AEINSE E21/23. Materias formativas de los Ingenieros de Seguridad

ENERO 2023

Contenido

Introducción

El presente estudio, realizado por el Grupo de Trabajo de Formación de AEINSE, constituido por miembros voluntarios de la Asociación, es una continuación obligada del anteriormente publicado “AEINSE E20/22. Necesidades formativas de los Ingenieros de Seguridad”.

En aquel primer documento se intentó concretar una definición de lo que se entiende como Ingeniero de Seguridad en AEINSE, las funciones que realiza (variadas), los tipos de actividad en los que se desempeña (también variados) y, finalmente se enumeraron una serie de áreas de conocimiento que deberían ser adquiridas por los Ingenieros de Seguridad

En este estudio se pretende dar continuidad a lo expuesto en el anterior, profundizando en la definición de las materias que han de constituir el conjunto de los teóricos estudios del Ingeniero de Seguridad.

Una de las aplicaciones de este trabajo puede ser de servir de guía para un teórico desarrollo de estudios de posgrado para ingenieros o graduados en ciencias tecnológicas para su especialización como Ingenieros de Seguridad.

Redacción:

- Ballesteros Ballesteros, Iván
- Bilbao Iglesias, Alfonso
- García Palermo, Gabriel
- González Blázquez, Alfonso
- Hernández de la Encina, Juan José
- Herrero Prieto, Gabriel
- Sanz Ortega, Inmaculada

Revisión:

- Martínez Hernández, Carlos

---

1 Áreas de conocimiento

Conviene recordar las llamadas Áreas de Conocimiento del Ingeniero de Seguridad recogidas en el documento AEINSE E20/22, y que se desarrollan mediante las materias que las constituyen:

- Gestión del Riesgo
- Legal
- Normativa Técnica
- Proyectos
- Controles Técnicos
- Infraestructuras Físicas
- Infraestructuras Lógicas

En los apartados siguientes se exponen las materias a considerar para cada Área de Conocimiento.

Una definición de estas Áreas se puede consultar en el citado documento AEINSE E20/22.

2 Materias del Área de Gestión del Riesgo.

2.1 Introducción a la gestión del riesgo

Es necesario que la actividad de los ingenieros de seguridad sobre los controles o medidas de Seguridad sea coherente con los riesgos a mitigar, y en particular, con el factor de riesgo que se propone reducir al aplicar la medida.

Se espera que el ingeniero tenga alguna experiencia en la justificación de controles o medidas, o aplicación de medidas a partir de un estándar, o uso de alguna metodología de evaluación de riesgos básica, o cualquier experiencia que le haya sugerido cuestionar el ¿por qué es necesario proteger una instalación?

Las decisiones de los controles y su diseño se realizan dentro del proceso de gestión del riesgo. En esta introducción se propone que el ingeniero desarrolle competencias generales en el proceso de gestión de riesgos basado en la norma ISO31000, haga suyo el proceso, y lo pueda aplicar.

La evaluación de las competencias adquiridas debe demostrar que conoce y domina el proceso de gestión del riesgo indicado en la ISO 31000. En los próximos capítulos, adquirirá competencias específicas para cada fase del proceso.

2.2 Cultura del riesgo en la empresa y su organización.

La gestión del riesgo de la seguridad debe ser coherente con la gestión de riesgos de la empresa. Las empresas cotizadas en bolsa publican información, a muy alto nivel, sobre el sistema de gestión de riesgo. Las empresas de menor tamaño no siempre disponen de información sobre su sistema de gestión del riesgo.

Entender la cultura del riesgo de las empresas facilita al ingeniero a proponer niveles del apetito y la tolerancia para que la gestión del riesgo de la seguridad sea coherente a la organización.

La gestión del riesgo de seguridad se realiza a distintos niveles de la empresa, y los controles son más eficientes en la medida que se aplican más próximos al origen de la amenaza. Conocer la cultura de riesgo de la empresa y su organización facilita al ingeniero el diseño de medidas más eficientes para reducir los riesgos.

Se supone que el ingeniero no tenga experiencia ni formación previa en organización, así como tampoco en sistemas de control y gestión. Se espera que con en este capítulo el ingeniero descubra la importancia de comprender la organización para proponer controles adecuados y coherentes con los procesos y la cultura del riesgo de la empresa.

2.3 Métodos básicos en la evaluación de riesgos.

Es necesario poner en un mismo nivel los conocimientos básicos en la evaluación de riesgos que algunos de los ingenieros de seguridad pueden tener, por su práctica profesional, o por haber cursado algún curso de Dirección de Seguridad, con el desconocimiento que puedan tener otros.

