MODELO DE CUESTIONARIO UNIFICADO PARA EL CONTROL DE LA CADENA DE SUMINISTRO

CCN-CERT
centro criptológico nacional

isms forum

CSC
CYBER SECURITY CENTRE

AUTORES

Franciso Lázaro
Mariano J. Benito
Pablo Blanco
Ángel Camacho
Francisco Esteban
Amelia Torres
Carlos López
José Ramón Monleón
Javier Calahorra
Víctor Manuel Ruiz
Firas Atassi
Antonio García

CONTACTA CON NOSOTROS

Si estás interesado/a en colaborar con nosotros o necesitas más información sobre nuestros proyectos, escríbenos a:
proyectos@ismsforum.es

isms forum

Contexto

En la actualidad tenemos ya un conjunto de Reglamentos y Directivas Europeas, así como leyes Nacionales que establecen obligaciones a los sujetos obligados en relación con la gestión del nivel de ciberseguridad de su cadena de suministro (proveedores); cuando estos proporcionan, un servicio, proyecto o producto en relación con la información digital y con los sistemas y redes que la tratan (ya sea como objeto principal o como parte del objeto contratado).

En ese campo legislativo destaca el Esquema Nacional de Seguridad (controles op.ext, exigible a administraciones públicas) y RGPD (como encargados del tratamiento) y recientemente y de una forma más exigente en DORA, NIS2, o CRA. Todas ellas obligan de forma directa a llevar a cabo este control de nuestros proveedores y también, ya sea por voluntad propia o como consecuencia de tener un sistema de gestión de la seguridad de la información como la Norma ISO27001:2022 (5.19 a 5.23).

La supervisión de la ciberseguridad de la cadena de suministro es una necesidad empresarial inexcusable, dado que hay que entender la ciberseguridad y por tanto, el sistema de gestión de riesgos en esta materia, como una cadena, en la que el eslabón más débil es el que establece el grado máximo de la fortaleza de la misma.

¿Cómo se puede gestionar la cadena de suministro?

Para una eficaz gestión de la cadena de suministro se pueden llevar a cabo las siguientes actividades/acciones, ordenadas de la más básica a la que requiere un mayor esfuerzo por parte de las organizaciones:

- Dar por válido el compromiso tácito del proveedor con los requisitos de seguridad establecidos en las especificaciones técnicas y, en todo caso con reuniones periódicas.
- Identificar el nivel de ciberseguridad del proveedor (que no específicamente de lo contratado) a través de la monitorización con herramientas de Rating de Ciberseguridad.
- Conocer, analizar y verificar, del estado de ciberseguridad del proveedor a través de la exigencia de cumplimentación por parte de este, de Declaraciones Responsables sobre aspectos concretos involucrados en la ciberseguridad de lo contratado.
- La monitorización activa sobre los sistemas y servicios de los que haga uso el proveedor.
- Monitorizar el estado de ciberseguridad de un proveedor mediante la exigencia de la presentación de resultados de auditorías.
- Realizar Auditorías, con medios propios o de terceros contratados a tal fin, del proveedor, para el alcance contratado.

  Se puede utilizar, y es lo deseable, una combinación de las acciones anteriores, o alguna de ellas.

Iniciativa “Cuestionario cadena de suministro”

Lo que en principio menos trabajo exige, y seamos sinceros, en muchísimos casos se hace es: no conocer, evaluar ni verificar, los controles con los que se está suministrado lo contratado. Para combatir esa situación, con un esfuerzo moderado, es por lo que de entre las anteriores acciones que podemos llevar a cabo para supervisar no a uno, sino el conjunto de proveedores es a través de los formularios en los que se pide una declaración responsable de cómo se está proporcionando la ciberseguridad asociada al contrato.

Adicionalmente hemos de señalar que, en relación con las Declaraciones Responsables, y dado que en muchos casos la empresa cliente es, a su vez, proveedor de otras empresas, la asociación de profesionales y empresas del sector de la Ciberseguridad ISMS Forum, ha identificado la necesidad de minimizar la heterogeneidad de los modelos de Declaración Responsable que circularon entre las empresas, cuando, poco a poco, se vaya haciendo más habitual la gestión de la cadena de suministro.

ISMS Forum, a través del Grupo de trabajo de la cadena de suministro, busca confeccionar un modelo de referencia de Declaración Responsable con el que reducir la carga de trabajo de quien tiene que solicitar y cumplimentar dicho documento, así como quién debe evaluar las respuestas.

El Grupo de trabajo ha identificado un conjunto de preguntas o cuestiones esenciales que deben ser respondidas por el proveedor.

Este modelo podría incorporar más o menos cuestiones, pero se ha buscado el consenso entre expertos que han participado, incorporado, por un lado, un mínimo de preguntas que nos permitan satisfacer un conocimiento básico, y por otro lado un máximo de preguntas que razonablemente deben ser contestadas para alcanzar un conocimiento más concreto.

Este trabajo nace con el convencimiento de que se deberá ir adaptando a lo largo del tiempo, conforme a nuevas necesidades o contextos legales.

Por todo ello, queremos conocer la opinión de las autoridades de control y en la medida de lo posible con sus comentarios. Nuestra máxima aspiración es contar no solo con el apoyo institucional, sino incluso con su refrendo para que sea o bien una buena práctica o incluso un modelo obligado de control.

FRANCISCO LÁZARO ANGUIS

Co-Coordinador del Grupo de trabajo.

DESCARGA EL FORMULARIO