedor, en la medida en la que sus sistemas estén vinculados con los del cliente, podría solicitar incorporar controles para mantener su propio sistema de gestión de seguridad de la información.** Esto se ejecutaría atendiendo a los criterios de necesidad, idoneidad y proporcionalidad anteriormente mencionados. De igual modo, el cliente podría requerir el cumplimiento, en iguales circunstancias de una serie de controles o estándares.

El proveedor puede estar interesado en llevar a cabo pruebas **FAT (Factory Acceptance Test)** para asegurarse que su sistema o subsistema cumple con las expectativas del cliente. De esta forma limita la responsabilidad civil por falta de cumplimiento. De igual modo, si el está interesado en ejecutar **SAT (Site Acceptace Test)** con el fin de justificar que la integración ha sido exitosa.

Si por modelo o necesidades de negocio, el proveedor quisiera recuperar el sistema para seguir explotándolo comercialmente, podría realizar una prueba FAT al reincorporar el sistema a su inventario disponible. Esto permitiría que, en caso de apreciarse deterioro en el sistema o subsistema, pudieran iniciarse las acciones correctivas o compensatorias pertinentes.

Con esto se justificaría totalmente la existencia del testeo de sistemas y la incorporación de requisitos de seguridad en dichos testeos.

5.3. EXIGENCIAS DE DOCUMENTACIÓN Y CÓDIGO FUENTE

Durante la fase de commissioning o puesta en marcha es primordial exigir a los proveedores y terceras partes la documentación detallada y el código fuente del software o aplicación que se va a integrar en el SGCI, además de la plataforma de integración (Herramientas, compiladores, ficheros de configuración, etc.). Esto garantizará a la empresa poder mantener un inventario de activos de todas las partes que conforman el **sistema OT,** para su posterior gestión de activos (análisis de riesgos, gestión de vulnerabilidades, instalación de parches de seguridad, etc.). No disponer de dicha documentación y código fuente puede suponer un gran riesgo para el compromiso de la seguridad y el cumplimiento dentro de un SGCI.

En este momento, no hay ninguna normativa que obligue a terceras partes de un SGCI a compartir una documentación específica del componente a integrar, más allá de menciones genéricas alrededor de proporcionar garantías suficientes ciberseguridad en proveedores ***(por ejemplo, en el RGPD, NIS2, la ISO/IEC 62443 o la ISO 27001).*** Normalmente, estas "garantías" se satisfacen por contrato, asegurando materias como la confidencialidad o el copyright. Es por ello, que esta guía pretende dar las pautas para extender las exigencias de ciberseguridad a proveedores de una forma más práctica y concreta.

Entre la documentación específica que se debería pedir a los proveedores podemos destacar:

1. **Listado de activos software y hardware** del componente o sistema de terceros. Esto puede ser en diferentes formas o versiones. Dentro de los activos software una de esas formas podría ser un Software Bill of Materials (SBoM); un listado de todas las librerías, dependencias y paquetes software de terceras partes, junto con sus números de versiones, que componen a su vez el software del proveedor. Estos SBoMs están cada vez tomando mayor relevancia y se espera que empiecen a ser obligatorios en diferentes organismos de Estados Unidos, incluido el ejército, que integren programas de terceros.

2. En muchas ocasiones, los contratos con proveedores son "llave en mano". Así, para componentes software donde aplique, no basta con requerir un SBoM, si no que directamente se comparte el **código fuente y/o ejecutables** del programa. En este sentido, es importante que el código fuente esté bien documentado. Por otro lado, si el proveedor usara un repositorio de control de versiones para el desarrollo software, se podrá pedir el acceso a dicho repositorio de código, facilitando la trazabilidad de los cambios.

3. Dado que podemos encontrarnos con cierto rechazo del proveedor a la hora de compartir su código fuente propietario, en muchas ocasiones se usan figuras como *"code strokes"* o *"escrows de código fuente"*. Éstos son acuerdos legales en los que una tercera parte independiente guarda en custodia el código fuente del proveedor, asegurando que el integrador del software pueda seguir teniendo acceso al código fuente si el proveedor cesara su actividad o dejara de cumplir sus obligaciones. Así, el escrow supone una medida de seguridad o protección para el implementador del SGCI ante la dependencia del código fuente del proveedor, garantizando la continuidad de las operaciones del SGCI.

4. **Manuales de operación y guías técnicas** con instrucciones detalladas sobre la operación y mantenimiento del activo, así como sus opciones de configuración de elementos de seguridad y despliegue de actualizaciones. Estos manuales también deberán detallar, como vimos en el punto 3.4 de esta guía, los pasos a seguir para cambiar las contraseñas por defecto del fabricante y habilitar mecanismos de control de acceso seguros. Dentro de este apartado, y también relacionado con el punto 3.4 de la presente guía, se puede esperar que los manuales técnicos describan cómo se puede acceder a los logs de eventos del sistema y cómo interpretarlos..

5. **Documentos específicos de seguridad.** Desde certificados de cumplimiento con normativas y/o regulaciones, hasta políticas internas de seguridad (gestión de amenazas o corrección de vulnerabilidades) que proporcionen un óptimo nivel de confianza respecto al programa de seguridad del proveedor. Además, pueden incluirse en esta categoría ***Service Level Agreements (SLAs)*** para garantizar que la notificación de incidentes y la corrección de vulnerabilidades se realiza dentro de unos períodos de tiempo acordados.

6. **Registros de pruebas y auditorías** que certifiquen, por un lado, que el software o hardware ha pasado satisfactoriamente pruebas internas de funcionalidad y de seguridad y, por otro lado, que terceros independientes han certificado el cumplimiento de normativas y regulaciones de seguridad.

7. Cuando se trate de software, **licencias** sobre el software entregado, que detallen claramente los términos **de uso**, así como los **derechos** modificación, adaptación o comercialización que tendrá la empresa dueña del SGCI sobre el código fuente.

8. Si procediera, un **mapa de red o un diagrama con la infraestructura** de los componentes que forman el sistema a integrar, con sus ubicaciones y conexiones entre sí.

06.

CIBERSEGURIDAD EN LAS FASES DE O&M

6.1. SERVICIOS DE MANTENIMIENTO Y SOPORTE REMOTOS

Los servicios de mantenimiento y soporte remoto son una práctica que se está expandiendo rápidamente en las empresas, dado que **resuelve las problemáticas relacionadas con el acceso a instalaciones con alta dispersión geográfica, así como la inmediatez en la prestación de servicios.**

Estos servicios son esenciales para garantizar la continuidad del negocio, la continuidad operativa, así como la eficiencia de los sistemas tecnológicos de las instalaciones, por lo que no cabe duda de que la ciberseguridad debe constituir un requisito fundamental para garantizar que la prestación de estos servicios, tanto llevados a cabo por personal interno como por externo, se realiza con total seguridad.

Así, los proveedores pueden ofrecer soporte técnico, realizar actualizaciones y resolver incidencias sin necesidad de estar físicamente presentes en las instalaciones del cliente.

Sin embargo, la prestación de servicios en esta modalidad introduce desafíos y riesgos de ciberseguridad significativos que deben ser gestionados adecuadamente, dado que habilitan el acceso remoto a sistemas sensibles, pudiendo aumentar la posibilidad de existencia de brechas de ciberseguridad que pudieran ser empleadas por terceros para comprometerlos.