El método que se utilice para la evaluación del riesgo no es lo importante. Lo importante es el proceso de gestión del riesgo, las decisiones que se toman y el ajuste de las métricas para que los resultados sean adecuados. Esa es la razón por la cual las competencias se desarrollan en este orden:

- Primero, conocer el proceso de gestión del riesgo.
- Segundo, aprender sobre la cultura del riesgo en la empresa y su organización.
- Tercero, aprender algunos métodos básicos para la evaluación de riesgos.
- Los siguientes capítulos tratan con profundidad cada una de las fases del proceso.

2.4 El contexto en la evaluación de los riesgos.

El estudio del contexto es un elemento clave, y su importancia aumenta en la medida que el entorno influye en los riesgos de la empresa.

Se viene escuchando desde hace tiempo que se está ante un entorno volátil, incierto, complejo, ambiguo e hiperconectado, y su influencia se manifiesta con el dinamismo de los riesgos emergentes.

El ingeniero de seguridad debe entender el contexto externo e interno de la empresa, los grupos de interés y demás actores, las variables motrices y las relaciones de interdependencia entre los riesgos.

Desarrollar esas competencias le permitirá disponer de herramientas para justificar la aplicación o diseño de determinados controles, a veces antes de que se evidencie su necesidad.

Entender el contexto, también le permitirá decidir al ingeniero de seguridad sobre mitigar el riesgo mediante controles preventivos, o bien con el diseño de controles correctivos.

El estudio del contexto se debería evaluar mediante la realización de casos prácticos.

2.5 Evaluación de los riesgos.

En este capítulo el ingeniero de seguridad profundizará competencias en los tres pasos para la evaluación de los riesgos: identificación, análisis y valoración.

En el proceso de identificación de los riesgos el ingeniero desarrollará competencias para aplicar la información obtenida en el estudio del contexto, identificación de amenazas, zonas de riesgos, creación de un mapa de amenazas, así como entender la importancia de realizar un análisis preliminar de peligros para enfocar la evaluación en los riesgos relevantes para la empresa.

En el proceso de análisis y evaluación de los riesgos, el ingeniero de seguridad desarrollará competencias en la aplicación de técnicas específicas que permitan mejorar el proceso de análisis y evaluación de los riesgos, así como ajustar las métricas para disponer de una clasificación acorde a la cultura de riesgo de la empresa.

2.6 Tratamiento de los riesgos.

Es quizás el tratamiento de los riesgos el espacio del proceso que más impacta en la actividad del Ingeniero de Seguridad. En esta etapa se desarrollarán competencias para tomar decisiones sobre qué riesgos tratar, qué tipo de medidas son adecuadas en función de las características de cada factor de riesgo, el lugar y los detalles que requiere su instalación para cada uno de los riesgos.

Durante el proceso, eminentemente práctico y basado en casos, el Ingeniero de Seguridad propondrá los riesgos a tratar, las recomendaciones de tratamiento y el riesgo residual que se espera.

2.7 Técnicas en la gestión del riesgo

A lo largo de la actividad formativa, el Ingeniero de Seguridad adquirirá competencias en el uso de técnicas que facilitan y hacen más objetiva cada una de las fases del proceso de gestión del riesgo.

Es necesario que el Ingeniero de Seguridad conozca distintas técnicas aplicables para sortear las dificultades de la gestión del riesgo.

Se espera que el Ingeniero conozca algunas técnicas aplicables a la gestión del riesgo, aunque en algunos casos no sea consciente de ello. En esta sección se propondrá provocar el uso de distintas técnicas para la solución de problemas en el proceso de gestión el riesgo.

2.8 Plan de seguridad en general.

El proceso de gestión del riesgo de seguridad y sus resultados debe documentarse e informarse en la empresa.

El Plan de Seguridad se redactará como resultado del proceso de gestión del riesgo de una instalación, cuyos controles o medidas a implantar cambian el Plan de Seguridad vigente, en su caso, o generan el primer Plan del usuario.

En esta sección, el Ingeniero de Seguridad adquirirá conocimientos sobre el contenido de los distintos documentos que se pueden utilizar para informar sobre la gestión del riesgo, entre los que se indican:

- Plan de seguridad de una instalación.
- Plan de gestión del riesgo en seguridad.
- Auditoría basada en riesgos de seguridad.
- Informe de riesgos.
- Estudio de seguridad.
- Cuestionarios de evaluación.
- Informe de madurez del sistema de seguridad.

2.9 Planes específicos de protección.

La importancia de la protección de algunas instalaciones para la sociedad es un factor clave para que la legislación obligue a determinadas instalaciones disponer de planes específicos de protección.

En esta sección, el Ingeniero de Seguridad adquirirá conocimientos sobre los distintos planes de seguridad que son obligados en determinadas instalaciones, así como el enfoque en la gestión de los riesgos.

