AEINSE G31/23
Toma de Datos para Proyectos de Sistemas de Seguridad

FEBRERO 2023

Índice

Autores:

Pedro Carpintero Pérez
Domingo Martínez Lacal

Revisores:

Carlos Martínez Hernández
Alfonso Bilbao Iglesias

1 Introducción

La toma de datos es el inicio de la relación con el cliente desde el punto de vista operativo. Será uno de los puntos más importantes del proyecto para conocer qué desea conseguir el cliente con el Sistema de Seguridad, qué le lleva a contratar los servicios de seguridad, el cumplimiento de la legislación, riesgos, amenazas, etc.

En esta etapa es muy importante la discreción y generar confianza en el cliente, ya que se tendrá acceso a amplia información referente al negocio del cliente, bienes patrimoniales, vida personal, etc. Por ello es recomendable la creación en este momento de un documento de confidencialidad que obligue a la empresa de seguridad a custodiar y no facilitar información de los datos del cliente. Así mismo se puede pedir al cliente que no haga uso de los datos del proyecto de seguridad a terceros

2 Objetivo

Los principales objetivos de la Toma de Datos son:

- Identificar los tipos de riesgo y el nivel de estos que afectan a las personas y bienes que se quieren proteger, para lo que se debe tener en consideración los conocidos por el cliente, los tipificados en las metodologías de análisis de riesgo y los aportados por nuestra experiencia.
- Identificar los escenarios a proteger.
- Disponer de la información que permita definir los medios físicos y organizativos de protección adecuados en cada caso.

La toma de datos será primordial para:

- Elaborar el análisis de riesgos.
- Conocer las necesidades del cliente.
- Realizar mediciones de las nuevas instalaciones.
- Conocer el alcance de infraestructuras existentes. Suministro e instalaciones eléctricas, redes de comunicaciones, etc.
- Considerar posibles ampliaciones.
- Clasificar el personal que accede a la empresa, horarios, contratas, etc.
- Necesidades de PRL para la instalación que se vaya a realizar.
- Etc.

3 Toma de datos

Para recopilar la información necesaria será conveniente tener un interlocutor dentro de la organización que sirva de enlace al ingeniero con los diferentes departamentos dentro de la empresa.

Los departamentos con los que será necesario relacionarse serán:

- Mantenimiento. Será útil para conocer las infraestructuras eléctricas, de datos y de canalizaciones existentes.
- Riesgos Laborales. Se deberá coordinar con ellos los trabajos que se vayan a realizar.
- IT. Las redes de datos para seguridad deberían ser independientes a las de la organización, si bien, en ocasiones, será necesario utilizar redes propiedad del cliente como VPN, enlaces WiFi, etc. Por estos motivos y con el fin de gestionar las necesidades de ciberseguridad se habrá de coordinar con el departamento de IT la seguridad informática del sistema.
- Recursos Humanos. Este será necesario si proponemos implantar un sistema de control de accesos.
- Departamento de seguridad, propio o externo

Pueden verse involucrados otros departamentos, pero esto dependerá del alcance del proyecto.

Los datos a recopilar se refieren en los apartados siguientes

3.1 Datos sobre la empresa:

Esta información es necesaria para entender el negocio del cliente, sus puntos críticos, la transcendencia de los incidentes y su repercusión. Los principales puntos a conocer son:

- Actividad de la empresa.
- Operativa de negocio. Producción.
- Áreas críticas (unidades de producción, almacenes, etc.).
- Histórico de incidentes.
- Repercusión a terceros por discontinuidad del negocio o denegación de servicio.

3.2 Datos sobre la situación del activo a proteger.

Se tendrán en consideración diferentes aspectos del entorno en el que se encuentra, aspectos diversos como el entorno social, comunicaciones, etc. Estos puntos para analizar y tener en cuenta son:

- Ubicación del activo que se vaya a proteger. Puede ser una empresa con un perímetro y diferentes edificaciones en su interior, una zona específica, un edificio, una vivienda, etc.
- Entorno en el que se encuentra. Urbano, industrial, residencial, etc.
- Climatología de la zona y orografía.
- Vecinos y tipo de actividad que realizan.
- Situación proximidad de las Fuerzas y Cuerpos de Seguridad, con el fin de conocer tiempos de respuestas estimados.
- Accesos y uso de estos.

3.3 Datos sobre infraestructuras.

Puesto que se habrá que realizar la instalación de un sistema se deberá conocer el estado en el que se encuentran las infraestructuras existentes, por si fuese necesario reforzar o modificar alguna de ellas. Estas infraestructuras son:

- Electricidad, agua, comunicaciones, etc.
- Infraestructura de canalizaciones.
- Iluminación.
- Red informática.
- Aparcamientos.

3.4 Interdependencias

Se recogerán aquí los suministros que, en caso de fallar, pondrían en peligro el negocio del cliente, con el objetivo de diseñar las salvaguardas que puedan ser necesarias

- Empresas suministradoras de energía eléctrica, gas, agua, comunicaciones, etc.
- Empresa instaladoras y mantenedora de seguridad si procede

3.5 Datos sobre el personal.

Otro aspecto a tener en consideración es el de los recursos humanos y los horarios de actividad. Ya que esto afectará, sobre todo, a la operativa y gestión del sistema. Si se está diseñando un sistema de control de accesos, esta información será fundamental.

La información a recopilar será la siguiente:

- Horarios de actividad, turnos, etc.
- Trabajadores propios, temporales, subcontratas, limpieza, etc.
- Acceso del personal, a pie, en vehículo, etc.
- Entrada salida de mercancías y suministros.
- Vigilantes de seguridad.

3.6 Organización y Procedimientos

Esta información nos permitirá conocer el grado de madurez de la seguridad dentro de organización e incorporar en el proyecto los procedimientos necesarios. Se obtendrá información sobre:

- Organigrama de seguridad física de la empresa
- Procedimientos operativos de seguridad

3.7 Requisitos de PRL

Información a considerar que puede tener repercusión en los costos de instalación y mantenimiento de los sistemas

- Plan de autoprotección

3.8 Plazos estimados.

Será necesario consensuar con el cliente plazos estimados de entrega y ejecución de las diferentes fases del proyecto.

Esto permitirá que el cliente disponga de una planificación y pueda realizar cambios en su sistema productivo en caso de verse afectados por las obras. Por otra parte, permite dimensionar con mayor precisión los recursos, humanos y materiales, para cumplir los plazos que se acuerden.

4 Otros documentos de aplicación

- Guía AEINSE 10/21. Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física.
- Guía AEINSE 30/23. Guía del proceso de proyectar e instalar un Sistema de Seguridad.