Por lo tanto, es crucial para las empresas implementar medidas robustas que atiendan y permitan proteger la confidencialidad, la integridad y la disponibilidad de los datos y sistemas IT y OT durante las conexiones remotas.

Por otro lado, y considerando la necesidad imperiosa de gestionar adecuadamente los accesos remotos, se recomienda encarecidamente que todas las actividades relacionadas con la gestión se encuentren procedimentadas formalmente, y que la aplicación del procedimiento se realice de forma estricta.

A continuación, se detallan los aspectos clave de cara a prestar un servicio de mantenimiento y soporte remoto más seguro.

6.1.1. Vías de conexión

Uso de canales seguros

Sin duda alguna, es imprescindible que todas las conexiones remotas se establezcan a través de canales seguros y cifrados. Ejemplos de esto son las redes privadas virtuales (VPN), y el uso de protocolos seguros en el establecimiento efectivo del acceso al elemento final sobre el que se requiere el acceso (como SSH, RDP, etc.) en múltiples factores de autenticación).

Adicionalmente a lo anterior: Implementar TLS para garantizar la confidencialidad e integridad de los datos, especialmente cuando se necesite integrar la seguridad de las conexiones VPN con otros servicios que ya utilizan TLS. Aunque también podemos valorar WireGuard, IKEv2/IPSec, etc.

Evitar el uso de protocolos inseguros (telnet, FTP, ...) en los que el tráfico, incluyendo los procesos de autenticación, viajan en texto claro a través de la red. prestar un servicio de mantenimiento y soporte remoto más seguro.

Autentificación robusta

El acceso remoto debe estar protegido mediante autenticación multifactor (MFA), combinando la autenticación basada en el clásico usuario/contraseña (que lógicamente deben ser construidas de forma robusta) o certificados digitales con factores adicionales integrados en el proceso de autenticación, como biometría, tokens o dispositivos de autenticación física.

Segmentación de red

Las conexiones remotas deben tener como origen y destino redes ya segmentadas que permitan aislar los sistemas críticos del resto de la infraestructura. Esto ayuda a reducir la superficie de impacto, en ambos extremos, en caso de materialización de un ciberincidente en caso de compromiso del entorno.

Por lo tanto, para lograr estar alineados con estos tres puntos y lograr en ambos extremos (sistema/s del proveedor y del cliente) que las vías de conexión utilizadas para los servicios remotos sean seguras y confiables, se contemplan varios mecanismos:

Redes privadas

siempre que sea posible, el uso de redes privadas de comunicaciones (como las redes MPM 5G, por ejemplo) en lugar de redes públicas (Internet) para minimizar el riesgo de interceptación de datos e información.

Conexiones VPN (Virtual Private Network)

son una opción común, ya que proporcionan un túnel cifrado entre el proveedor y el cliente (entre los extremos de la comunicación), protegiendo los datos en tránsito. Además, y como se ha indicado anteriormente, es crucial implementar autenticación multifactor (MFA) para asegurar que solo personal autorizado pueda acceder a los sistemas. Entre las opciones, tenemos:

OPEN VPN

Ampliamente utilizado y muy seguro. Soporta múltiples cifrados y autenticación robusta. Puede configurarse para usar TLS para el handshake y luego cambiar a cifrados simétricos para el tráfico de datos

WIREGUARD

Conocido por su simplicidad, alta velocidad y seguridad, utiliza criptografía moderna **(Curve25519, ChaCha20, Poly1305, BLAKE2s)** que es muy eficiente para proteger datos en tránsito.

IKEV2/IPSEC

Ofrece una buena combinación de seguridad y movilidad, ideal para usuarios que necesitan cambiar de red con frecuencia.

SSL/TLS VPNS

Se trata de soluciones basadas en navegadores que utilizan SSL/TLS para cifrar el tráfico. Proveen acceso seguro a aplicaciones internas sin necesidad de instalar software en el cliente.

Protocolos de acceso a elementos finales, entre otros:

RDP con NLA (Network Level Authentication): el servicio de RDP (Remote Desktop Protocol) de Microsoft puede ser configurado con autenticación de nivel de red para prevenir ataques de tipo MitM (Man-in-the-middle) y por fuerza bruta. Por lo tanto, conviene combinarlo con TLS, con objeto de cifrar la sesión de RDP, asegurando que los datos sean confidenciales durante la transmisión.

VNC: algunas versiones del protocolo de acceso remoto VNC permiten establecer parámetros de configuración seguros para el establecimiento de las conexiones, con la integración de la autenticación con repositorios de usuarios externos, el cifrado de las comunicaciones, o el rechazo de conexiones entrantes en caso de que no se acepten expresamente.

SSH (Secure Shell): Para acceso a servidores Linux o Unix, SSH es el estándar para proteger el tráfico de comandos y datos. Aunque no es tradicionalmente usado para soporte de escritorio, puede ser parte de una estrategia de acceso remoto seguro.

Autenticación multifactor (MFA)

Integrar MFA con cualquier solución de acceso remoto aumenta significativamente la seguridad, asegurando que solo usuarios autorizados puedan acceder a los datos en base a el uso necesario de dos o más medios de autenticación.

Conexiones directas vs. conexiones a través de plataformas de terceros:

Las conexiones directas ofrecen un control más riguroso dado que no existen intermediarios que actúen como “enrutadores” del tráfico entre los extremos, mientras que las plataformas de acceso remotos de terceros como TeamViewer o AnyDesk, cuyos nudos de comunicaciones que realizan el enrutamiento del tráfico entre los extremos de las comunicaciones se localizan generalmente en entornos cloud, brindan mayor comodidad a costa de establecer una relación de confianza en las medidas de seguridad implementadas en su infraestructura cloud por los fabricantes.

Indudablemente, el uso de conexiones a través de plataformas de terceros, de usarse, deben ser valoradas y aprobadas previamente y ser configuradas para cumplir con los estándares de seguridad fundamentales definidos en la organización, incluyendo como mínimo la encriptación de extremo a extremo y la gestión de permisos de acceso.

IMPORTANTE: en ningún caso deberían habilitarse medios de conexión basados en la exposición directa de protocolos de acceso remoto a los dispositivos finales, accesibles desde Internet, generalmente configurados como redirecciones de puertos en los dispositivos de comunicaciones (routers) o de seguridad (cortafuegos). Esta práctica conlleva un elevado riesgo no admisible.

Evaluaciones de seguridad

Realizar evaluaciones de seguridad periódicas en los dispositivos y medios de acceso corporativos para identificar y mitigar vulnerabilidades, tanto de los propios dispositivos empleados (vulnerabilidades en firmware, por ejemplo) como en la propia configuración de estos (malas prácticas en la definición de reglas de seguridad, por ejemplo).

6.1.2. *Control de las conexiones por parte de los clientes finales*

Registro y aprobación previa

Para asegurar que el soporte remoto se realice de manera segura, consensuada y de acuerdo con unos objetivos previos establecidos previamente, toda conexión remota debe ser registrada y aprobada previamente por el cliente final. Los mecanismos de aprobación podrían incluir:

- ***Sistemas de tIckets o solicitudes formales:***
  los clientes pueden emitir un ticket o una solicitud formal a través de un sistema de gestión de incidencias, correo electrónico, especificando o acordando los detalles y necesidades para la conexión.