Sin carácter limitativo, en esta sección el Ingeniero de Seguridad adquirirá conocimientos de:

Plan de Seguridad del Operador de infraestructuras Criticas “PSO”.

Plan de Protección Específico “PPE”.

Plan de Seguridad Ciudadana “PSC”.

Plan de Autoprotección y Emergencias

2.10 Inteligencia en la Gestión del Riesgo.

La Gestión del Riesgo está orientada a gestionar la incertidumbre en las empresas, en este caso, contra amenazas de origen antisocial o ataques deliberados.

Para finalizar la Gestión de Riesgo, se pretende iniciar al Ingeniero de Seguridad en conocimientos y capacidades en el análisis de inteligencia orientado a la gestión de riesgos, donde es necesario identificar, entender y si es necesario, supervisar, la intencionalidad del adversario y sus motivaciones.

2.11 Referencias

- AEINSE E20/22 “Necesidades formativas de los Ingenieros de Seguridad”, febrero 2022.
- UNE-ISO GUIA 73 IN “Gestión del riesgo. Vocabulario”. Traducido por AENOR (Asociación Española de Normalización y Certificación), julio 2010.
- UNE-ISO 31000:2018 “Gestión del riesgo. Principios y Directrices”. Traducido por AENOR (Asociación Española de Normalización y Certificación), marzo 2018.
- UNE-ISO 31010:2011 “Gestión del riesgo. Técnicas de apreciación del riesgo”. Traducido por AENOR (Asociación Española de Normalización y Certificación), mayo 2011.
- ANSI/ASIS/RIMS RA.1-2015 “Evaluación de riesgos”. Traducido por AENOR (Asociación Española de Normalización y Certificación), 2016.
- ASIS ESRM-2019 “GUIDELINE Enterprise Security Risk Management”. ASIS INTERNATIONAL, 2019.

3 Materias del Área Legal

El Ingeniero de Seguridad debe tener conocimiento sobre el principio de jerarquía normativa en el ámbito jurídico en España.

El orden jurídico está formado por leyes y normas de distinto rango, ordenadas conforme a un principio de jerarquía. Este principio indica que las normas de menor grado no pueden contrariar las de mayor grado.

3.1 Seguridad Privada

Este campo es la base legal de actuación del Ingeniero de Seguridad, en el marco de la Seguridad Privada. Se estudiarán el conjunto de documentos que conforman el sector de la seguridad privada en el país. Sin ser excluyentes, a la fecha de publicación de esta guía, los textos mínimos a estudiar deberían ser:

- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana *(BOE núm. 77, de 31 de marzo)*.
- Ley 5/2014, de 4 de abril, de Seguridad Privada *(BOE núm. 83, de 5 de abril)*.
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada *(BOE núm. 8, de 10 de enero de 1995)*.
- ORDEN INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada.
- ORDEN INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada.
- ORDEN INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada
- Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada *(BOE núm. 42, de 18 de febrero).*

Cataluña y País Vasco son comunidades autónomas con competencias en Seguridad Privada. El Ingeniero de Seguridad con actividad en estas comunidades deberá conocer la legislación específica de la región.

Para el estudio de estas competencias, el alumno no necesita poseer conocimientos previos, ya que precisamente son estos los que se van a adquirir.

La evaluación debería ser mediante la resolución de casos prácticos.

3.2 Protección Infraestructuras Críticas

Las infraestructuras críticas son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales; y que son indispensables y no permiten soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales

Los Ingenieros de Seguridad que actividad en el marco de Protección de Infraestructuras Críticas deberán conocer a la fecha de publicación de esta guía:

- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.
- Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Directiva NIS 2 publicada en el Diario Oficial de la Unión Europea el 27 de diciembre 2022

3.3 Protección de la información

La información es un activo o un recurso cada vez más valorado por las personas, las empresas y los estados. En este sentido, el Ingeniero de Seguridad debe conocer la legislación que aplica:

3.3.1 Protección de datos personales

La LOPDGDD viene a sustituir la conocida LOPD 15/1999, por lo que la deroga en su totalidad. No obstante, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal se mantiene en tanto no se oponga o resulte incompatible con el Reglamento (UE) 2016/679 conocido como RGPD o GDPR (en sus siglas en inglés) y la presente LOPDGDD.

Sin ser excluyentes, los textos mínimos a estudiar deberían ser:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- R.D. 1720/2007 Reglamento que desarrolla la Ley de protección de datos

3.3.2 Protección de secretos empresariales

Las empresas están cada vez más expuestas a prácticas desleales que persiguen la apropiación indebida de secretos empresariales, como el robo, la copia no autorizada, el espionaje económico o el incumplimiento de los requisitos de confidencialidad.

La protección de los secretos empresariales debe ser conocida por el Ingeniero de seguridad.

- Ley 1/2019, de 20 de febrero, de Secretos Empresariales

3.3.3 Protección de materias clasificadas

Protección de la información clasificada en España y conforme a las obligaciones contraídas en el ámbito internacional por nuestro país con otros estados u organizaciones internacionales.

- Ley 9/1968, de 5 de abril, sobre secretos oficiales.
- Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de abril sobre Secretos Oficiales.
- Ley 48/1978, de 7 de octubre, por la que se modifica la Ley de 5 de abril de 1968, sobre Secretos Oficiales.
- Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad
- Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia
- Normas y recomendaciones dictadas por la Autoridad Nacional de Seguridad para el tratamiento y custodia de la información clasificada

3.4 Protección de armas y explosivos

Dentro de este ámbito, el Ingeniero de Seguridad debe conocer la legislación específica que aplica a las medidas de protección, en las siguientes áreas:

- Protección de armas
- Protección explosivos
- Protección de pirotecnia y cartuchería
- Protección en la actividad de seguridad privada
- Protección de material de defensa, y de doble uso

La legislación que aplica es extensa, y se recomienda el Código Electrónico: “Armas y Explosivos”, edición actualizada a 2 de diciembre de 2022

3.5 Protección física en el ámbito del CSN

El CSN (Consejo de Seguridad Nuclear) es el único organismo en España con competencias en materia de seguridad nuclear y protección radiológica.

En materia de protección física, el ingeniero de seguridad debe conocer la generalidad de la normativa específica que aplica: Internacional, europea, nacional, e instrucciones del CSN. El Ingeniero de Seguridad debe conocer:

- Real Decreto 1086-2015, de 4 de diciembre, por el que se modifica el Real Decreto 1308-2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas
- Real Decreto 1308-2011, de 26 de septiembre, sobre protección física de las instalaciones y los materiales nucleares, y de las fuentes radiactivas

Las instrucciones de CSN son normas técnicas en materia de seguridad nuclear y protección radiológica que tienen carácter vinculante para los sujetos afectados por su

ámbito de aplicación, una vez han sido publicadas en el Boletín Oficial del Estado. El ingeniero de seguridad debe conocer:

- Instrucción IS-09, de 14 de junio de 2006, del Consejo de Seguridad Nuclear, por la que se establecen los criterios a los que se han de ajustar los sistemas, servicios y procedimientos de protección física de las instalaciones y materiales nucleares
- Instrucción IS-41, de 26 de julio de 2016, del Consejo de Seguridad Nuclear por la que se aprueban los requisitos sobre protección física de fuentes radiactivas

Las guías de Seguridad del CSN, son documentos técnicos de carácter no obligatorio dirigidos a orientar a los sujetos afectados por la normativa vigente en materia de seguridad nuclear y protección radiológica. Su finalidad es orientar y facilitar a los usuarios la aplicación de dicha normativa. Puesto que las Guías no son de obligado cumplimiento, los usuarios pueden seguir métodos y soluciones diferentes al contenido de estas, siempre y cuando estén debidamente justificados

- GS 08-01 Protección física de los materiales nucleares en instalaciones nucleares y en instalaciones radiactivas (Marzo 2000)
- GS 08-02 Elaboración, contenido y formato de los planes de protección física de las instalaciones y los materiales nucleares (Julio 2012)

3.6 Ciberseguridad

La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización *(fuente:https://www.ibm.com/es-es/topics/cybersecurity)*

Si bien es cierto que la práctica del Ingeniero de Seguridad está orientada a la protección física de las instalaciones, las personas y la información; las amenazas hibridas cada vez más frecuentes, requieren que el Ingeniero de Seguridad conozca el entorno regulatorio y obtenga capacidades para la protección ciber de los propios sistemas de seguridad.

La legislación que aplica es extensa, y se recomienda el Código Electrónico:

- Código de Derecho de la Ciberseguridad, edición actualizada a 19 de septiembre de 2022.

3.7 Seguridad contra incendios

Este campo, aunque no aparece detallado en la legislación de Seguridad Privada, tiene una relación real y práctica con ella. Es por esto, que el ingeniero debe conocer un mínimo de legislación, sin entrar en detalle profundo de los sistemas. Sin ser excluyentes, los textos mínimos a estudiar deberían ser:

- Real Decreto 513/2017, de 22 de mayo, por el que se aprueba el Reglamento de instalaciones de protección contra incendios.