- ***Notificaciones automáticas:***
  envío de notificaciones al cliente cada vez que un proveedor intente establecer una conexión remota. Esto permite al cliente verificar y aprobar la conexión antes de que se establezca, asegurando que todas las interacciones sean las esperadas y autorizadas.

- ***Firmas digitales:***
  los clientes pueden usar firmas digitales para aprobar conexiones remotas, proporcionando una verificación segura y legalmente vinculante de su consentimiento para el acceso remoto.

Visibilidad y monitorización

El cliente final debería tener visibilidad completa de las actividades realizadas por el proveedor a través de la conexión remota. Esto podría incluir:

Monitorización en tiempo real de las sesiones remotas

Permite al cliente observar en tiempo real todo lo que está haciendo el técnico de soporte en su sistema. Esto asegura transparencia y confianza durante la sesión de soporte.

Grabación de las acciones realizadas durante la conexión para auditorías futuras

Todas las acciones realizadas en la sesión remota son grabadas, proporcionando un registro detallado que puede ser revisado en caso de que sea necesario investigar o auditar el soporte técnico brindado.

Alertas de actividad inusual

Implementación de sistemas que notifiquen al cliente de cualquier actividad que se desvíe de los patrones normales o de las acciones previamente aprobadas, permitiendo una respuesta rápida ante posibles irregularidades.

Acceso a logs detallados

Proveer al cliente de registros completos de cada sesión de soporte, que incluyan no solo las acciones técnicas, sino también la duración de la sesión, los cambios realizados en el sistema, y cualquier dato transferido o consultado.

Políticas de acceso basadas en roles (RBAC)

Definir y aplicar políticas de acceso basadas en roles, siempre aplicando el principio de mínimo privilegio, para asegurar que los usuarios solo tengan acceso a los recursos que se requieren para la intervención remota.

Políticas de “qué, quién, cuando y para qué”

El cliente final debe definir claramente los criterios para las conexiones remotas. Es esencial disponer de un control total sobre las conexiones remotas, y la actividad realizada a través de ellas, para garantizar que solo el personal autorizado pueda acceder a los sistemas.
Ante esto, corresponde definir lo siguiente:

Qué

Identificar los sistemas y recursos a los que se requiere acceder.

Quién

Debe existir una política clara sobre quién está autorizado para iniciar conexiones remotas. Esto incluye roles específicos dentro de la organización y proveedores externos con acuerdos de confidencialidad y cumplimiento de normativas de ciberseguridad. Por lo tanto, es necesario definir qué usuarios del proveedor dispondrán de autorización para el establecimiento de la conexión remota.

Cuándo:

Las conexiones deben ser programadas y autorizadas previamente, con registros detallados de inicio y fin de sesión. Es necesario especificar franjas temporales (fechas y horarios permitidos) para el establecimiento de las conexiones remotas.

Para qué:

Cada conexión debe tener un propósito claro y documentado. Detallar inequívocamente los objetivos permitidos para cada conexión remota.

6.1.3. *Exigencias en medios de acceso alternativos no corporativos*

Un aspecto fundamental en relación con los medios de acceso remoto es la importancia de que la organización comprenda que únicamente es posible el empleo de los medios corporativos autorizados, y que en ningún caso deben establecerse "puertas traseras" que permitan, puntual o permanentemente, las conexiones a las redes corporativas IT/OT. El uso de medios no corporativos de forma puntual deberá siempre, previo a su uso, ser puesto en conocimiento del responsable de ciberseguridad para obtener una autorización de uso.

Una vez finalizada la intervención, se procederá con el apagado y retirada inmediata del medio de acceso remoto alternativo.

Con el objetivo de disponer de una bitácora del uso de medios de acceso excepcionales, se recomienda mantener un registro de estos.

6.1.4. *Requisitos en dispositivos empleados por terceros*

Prohibición del uso de dispositivos personales

Los proveedores deben utilizar dispositivos corporativos gestionados para garantizar el cumplimiento de las políticas de seguridad. El uso de dispositivos personales no gestionados (BYOD) por parte del personal de los proveedores debe estar estrictamente prohibido, dado que no se puede garantizar que estos dispositivos dispongan de las medidas de seguridad adecuadas (antivirus efectivo y actualizado, últimos parches y actualizaciones de seguridad en el sistema operativo, etc.) para el establecimiento de una conexión a un tercero, sin incorporar un riesgo implícito a la propia conexión.

Requerimientos en los dispositivos empleados para el acceso remoto

Los dispositivos utilizados por los proveedores para el acceso remoto deben cumplir con una serie de requisitos de ciberseguridad, tales como:

Sistemas operativos actualizados y parcheados

Asegurar que el sistema operativo del dispositivo de acceso remoto esté al día con las últimas actualizaciones de seguridad para proteger contra vulnerabilidades conocidas

Software antimalware activo y actualizado

El dispositivo debe tener instalado y funcionando un software antimalware, de probada eficacia, que disponga de las últimas actualizaciones (motor, firmas) proporcionadas por el fabricante, para detectar y neutralizar amenazas antes de que puedan comprometer la sesión de acceso remoto.

Cifrado de almacenamiento

Garantizar que cualquier dato sensible en el dispositivo esté cifrado, protegiendo la información en caso de pérdida o robo del equipo.

Requerimientos en la infraestructura de red y seguridad del proveedor

Sistemas operativos actualizados y parcheados

la red interna del proveedor debería disponer de una segmentación en la que los puestos empleados para los accesos remotos a los clientes finales se encontraran aislados del resto de equipos de propósito más general, de forma que se disminuya la superficie de inicio de un ataque a los grupos de equipos del soporte técnico.

Configuración de firewall local, en función de la política de empresa

el firewall del proveedor, en caso de que la conexión se estableciera a través de una conexión VPN site-to-site, debe estar configurado de forma que limite el acceso a la rede del cliente únicamente a los puestos de los usuarios autorizados, y limitando el acceso únicamente a las aplicaciones y servicios necesarios para el soporte remoto.

6.1.5. *Consideraciones adicionales*

Las organizaciones deben garantizar que los servicios remotos cumplen con las normativas y buenas prácticas. Esto incluye:

- **Realizar evaluaciones periódicas de los procedimientos de acceso remoto.**
- **Exigir acuerdos de nivel de servicio (SLA) que incluyan responsabilidades de ciberseguridad para los proveedores.**
- **Mantener registros de auditoría que demuestren el cumplimiento continuo de las normativas.**
- **Formar y sensibilizar a todo el personal sobre las implicaciones legales y regulatorias de la ciberseguridad en servicios remotos.**
- **Implementar políticas de privacidad y protección de datos que sean compatibles con las normativas vigentes.**

6.2. ASISTENCIA IN SITU

La asistencia in-situ siempre ha sido y es una práctica común en la industria, donde **los proveedores realizan intervenciones presencialmente en las instalaciones del cliente.**

Estas intervenciones pueden incluir tareas de mantenimiento, soporte, implementación e instalación de hardware IT u OT, la configuración de sistemas, la resolución de problemas y la implementación de medidas de ciberseguridad, entre otras.