- Real Decreto 314/2006, de 17 de marzo, por el que se aprueba el Código Técnico de la Edificación, y en documentos asociados DB-SI
- Real Decreto 2267/2004, de 3 de diciembre, por el que se aprueba el Reglamento de seguridad contra incendios en los establecimientos industriales.

Para el estudio de estas competencias, el alumno necesita poseer conocimientos mínimos de sistemas contra incendios, tanto de la vertiente activa como pasiva.

3.8 Otros reglamentos técnicos

3.8.1 Reglamento de baja tensión

El diseño en baja y muy baja tensión de los sistemas de seguridad requieren del Ingeniero conocimiento y competencias en este área. Sin ser excluyentes, los textos mínimos a estudiar deberían ser:

- Real Decreto 842/2002, de 2 de agosto, por el que se aprueba el Reglamento electrotécnico para baja tensión (BOE 18/09/02).

Código electrónico Reglamento electrotécnico para baja tensión e instrucciones técnicas complementarias (ITC) actualizado a 16 de marzo de 2022.

3.8.2 Reglamento de infraestructuras de telecomunicaciones

Las infraestructuras de telecomunicaciones dan servicio a los sistemas de seguridad. Es por esto, que el ingeniero debe conocer un mínimo de legislación, sin entrar en detalle profundo de los sistemas. Sin ser excluyentes, los textos mínimos a estudiar deberían ser:

- Infraestructuras comunes en edificios para el acceso a servicios de telecomunicación.
- Reglamento regulador de las infraestructuras comunes de telecomunicaciones
- Desarrollo Reglamento regulador de las infraestructuras comunes de telecomunicaciones.
- Medidas para reducir el coste del despliegue de redes de comunicaciones electrónicas.
- Regulación de características de reacción al fuego de cables de telecomunicaciones (parcial).
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

4 Materias del Área de Normativa Técnica

4.1 Introducción a la Normativa Técnica

El conocimiento del conjunto de la Normativa técnica, su utilidad, su diferencia con la reglamentación legal y, a su vez, la complementariedad de ésta que supone se considera de gran importancia para el uso adecuado de la normativa por parte del ingeniero, ya sea por imperativo legal o como apoyo a su especialidad técnica basada en buenas prácticas.

Esta materia introductoria debe permitir al alumno saber qué normas ha de utilizar en cada especialización técnica, cuáles son sus ámbitos de aplicación y, en su caso, qué debe exigir a los materiales, equipos, sistemas o aplicaciones que utiliza en su actividad profesional, así como entender las referencias que pueden plantear los fabricantes de este tipo de elementos.

La materia debe incluir una descripción de los organismos generadores de materias (ISO, IES, CEN, CENELEC, AENOR, ANSI, IEEE, etc.) y su campo de aplicación y características principales.

También debe exponer las diferencias entre normalización, certificación, homologación, etc. y entender el alcance de cada uno de estos conceptos.

En general, en todas las materias correspondientes a grupos de normas técnicas que a continuación se exponen, se hará hincapié en las que estén recogidas en el ordenamiento legal de la Seguridad Privada en España.

Se enumerarán las principales normas existentes y se explicarán en detalle las de aplicación obligatoria (incluyendo en qué circunstancias lo son) o las de uso más extendido.

Las competencias de este conocimiento se demostrarán mediante la aplicación de ejemplos y respuestas a cuestionarios estructurados, que permitan valorar el nivel de dominio del aspecto normativo del Ingeniero.

4.2 Normativa de equipos y sistemas electrónicos

Descripción ordenada de las normas técnicas vigentes de los elementos y sistemas de electrónicos, tanto de grandes Sistemas como de instalaciones conectadas a Centrales Receptoras de Alarma, incluso las que afecten a éstas.

Se incluirán las normas correspondientes a las especialidades de:

- Detección de Intrusión
- Recepción y gestión de alarmas
- Control de accesos
- Videovigilancia
- Detección y extinción automática de Incendios

- Interfonía de Seguridad
- Sistemas anti-atraco
- Inspección de valijas y paquetería

4.3 Normativa de las barreras físicas

Descripción ordenada de las normas técnicas vigentes de los materiales y los elementos y sistemas mecánicos que presentan en general resistencia a las intrusiones a los accesos indebidos de personas y vehículos y al paso de proyectiles.

Se incluirán las normas correspondientes a las especialidades de:

- Vallados y cercados
- Puertas y cerraduras
- Tornos, torniquetes y elementos de control de paso de personas
- Barreras y elementos de control de paso de vehículos
- Cajas fuertes, cámaras acorazadas, contenedores varios de seguridad
- Blindajes

4.4 Normativa de la gestión de la Seguridad.

Descripción ordenada de las normas técnicas vigentes que afecten a la gestión de la Seguridad, muy especialmente en lo correspondiente a la planificación.

Se incluirán las normas correspondientes a las especialidades de:

- Gobernanza de la Seguridad
- Análisis de riesgos
- Gestión de servicios de vigilancia
- Gestión de Centros de Control

4.5 Normativa relacionada de carácter general

Descripción ordenada de las normas técnicas vigentes relacionadas con aspectos generales, colaterales a la Seguridad, pero que han de conocerse (y a veces aplicar obligatoriamente) para un correcto desempeño de la labor del ingeniero.

Sin ser limitativos, se incluirán las normas correspondientes a las especialidades de:

- Elaboración y gestión de Proyectos
- Protección de Incendios

- Ciberseguridad de los Sistemas de Seguridad y OT
- Instalaciones eléctricas
- Evacuación y autoprotección de edificios
- CPTED

4.6 Referencias

Las referencias normativas específicas que se citan en cada uno de los apartados. Así como aquellos documentos y normas que definen el proceso de redacción, aprobación y revisión de los principales organismos de normalización.

“Directivas ISO/IEC, Parte 1 — Suplemento ISO Consolidado - Procedimientos específicos de ISO”, Novena Edición, ISO/IEC_2018.

“Guía para la redacción de normas teniendo en cuenta las necesidades de las micro, pequeñas y medianas empresas”, CEN/CENELEC Guía 17.

“IT.34.03 - Guía para la redacción de documentos normativos UNE”, UNE.

5 Materias del Área de Proyectos.

La principal expresión de la actividad de los ingenieros de seguridad son los proyectos. En esta área se incluye el conocimiento necesario para el desarrollo de los proyectos de seguridad, durante todo su ciclo de vida.

Los términos que el Ingeniero de Seguridad emplee en los proyectos tendrán un impacto positivo o negativo en el entorno profesional de su realización. Es importante para el ingeniero de seguridad emplear términos unívocos en los proyectos que:

- Permitan una única interpretación y no sean fuente de confusión.
- Faciliten la comprensión y el apoyo de la actividad por los grupos de interés.
- Eviten las interpretaciones equivocadas sobre el alcance de la actividad.

Una definición completa del proyecto es esencial para orientar la actividad del Ingeniero durante su desarrollo. En esta sección nos referiremos a proyectos de instalaciones de seguridad, simplemente como “proyectos”

5.1 Definición del Proyecto

En esta sección debe abordarse la definición del Proyecto de Instalaciones de seguridad. Se identifican cuatro dimensiones en el ámbito de aplicación:

- Proceso de Seguridad
- Tipo de Medidas de Seguridad
- Entorno Legal del Proyecto
- Etapa del proyecto durante su vida útil, Seguridad en las Personas, Seguridad de la Información y Seguridad Física.

Aunque la mayoría de los proyectos están dentro de la Seguridad Física, son cada vez más los que incluyen medidas para la protección de la información y de seguridad en las personas.

Desde el punto de vista del tipo de medidas, la formación sobre el proyecto ha de incluir medidas técnicas, humanas y organizativas. Por ello la formación se apoyará en:

- La Seguridad como Proceso
- Competencias de la Ingeniería en Organización Industrial

Desde el punto de vista de su etapa en la vida útil, se tendrá en cuenta en la formación que los proyectos se pueden abordar de manera distinta:

- Inclusión de la seguridad en el diseño de los espacios antes de la construcción
- Reforma o cambio de uso de los espacios
- Instalaciones en espacios construidos
- Renovación de medidas
- Mantenimiento

5.2 Entorno de los proyectos

En esta sección, el Ingeniero de Seguridad debe aprender a abordar sus proyectos desde la perspectiva de otras disciplinas profesionales en el marco de:

- La Seguridad Privada.
- Ley de Ordenación de la Edificación.
- La gestión de proyectos y el PMBOK (Project Management Body of Knowledge).
- El Facility Management.
- Prevención de Riesgos Laborales.

Se incidirá en los requisitos adicionales, por ejemplo:

- Requisitos específicos de la seguridad ciudadana.
  - Protección de infraestructuras críticas
  - Protección de la información clasificada
  - Protección de artículos pirotécnicos y cartuchería
  - Protección de explosivos
  - Protección de armas
  - Protección de datos
- Requisitos de buenas prácticas o normas certificables, por ejemplo:
  - TAPA, ISO 28001
  - Certificaciones LEED, BREEAM, WELL o Passive House

5.3 La oficina Técnica en Seguridad

Está orientada a la gestión de proyectos de seguridad, y en particular a la preparación de ofertas, elaboración de proyectos, asistencia técnica en obras y liquidación de las obras.