Por esto mismo, la presencia física de técnicos externos en las instalaciones del cliente introduce riesgos de ciberseguridad que deben ser gestionados adecuadamente. Es crucial establecer medidas de seguridad rigurosas para proteger los activos de la empresa durante estas intervenciones, evitando que se comprometa la ciberseguridad de la infraestructura de la planta o instalación.

A continuación, se detallan los puntos clave a considerar:

ADMISIBILIDAD DE EQUIPAMIENTO EXTERNO

Políticas de control de dispositivos externos

Es fundamental establecer políticas claras para la admisión y uso de dispositivos externos, como ordenadores portátiles, dispositivos USB, soportes de almacenamiento u otros equipos electrónicos. Deben establecerse restricciones sobre qué tipos de dispositivos se pueden utilizar y bajo qué condiciones.

A modo de guía:

- Requerir la autorización previa de cualquier dispositivo externo antes de su ingreso a las instalaciones.
- Antes de permitir la entrada de cualquier equipamiento externo, es fundamental realizar una inspección y autorización previa. Esto puede incluir la verificación de que los dispositivos están libres de malware y cumplen con las políticas de seguridad de la organización.
- Realizar auditorías regulares para asegurar el cumplimiento de estas políticas por parte de todo el personal y proveedores.

Inventariado y registro

Todos los dispositivos externos deberían ser registrados en un sistema centralizado que debería incluir:

- Identificación del dispositivo (modelo, número de serie).
- Identidad del propietario y motivo de uso.
- Fecha y hora de ingreso y salida.
- Estado de seguridad tras la verificación inicial (si pasa o no las pruebas de seguridad).
- Historial de uso dentro de las instalaciones, incluyendo qué sistemas o redes se conectaron, etc.

CONEXIÓN A REDES DE PLANTA

La conexión de dispositivos externos a las redes de planta puede ser una fuente de vulnerabilidades si no se gestiona adecuadamente. Cabe destacar que, en ocasiones, las intervenciones in-situ en entornos OT se realizan únicamente con el objeto de verificar visualmente que la intervención realizada por el personal técnico del proveedor funciona de acuerdo con lo esperado en la máquina, sistema, etc. Por lo tanto, antes de permitir la conexión de un dispositivo externo a redes corporativas, es necesario preguntarse si realmente es o no necesario, de forma que pueda sustituirse la conexión directa a la red de planta por un acceso a través de la conexión VPN corporativa (tal y como si se actuara desde una ubicación remota).

Las siguientes prácticas se estiman como recomendadas:

Segmentación de redes

Los dispositivos conectados in-situ deben estar restringidos a redes segmentadas que aíslen los sistemas críticos del resto de la infraestructura. Estas redes deben contar con controles estrictos de acceso.

Uso de puntos de conexión seguros

Las conexiones físicas deben realizarse exclusivamente a través de puntos de conexión designados como seguros, que estén equipados con firewalls locales y sistemas de detección de intrusiones. Podrían emplearse incluso microfirewalls en L2 entre la interfaz de red del ordenador del proveedor y la boca del switch o el elemento final accedido, con las correspondientes políticas IDS y virtual-patching.

Proporcionar acceso temporal y controlado a las redes de planta

Esto puede incluir el uso de credenciales de acceso temporales que expiran una vez completada la intervención.

Monitorización de actividades

Monitorizar en tiempo real las actividades de los dispositivos conectados a la red para detectar y responder rápidamente a cualquier comportamiento sospechoso.

Autenticación y autorización

implementar mecanismos de autenticación y autorización para asegurar que solo los dispositivos y usuarios autorizados puedan acceder a la red de la planta. Esto puede incluir el uso de certificados digitales y autenticación multifactor.

ZONAS DE CONEXIÓN SEGURA

Definición de zonas seguras

En las instalaciones, deben establecerse zonas de conexión seguras que estén físicamente delimitadas y supervisadas. Estas zonas deben cumplir con los siguientes requisitos:

- Acceso restringido al personal autorizado.
- Equipamiento de red dedicado exclusivamente para tareas de mantenimiento.
- Implantación de sistemas de monitorización y auditoría de las actividades realizadas en estas zonas.
- Segmentación de la red para aislar estas zonas del resto de la infraestructura, minimizando así el riesgo de propagación de amenazas.
- Definir o designar áreas específicas dentro de las instalaciones donde se permitan la conexión de dispositivos externos. Estas áreas deben estar equipadas con medidas de seguridad adicionales, como firewalls y sistemas de detección de intrusiones.
- Implementar controles de acceso físico para restringir el acceso a las zonas de conexión segura solo al personal autorizado.
- Establecer procedimientos claros para la conexión de dispositivos externos, incluyendo la verificación de identidad y la autorización previa.
- Redes seguras vs. redes de producción: la conexión directa a redes de producción debe ser evitada o, si fuera necesario, controlada estrictamente mediante interfaces de acceso seguras. La autenticación y autorización para acceder a estas redes deben ser rigurosas.
- Supervisión de actividades: cualquier actividad realizada en las zonas seguras debe ser supervisada, ya sea mediante monitorización en tiempo real o grabaciones para auditorías futuras.

6.3. GESTIÓN DE VULNERABILIDADES EN EL CICLO DE VIDA DE COMPONENTES, EQUIPOS Y DISPOSITIVOS

Una vulnerabilidad de ciberseguridad es una debilidad en el diseño o configuración de un componente (software, hardware) que puede ser explotada por un tercero para comprometer su seguridad.

La información sobre las vulnerabilidades de los sistemas de información y los equipos industriales es parcialmente accesible al público. En general, los fabricantes publican esta información después de haber desarrollado un parche o actualización que permite mitigar o corregir la vulnerabilidad identificada.

Organismos como **MITRE** identifican, asignan y publican las vulnerabilidades en la base de datos **CVE** para su referencia pública. **A modo de referencia, durante el 2024 se registró una media de 3400 nuevas vulnerabilidades al mes.**

Las vulnerabilidades afectan a prácticamente todo el ciclo de vida de los activos O, y abarca especialmente a la fase de diseño y desarrollo (donde puede que el fabricante no haya considerado todas las medidas de seguridad adecuadas para la protección del dispositivo –ciberseguridad desde el diseño-), la instalación/puesta en marcha, así como la operación y mantenimiento (O&M).

Si desestimamos las fases que generalmente se corresponden a los fabricantes, vamos a centrar este apartado sobre la gestión de las vulnerabilidades en las fases de instalación/puesta en marcha, así como en la fase de O&M.

Dado que la gestión de vulnerabilidades debe ser un proceso periódico, es necesario que las organizaciones definan su propio proceso de gestión de vulnerabilidades y parches, en el que se debe recoger, al menos:

PROCESO DE IDENTIFICACIÓN DE VULNERABILIDADES

Determinando claramente cuales son las fuentes que se emplearán para determinar si un activo es o no vulnerable: escaneos de vulnerabilidades, análisis de información de los boletines de seguridad de los fabricantes, feed de notificación de vulnerabilidades de organismos competentes en la materia, etc.

CRIBADO DE VULNERABILIDADES

en el que se determina el criterio por el cual una vulnerabilidad requiere o no de un análisis para determinar si es necesario (o no) llevar a cabo algún tipo de acción de remediación.

ESTABLECIMIENTO Y EJECUCIÓN DE MEDIDAS DE REMEDIACIÓN

para aquellos activos sobre los que se haya decidido actuar directamente (dado que la mitigación sobre el propio componente es factible sin impactos no asumibles por la organización) o bien con la puesta en marcha de medidas compensatorias (virtual-patching, por ejemplo).

A continuación, se realizan una serie de recomendaciones relacionadas con la gestión de vulnerabilidades y parches en las fases anteriormente mencionadas.

1. FASE DE INSTALACIÓN Y PUESTA EN MARCHA

De forma general, durante esta fase es necesario proceder con el inventariado de los activos, obteniendo la información necesaria para, entre otras cosas, poder determinar si presentan algún tipo de vulnerabilidad conocida, de forma que pueda aplicar el procedimiento establecido para la gestión de vulnerabilidades y parches antes de la entrada en producción.

En caso de que el activo fuera proporcionado dentro de los servicios contratados a un proveedor, el contrato del suministro debería contemplar que los activos deben encontrarse libre de vulnerabilidades en el momento del comissioning, aspecto que debe ser verificado por el personal técnico del cliente. El incumplimiento de este requisito en el suministro podría ser objeto de no aceptación de la entrega del suministro.

2. FASE DE OPERACIÓN Y MANTENIMIENTO (O&M)

La fase de O&M puede diferenciarse en tres periodos o casuísticas:

Periodo durante el cual el equipamiento suministrado se encuentra en periodo de garantía por parte del proveedor.

Debería plantearse, por contrato, la posibilidad de que sea el propio proveedor quien se encargue de la supervisión del equipamiento en materia de identificación de vulnerabilidades, debiendo realizar las tareas de notificación al cliente de la presencia de vulnerabilidades en el equipamiento instalado, así como de las acciones de remediación que sean oportunas.

Periodo post-garantía sin contrato de mantenimiento posterior.

La responsabilidad de la gestión de las vulnerabilidades durante este periodo de tiempo recae completamente en el cliente, debiendo asumir el ciclo de vida de la gestión de las vulnerabilidades de forma íntegra.

Periodo post-garantía con contrato de mantenimiento posterior con proveedor.

En la medida que sea factible, y el proveedor pueda o desee ofrecer este servicio, se recomienda incluir la gestión de vulnerabilidades en este tipo de contratos de mantenimiento.

6.4. EL CLIENTE CAUTIVO

A la hora de la puesta en marcha de una nueva iniciativa para la implantación o sustitución de componentes de automatización industrial, ya sea por fallo, fin de vida o nuevos requisitos, surge el proceso de selección de proveedores de entre el porfolio de la organización.

Ya en los últimos años ha cobrado especial relevancia la gestión de riesgos de terceros, y vemos con frecuencia su impacto en las noticias, se evidencia que la cadena de suministro es un vector de ataque cada vez más frecuentado como vía indirecta para atacar a un objetivo final.

Siempre es importante dedicar el tiempo necesario para tener un inventario actualizado tanto de activos reales como de proveedores, y sobre estos, un análisis de riesgos que nos permita conocer nuestra exposición a las distintas amenazas que pueden venir sobre él. Es muy posible que sin darse cuenta se haya caído en este riesgo, o si ya se conoce, ayudará a tener cuantificado el alcance del mismo.

Se pretende en este apartado invitar a la reflexión sobre la casuística que implica este proceso, los riesgos que aparecen, y comentar ideas que pueden ayudar a mitigar en cierta medida el riesgo anticipado en el título. Hablando del área industrial, uno de los mayores riesgos viene por la parte de ciclo de vida de la gestión de proveedores, y concretamente la dependencia que provoca tener un proveedor único, ya sea por concentración, o por actor de nicho para un determinado propósito.

Se puede establecer que una organización es cautiva de un proveedor en particular cuando no se conoce un proveedor alternativo, o, si se conoce, el coste del cambio es inasumible. Supongamos el siguiente ejemplo:

“Una empresa de distribución de agua o gas plantea un despliegue de cientos de miles de contadores inteligentes que comunicarán vía conectividad celular (tipo 2G/3G/NB-IoT), para lo cual estiman necesario una tarjeta sim de un operador de telefonía que irá instalada en cada contador desde fábrica. Se licita el contrato de conectividad, y se adjudica con condiciones muy ventajosas. Pasados unos años, el contrato acaba, y se vuelve a licitar, ahora el proveedor incumbente ya no es el más ventajoso desde el punto de vista técnico/económico, pero un cambio supondría ir físicamente a cien mil contadores y cambiar la SIM, que incluso puede requerir manipular el contador instalado, o directamente reemplazarlos, en ambos casos el caso de negocio no sale y el resultado es un “encadenamiento” al operador durante todo el ciclo de vida del contador.”

Afortunadamente ahora existen la eSIM que vienen a salvar la vida a este tipo de despliegues, y un análisis de riesgos para un proyecto así levantaría esa necesidad tecnológica para evitar un despliegue con SIM tradicionales. De esto se trata, el llevar acabo un análisis de riesgo/beneficio y del coste de la oportunidad, forma parte de la visión estratégica a largo plazo.

En el ejemplo expuesto y otras casuísticas también conviene evaluar más riesgos:

Riesgos en la operación: posibles fallos de suministro, ya sea por roturas de stock o de producción, como fue la crisis de los semiconductores.

Riesgos regulatorios: el proveedor está obligado a cumplir en materia de ciberseguridad, calidad, riesgos laborales, etc., pero la organización cliente está obligada a velar por su cumplimiento, al menos, con la diligencia debida.

Riesgos estratégicos: la dependencia de los procesos de negocio de la organización con los procesos del proveedor puede afectar muy negativamente.

Riesgos financieros: si el proveedor quiebra, cierra, impone cambio de precios, o sufre un ciberataque y detiene su producción, no debe implicar congelar las operaciones de la organización.

El cómo mitigar todos estos riesgos atiende a muchos factores, pero frecuentemente implica que la organización se mantenga al día del mercado conociendo nuevos proveedores, e igualmente mantener un dialogo frecuente con los existentes para anticipar y gestionar posibles problemas, pudiendo llegar a diseñar y contar con un plan de continuidad más completo.

Por supuesto se puede encontrar el caso de que no sea posible, ya por la especificidad del proceso o cualquier otro motivo, en esos casos solo queda conocer el riesgo, su posible impacto, y aceptarlo, o mejor aún, buscar una alternativa más respaldada que mitigue el riesgo y su impacto, aunque suponga cambiar el proceso.

Siempre es mejor **acometer un proyecto de forma ordenada y controlada para adoptar una tecnología sustitutiva que ofrezca mejores garantías o menores riesgos,** que esperar a que nunca se materialice la amenaza. Las palabras nunca y siempre no existen en el diccionario del CISO.

6.5. GESTIÓN DE CIBERINCIDENTES

Hasta hace no mucho existía la creencia de que las tecnologías de operación estaban libres de incidentes de ciberseguridad, siendo esta una problemática específica de las redes IT de las compañías. El creciente número de incidentes ha cambiado paulatinamente esta visión y no se estima que la tendencia creciente vaya a cambiar en los próximos años.