Se espera que el Ingeniero de Seguridad pueda abordar aspectos técnicos, económicos, legales y de gestión básica de proyectos, así como la organización de una oficina técnica de seguridad y la documentación asociada a los proyectos.

Uno de los aspectos más relevante de la actividad de la oficina técnica corresponde con la planificación de los recursos necesarios para la ejecución de los proyectos.

Por lo tanto, la formación para adquirir destrezas y técnicas para elaborar mediciones, cálculos y valoraciones adecuadas es una actividad clave del Ingeniero de Seguridad.

Se espera del Ingeniero de Seguridad capacidad para la redacción de proyectos de instalaciones de seguridad en cualquiera de las fases que se requieran, en particular:

- Anteproyectos
- Estudios e informes
- Proyecto en instalaciones

5.4 Gestión de proyectos

La gestión de proyectos de seguridad requiere que el ingeniero disponga de competencias específicas para una planificación y control de las instalaciones en sus distintas fases.

Programar el tiempo requerido para cada una de las tareas necesarias para el proyecto y su relación con los recursos destinados es crítico para determinar si el trabajo se puede realizar con los recursos en presupuesto y los tiempos necesarios por la Unidad de Negocio (Dueño del Riesgo).

La gestión de los proyectos de seguridad basada en un estándar aporta las garantías de buen practica que las empresas requieren.

El cuerpo de conocimiento más reconocido para la gestión de proyectos es en PMBOK (Project Management Body of Knowledge), creado por el PMI (Project Management Institute)

5.5 Documentación de los proyectos

Los documentos del proyecto de seguridad deben estar orientados a su finalidad, en este sentido se agrupan en tres grandes grupos:

- Documentos para la aprobación
- Documentos para la instalación
- Documentos para el mantenimiento

El Ingeniero de Seguridad debe estar formado en aplicar proporcionalidad entre el alcance económico del proyecto y su documentación.

5.5.1 Documentos para la aprobación

El ingeniero aprenderá a redactar los documentos útiles y de aplicación hasta la aprobación del proyecto:

- Informe de riesgos: Es un informe que refleja el resultado del tratamiento propuesto para los riesgos conforme al proceso de gestión del riesgo de la norma ISO 31000:2018. Este informe puede ser utilizado por los responsables de seguridad para informar a su Unidad de Negocio (Dueño del Riesgo) sobre su exposición al riesgo y recomendaciones.
- Propuesta de Diseño: Conforme a la norma UNE-CLC/TS_50131-7, es el documento que refleja el estudio previo del emplazamiento, los riesgos y hace una propuesta de tratamiento mediante medios técnicos. Es un documento básico para decidir sobre la realización de un proyecto de instalaciones.
- Informes de evaluación de ofertas: Son informes que muestran el resultado de aplicar técnicas para una evaluación objetiva de las ofertas recibidas para un proyecto. Se trata de un documento que permita hacer una análisis precio/ valor y facilite la toma de decisiones sobre la adquisición.

5.5.2 Documentos para la instalación

El ingeniero aprenderá a redactar los documentos para la instalación y los necesarios durante su ejecución.

El documento básico para la instalación se denomina Proyecto de Instalación, conforme al código de Seguridad Privada, y debe ser realizado para la aprobación del cliente antes de iniciar la instalación.

El Proyecto de Instalación guarda relación con los objetivos previstos para la Propuesta de Diseño y Plan de instalación indicados en la norma UNE-CLC/TS_50131-7.

Se instruirá al ingeniero sobre los distintos documentos de control de calidad, reporte y control de la ejecución, así como informes sobre la propuesta de cambios y precios contradictorios.

5.5.3 Documentos para la explotación de los sistemas

Los documentos para la entrega del Proyecto de Instalaciones deben incluir tres grupos de información:

- Documentación “As Built”
- Pruebas de Recepción
- Documentación para la explotación

5.6 Referencias

M.A Sebastián Pérez (2017). **"Oficina Técnica y Proyectos"**, Ed.: Universidad Nacional de Educación a Distancia. Madrid

“**Guía de los Fundamentos para la Dirección de Proyectos**”, Quinta Edición, Project Management Institute.

6 Materias del Área de Controles Técnicos.

6.1 Introducción a los controles técnicos

Dentro de las responsabilidades de un Ingeniero de Seguridad, el diseño de los controles técnicos de un sistema de seguridad es uno de sus principales entregables, por ello en la formación del ingeniero de seguridad es parte troncal su capacitación en todo lo relacionado con los mismos.

En esta materia se describirá una primera clasificación de los controles técnicos (o medidas técnicas) de Seguridad y su función dentro de un Proyecto de Seguridad

6.2 Elementos pasivos frente a intrusión en edificios y cierre perimetral

Los elementos pasivos frente a la intrusión son mecanismos altamente importantes en un buen diseño de seguridad porque son los principales obstáculos que pueden impedir o dificultar la intrusión en un espacio físico.