Desde este punto de vista, la respuesta a ciberincidentes y la ciber resiliencia se convierten en un aspecto clave de la operación de las compañías, también en su componenteOTyrequiriendo un enfoque especializado debido a la naturaleza única de este tipo de entornos .

1.

LA PREPARACIÓN

Como en cualquier incidente de seguridad, la capacidad de respuesta está relacionada en buena medida por la preparación previa que la organización haya llevado a cabo. Las acciones típicas de preparación aplican también a los entornos OT con ciertos condicionantes:

Procedimientos

La respuesta a incidentes debe estar procedimentada (en lo que se denominan PRI –Procedimientos de Respuesta frente a Incidentes-) y preparada de antemano, de modo que, en caso de materialización de un incidente, todos los equipos conozcan la manera de proceder. A diferencia de los entornos TI, las redes de operación en muchas ocasiones no están operadas por los equipos II, o al menos no en su totalidad, lo que implica que los procedimientos deben contar con la participación de equipos específicos como pueden ser los ingenieros de control, operadores de planta o equipos de mantenimiento o instrumentación, que típicamente tienen la responsabilidad de la operación y mantenimiento, copias de seguridad y pruebas de los sistemas OT.

Los equipos de respuesta a incidentes, típicamente liderados por ciberseguridad deberán, en consecuencia, tener identificado el personal de operación necesario para gestionar la respuesta de manera adecuada, así como sus atribuciones. De la misma manera, el personal de operaciones debe tener identificados los contactos del equipo de respuesta para notificar cualquier comportamiento anómalo que detecten en su operativa diaria.

Ejercicios de escritorio

Realizar de manera periódica ejercicios de escritorio en los que participen tanto equipos de ciberseguridad y sistemas de información, como los equipos de operación y sus responsables, es fundamental para probar teóricamente los PRI existentes y generar la necesaria relación de coordinación y confianza entre los equipos que propicie la adecuada comunicación y respuesta en caso de incidente real. Adicionalmente estos ejercicios proporcionan fuente de información para ajustar los PRI en base al análisis de las lecciones aprendidas que emanan de los mismos.

Pruebas de aislamiento o de funcionamiento en isla

Los sistemas de operación requieren la máxima disponibilidad y, por tanto, y en la medida de las posibilidades que ofrece la orientación tecnológica estratégica que se haya establecido en la organización, en general deben ser capaces de cumplir su función con independencia de los sistemas IT. La creciente y necesaria conectividad entre ambos entornos, puede llegar a poner en entredicho este principio. Una manera de asegurarlo es realizar pruebas periódicas de funcionamiento en isla, cortando las conexiones entre ambas redes de manera análoga a como típicamente se haría en caso de un incidente, e identificando dependencias existentes entre los procesos de operación y las redes.

EL INCIDENTE

Una vez se detecta un incidente, los canales de comunicación previamente definidos y ensayados de acuerdo a los PRI, deben funcionar de manera eficiente y coordinada para poder ofrecer una respuesta que contenga y resuelva el incidente.

Identificación

La compañía puede identificar un incidente por diferentes medios, que van desde la aparición de alertas en herramientas de monitorización, a un malfuncionamiento o secuestro de procesos industriales. Los ejercicios y documentación de las fases preparatorias deben proporcionar a los equipos la habilidad para una comunicación rápida entre los equipos de operación (ingenieros de control, operadores de planta, equipos de mantenimiento o instrumentación, etc.) y el equipo de ciberseguridad en caso de que sea el primero el que detecte el incidente, o en sentido inverso en caso de que el incidente lo detecte el segundo. En cualquier caso, esta comunicación debe prevenir toma de decisiones precipitadas que vayan en contra de los pasos básicos de la gestión de incidentes.

Gestión del incidente

Una vez se confirma la veracidad del incidente, los procedimientos deben facilitar al menos la existencia de dos tipos de foros con equipos multidisciplinares:

Equipo técnico. Conformado por especialistas de operación que conocen tanto el equipamiento de operación como el impacto del incidente en los procesos, equipo de IT que puede colaborar en acciones de contención e investigación, y el equipo de ciberseguridad que se encartará de liderar la respuesta.

Equipo directivo y de gestión. Conformado por directivos y gerentes de las unidades técnicas y de negocio anteriores a los que se suman otras unidades como servicios jurídicos, comunicación o recursos humanos, y donde se toman decisiones estratégicas en el ámbito de comunicación a empleados y terceras partes (regulador, clientes, medios, etc.), continuidad de negocio o contacto con el atacante. Este foro tomará las decisiones basadas en la información que vaya recibiendo de manera periódica por parte del equipo técnico.

2.

DESPUÉS DEL INCIDENTE

Una vez mitigado el incidente, debe ser documentado de manera precisa de forma que puedan identificarse lecciones aprendidas en varios ámbitos para las partes implicadas. En un incidente con impacto en redes de operación típicamente pueden identificarse acciones de diferente índole:

Comunicación e interlocución.

Identificación de equipos con responsabilidad en la respuesta y que no estuvieran identificados en los PRI.

Monitorización

Identificación de la necesidad de implementar medidas adicionales para identificar intrusiones (activación de IPS o monitorización de redes hasta ese momento no monitorizadas).

Dependencia de procesos

Los procesos de operación deben ser capaces de funcionar de manera aislada de la red IT. En casos de incidentes IT, existen ocasiones donde al activar acciones de aislamiento o por el impacto del propio incidente, se identifican impactos en los procesos de operación que en principio no eran esperadas.

Continuidad de negocio

El incidente puede ayudar a identificar impactos que no fueran conocidos previamente y que puedan aparecer en caso de incidentes de ciberseguridad, así como mejoras en la continuidad de las operaciones como pueden ser la necesidad de redundancias adicionales o procesos alternativos

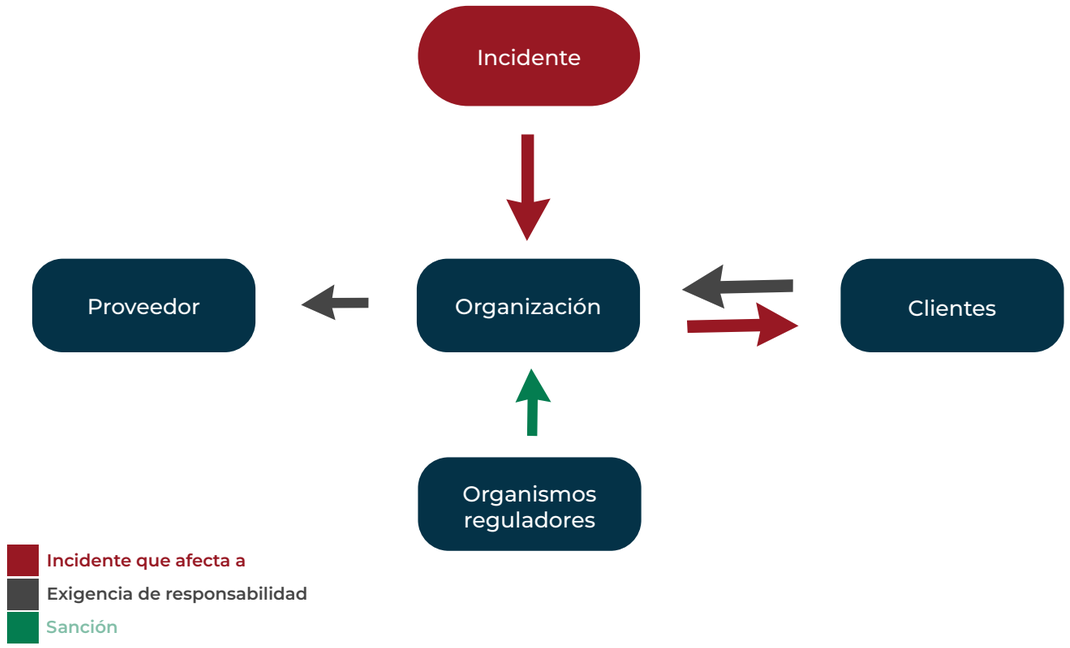
Existencia e integridad de las copias de seguridad

Identificación de mejoras en la gestión de copias desde el punto de vista de disponibilidad o completitud.

3.

6.6. RESPONSABILIDADES LEGALES EN CASO DE OCURRENCIA DE UN CIBERINCIDENTE

La legislación vigente en materia de ciberseguridad (ver epígrafe 3.2) contempla obligaciones específicas para las organizaciones cuyo incumplimiento puede suponer sanciones económicas de gran calado. Algunas de las obligaciones establecidas en la normativa, están asociadas al control y exigencia de medidas de seguridad a la cadena de suministro. En consecuencia, la exigencia de responsabilidades cobra especial relevancia en los supuestos en los que la organización está sujeta a legislación específica que establezca requisitos de ciberseguridad tanto a la propia organización, como a sus proveedores; debido a que un fallo por parte de su cadena de suministro, puede conllevar que la propia organización incurra en responsabilidades legales (sanciones administrativas) por parte de organismos reguladores, de manera adicional a las responsabilidades en las que pueda incurrir con sus propios clientes.



En el supuesto de que un proveedor sufra un ciberataque que afecte a la seguridad de la información de la organización, se deben valorar las posibles responsabilidades legales exigibles a este.

En primer lugar, es necesario realizar un análisis de las obligaciones contractuales asumidas por el proveedor con la organización. Como se ha descrito en el epígrafe precedente, es necesario que el contrato entre la organización y sus proveedores establezcan obligaciones relacionadas con la ciberseguridad, así como cláusulas específicas de responsabilidad, donde el proveedor se comprometa a resarcir los daños y perjuicios que pudiera sufrir su cliente como consecuencia de un incumplimiento contractual, incluidos incumplimientos relacionados con las obligaciones de implantación de medidas de seguridad adecuadas.

En este escenario, **la organización deberá valorar los daños y perjuicios sufridos con motivo del ciberataque que ha sucedido en su cadena de suministro.** Si no existe un daño cuantificable y evidenciable, difícilmente se podrán exigir responsabilidades al proveedor que ha sufrido el incidente de seguridad.

En el ámbito industrial los daños más relevantes normalmente se encuentran relacionados con el quebranto de la disponibilidad o la integridad de los datos o de la operación, pero igualmente puede causar un daño a la organización un incidente en su cadena de suministro que afecte a la confidencialidad, trazabilidad o autenticidad, entre otros.

De manera independiente a lo que disponga el contrato, **se debe tener presente que el Código Civil español establece que quedarán sujetos a indemnización los daños y perjuicios causados por quienes incumplan sus obligaciones, ya sea por dolo o negligencia;** debiendo entenderse dolo como una acción realizada con conocimiento de que esta supone un incumplimiento, y negligencia como un incumplimiento no realizado con conocimiento, pero que la acción realizada u omisión no cumple con lo que se debe esperar en una situación determinada (en este ámbito, no ser diligente en la implantación de medidas de seguridad).

Por otro lado, además de las responsabilidades económicas que puedan ser exigidas al proveedor por los daños y perjuicios causados a la organización con motivo de un incumplimiento, será necesario evaluar la idoneidad del propio proveedor para seguir prestando servicios a la organización. La normativa vigente exige que las organizaciones deben contar con proveedores que aseguren la implantación de medidas de seguridad adecuadas. La seguridad 100% no existe, por lo que todas las empresas están expuestas a sufrir un ciberataque; no obstante, sí que se debe poder acreditar que los proveedores seleccionados son diligentes en materia de seguridad de la información. En consecuencia, es necesario evaluar la gravedad del incidente y las medidas de seguridad implantadas por el proveedor, con la finalidad de tomar la decisión de continuar la relación contractual con este, o rescindir el contrato, con motivo de tales incumplimientos.

Finalmente, en relación con las posibles sanciones que un organismo regulador podría imponer a la organización por incumplimiento de sus obligaciones, es importante resaltar que la legislación vigente, así como la que está prevista aprobar en los próximos meses, establecen sanciones máximas muy elevadas. Como más relevantes se indican las siguientes:

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (norma de transposición Directiva NIS)

Hasta 1 millón de euros y la posibilidad de que la sanción sea publicada en el Boletín Oficial del Estado. Se espera que las sanciones previstas en la norma que transponga la Directiva NIS 2 sean más elevadas, con la finalidad de alinearlas a los límites sancionadores previstos en otras normas similares.

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA)

Actualmente DORA establece que las sanciones por incumplimiento pueden variar en función de su gravedad y cuantía. No obstante, indica expresamente que deben ser efectivas, proporcionales y disuasorias.

Reglamento (UE) 2016/679 General de Protección de Datos (RGPD)

Hasta 20 millones de euros hasta el 4% del volumen de negocio total anual.

Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (Ley 5G)

Hasta 20 millones de euros.

Propuesta de Reglamento de ciberresiliencia de la UE (CRA)

Hasta 15 millones de euros o hasta el 2,5% del volumen de negocio total anual (a la espera de conocer el texto definitivo).

En conclusión, las responsabilidades legales por incumplimiento de obligaciones contractuales y legales en materia de ciberseguridad pueden ser muy variadas e incluir a diferentes actores. Por lo tanto, es de vital importancia la realización de un análisis de la idoneidad de los proveedores involucrados en la cadena de suministro no solo desde el punto de vista operativo, sino también desde el punto de vista de cumplimiento en el ámbito de la ciberseguridad.

6.7. MONITORIZACIÓN DEL RIESGO EN LA CADENA DE SUMINISTRO

No cabe duda de que el riesgo es un factor variable, siempre sujeto al cambio de las circunstancias o factores que influyen en su cuantificación.

Por lo tanto, y en aras de mantener un control continuo del nivel de riesgo que presentan nuestros proveedores a lo largo de tiempo, es necesario establecer un sistema de supervisión o monitorización del riesgo en la cadena de suministro. Para ello se pueden definir diferentes actividades:

La evaluación periódica del riesgo, en base a una pauta de revisión basada en el cumplimiento de un periodo de tiempo preestablecido (asimilable a una “fecha de caducidad”), de acuerdo con lo determinado en el procedimiento de evaluación de proveedores que hayamos definido.

La activación del procedimiento de reevaluación en base a la materialización de eventos empresariales que puedan afectar a la gestión de la infraestructura del proveedor que se emplea para ofrecernos sus servicios. Un ejemplo podría ser la integración de los servicios del proveedor, tras un proceso de adquisición de la empresa, en la organización o empresa compradora.

Situaciones financieras adversas, que pudieran afectar al mantenimiento adecuado de los medios para la prestación segura de los bienes o servicios contratados.

La materialización de algún incidente de ciberseguridad en otros servicios o áreas del proveedor distintos a los contratados.

La existencia de alguna brecha o incidente de ciberseguridad en empresas que pudieran pertenecer al mismo grupo empresarial de la empresa proveedora, considerando posibles vías de comunicación digitales de información que pudieran encontrarse establecidas entre las diferentes empresas del grupo, y que pudieran facilitar movimientos laterales en una intrusión.

En este sentido, y considerando la diferente casuística de las circunstancias relacionadas con anterioridad, será necesario establecer procesos de monitorización adecuados, que podrán basarse en el empleo de la información relevante de forma manual o bien mediante la obtención y/o evaluación automatizada de aspectos de ciberseguridad relevantes, mediante el uso y explotación de herramientas especializadas.

Lo cierto es que la obtención manual de toda la información anterior puede resultar una tarea tediosa que requiera una importante dedicación de recursos, probablemente no sea necesario llevarla a cabo en determinados niveles de criticidad asignados a los proveedores. Sin embargo, y para aquellos quizás más críticos, es probablemente en uso de herramientas que simplifiquen la fase de obtención de información la opción más adecuada. Dentro del conjunto de herramientas que permiten la monitorización de forma automatizada, se podría destacar: continuo del nivel de riesgo que presentan nuestros proveedores a lo largo de tiempo, es necesario establecer un sistema de supervisión o monitorización del riesgo en la cadena de suministro. Para ello se pueden definir diferentes actividades:

1.

Herramientas de "rating" focalizadas en los aspectos empresariales, y que permiten calificar el riesgo de las empresas monitorizadas de forma que se puedan activar las acciones oportunas de reevaluación de riesgos en materia de ciberseguridad.

2.

Herramientas de inteligencia de ciberamenazas que permiten obtener información que pudiera encontrarse presente en la dark-web o similares (foros, mensajes, web, contenidos/ficheros publicados, etc.) en relación con nuestros proveedores, activando alarmas en caso de identificar actividad que pueda dar indicios de la existencia o probabilidad de materialización de un ciberincidente.

3.

Herramientas que evalúan de forma continua la ciberseguridad presente en la infraestructura tecnológica del proveedor, identificando posibles brechas de seguridad que pueden ser empleadas para llevar a cabo un ataque por parte de un tercero malicioso.

07.

CONCLUSIONES

La gestión eficaz de la ciberseguridad en la cadena de suministro industrial representa una prioridad ineludible para las empresas modernas, debido al alto nivel de riesgo asociado a los proveedores y terceras partes involucradas. Los incidentes de ciberseguridad que surgen en proveedores conectados directamente a las redes empresariales o que gestionan información sensible, pueden derivar en consecuencias operativas graves, pérdidas financieras significativas y daños reputacionales difíciles de revertir. Así lo identifican las empresas y las distintas regulaciones que exijan a estas que sea uno de sus focos de control.

Se ha identificado que un porcentaje considerable de organizaciones ha sufrido ataques o incidentes derivados de vulnerabilidades en su cadena de suministro.

Por ello, resulta imprescindible establecer requisitos claros y exigentes hacia los proveedores en términos de ciberseguridad, incluyendo medidas preventivas, certificaciones exigibles y auditorías periódicas. En este contexto, la Directiva NIS 2 y otras normativas como el RGPD y ENS, aportan un marco legal robusto que respalda la necesidad de una gestión cuidadosa y proactiva de estos riesgos.

La implementación de los análisis de riesgos en los encargos y durante todo el ciclo de vida del producto o servicio contratado, y consecuentemente la "ciberseguridad por diseño" (Security by Design) desde las primeras etapas del desarrollo de productos o servicios industriales se revela como una estrategia clave para reducir vulnerabilidades futuras. La adopción de metodologías como el ciclo de vida de desarrollo seguro (SDLC) permite integrar controles efectivos en cada fase del desarrollo, minimizando el impacto y los costos asociados a incidentes posteriores.

Además, **las fases de puesta en marcha (commissioning) y operación-mantenimiento (O&M) presentan puntos críticos en los que la evaluación y validación de la seguridad, a través de pruebas FAT (Factory Acceptance Test) y SAT (Site Acceptance Test),** resultan fundamentales para garantizar la resiliencia de los sistemas implementados. La exigencia de un punto de contacto de ciberseguridad, documentación exhaustiva, códigos fuente, mapas de redes y licencias adecuadas, así como procedimientos detallados que incluyan, por ejemplo, qué, cuando, a quién y cómo informar de incidentes de ciberseguridad que puedan impactar en el cliente, constituyen parte de la práctica esencial para mantener el control sobre los activos digitales y físicos de la empresa.

Por último, **la implementación efectiva de controles específicos para servicios remotos,** como canales seguros de conexión, registros de trazabilidad, autenticación multifactor, gestión estricta de accesos y formación continua en ciberseguridad, complementan un marco integral que reduce la superficie de ataque y asegura la continuidad operativa.

En conclusión, **las organizaciones deben abordar la gestión de ciberseguridad en sus cadenas de suministro con rigor, respaldándose en marcos legales y metodologías probadas,** estableciendo relaciones claras y exigentes, que incluyan acuerdos contractuales y mecanismos de monitorización y supervisión, con proveedores y terceros, y fomentando una cultura organizacional orientada a la prevención y mitigación de riesgos.

08.

REFERENCIAS

Agencia Española de Protección de Datos. (s.f.). *Esquema Nacional de Seguridad (ENS)*. CNI. https://ens.cni.es
Comisión Europea. (2019). *Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre ENISA y la certificación de ciberseguridad de las TIC*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80998
Comisión Europea. (2022). *Directiva (UE) 2022/2555 (NIS2) del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963
ENISA. (2021). *Good practices for supply chain cybersecurity*. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
ENISA. (2022). *Threat landscape for supply chain attacks*. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
ENISA. (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security management systems*. *https://www.iso.org/standard/27001*
International Society of Automation. (s.f.). *ISA/IEC 62443 Series of Standards*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
ISMS Forum. (2023). *Guía de ciberseguridad en entornos industriales*. https://www.ismsforum.es/ficheros/descargas/guia-entornos-industriales-20231686772410.pdf
Leet Security. (2023). *IV Estudio de ciberseguridad en las empresas españolas*. https://www.leetsecurity.com/es/documentacion/iv-estudio-empresas-ciberseguridad/dl/
SecurityScorecard. (2024). *The Cyber Resilience of the Global 2000*. https://securityscorecard.com/wp-content/uploads/2024/08/FINAL-SSC-Global-2000.pdf
TISAX. (s.f.). *TISAX Participant Handbook*. ENX. https://enx.com/tisax/
VDA. (s.f.). *Information security – VDA ISA*. https://vda.de/en/services/standards/information-security

Síguenos:

Email:
info@ismsforum.es

Website:
www.ismsforum.es

Teléfono:
(+34) 636 69 13 92