Por ello, el correcto diseño de los mismos es crítico y facilitará la efectividad del resto de controles técnicos principalmente electrónicos que se ubiquen posteriormente.

Por ello, será necesario conocer las características y posibles aplicaciones de diversos sistemas de vallado perimetral y cerramientos de seguridad en combinación con la arquitectura propia de la instalación y su complementariedad con el resto de sistemas de seguridad.

6.3 Elementos pasivos de cierre y bloqueo de puertas y vías de paso

El control de circulación de vehículos y peatones en las instalaciones a proteger forman parte del diseño principal de las mismas, no sólo a nivel de seguridad sino que está relacionado con los diferentes usos que se puedan realizar en las mismas.

Son los que permiten canalizar de una manera ordenada la entrada y la salida, tanto de personas como de vehículos, de unas instalaciones en las diferentes circunstancias ordinarias o extraordinarias, así como son los principales obstáculos que pueden impedir o dificultar la intrusión en un espacio físico.

Las múltiples posibilidades técnicas su posibles maniobras y usos son imprescindibles en el conocimiento del Ingeniero de Seguridad. Además son importantes las implicaciones legales y normativas como, por ejemplo, en los casos de rutas de evacuación o accesos para personas con discapacidad.

6.4 Detección de intrusión

Los sistemas de detección de intrusión son elementos básicos de un sistema de seguridad, se pueden encontrar instalaciones en las cuales el único sistema de seguridad es el de detección de intrusión. Estos sistemas tienen una larga historia y están condicionados por una alta carga normativa que se ha ido definiendo a lo largo de los años.

Para realizar un correcto diseño y dimensionamiento de un sistema de detección de intrusión será imprescindible formar al Ingeniero de Seguridad en profundidad sobre las posibilidades, limitaciones y aplicaciones de uso de las diferentes tecnologías de detección: infrarrojo pasivo, microondas, LIDAR; radar, analítica de vídeo, etc.

6.5 Sistemas antihurto

El ámbito de la distribución minorista, es uno de los ámbitos económicos más sensibles ante comportamientos antisociales como el hurto o la pérdida desconocida. Debido a los condicionantes propios de los establecimientos comerciales se hace altamente complicado la protección de los productos de valor comercializados en los mismos, lo que ha derivado en tecnologías de sistemas antihurto para dar una solución a esta problemática específica.

Se deberá formar al Ingeniero de Seguridad para conseguir una integración adecuada del sistema de seguridad con los propios procesos comerciales e industriales internos. Los sistemas antihurto también tienen su aplicación en otros ámbitos de la empresa, como son la gestión de almacenes o en el área de fabricación, por lo que será necesario tener en cuenta toda la cadena de fabricación y suministro de la propia organización.

6.6 Control de Accesos de personas, vehículos y materiales

Los sistemas de gestión de control de accesos son herramientas básicas en manos de las organizaciones de seguridad que permite una gestión adecuada de la capacidad de acceso a la instalaciones, así como el flujo y tránsito de personas reduciendo o minimizando posibles incidentes de seguridad. Igualmente juegan un papel importante de disuasión o también son utilizados por parte de las diferentes organizaciones para el control de procesos internos gracias al control de la movilidad.

Se deberá incidir en esta materia en que, además de los riesgos de seguridad a tener en cuenta, es necesario valorar otras muchas condicionantes que hacen que la configuración de un sistema de seguridad sea una de las actividades más extensas a la hora de la configuración por un Ingeniero de Seguridad.

6.7 Comunicación por voz: interfonía y megafonía

Tanto la interfonía de modo bidireccional, como la megafonía como comunicación unidireccional, son mecanismos electrónicos habituales de interacción con el equipo de seguridad en las diferentes ubicaciones de las instalaciones. Tienen un papel fundamental en instalaciones de pública concurrencia como estaciones de transporte, túneles, estadios o centros comerciales y son de alta criticidad en situaciones de riesgo elevado o evacuación.

Son elementos habituales de todo proyecto de seguridad y en su formación se tendrá que tener en cuenta su relación con otros sistemas como el control de accesos o el de videovigilancia con los cuales están comúnmente relacionados.

6.8 Circuito Cerrado de Televisión y videovigilancia

El vídeo de seguridad es claramente una de las disciplinas tecnológicas que más rápido están evolucionando en los últimos años. Se benefician de avances tecnológicos del mercado tecnológico general pero aplicado a la seguridad como son el vídeo IP, algoritmos de analítica de vídeo e inteligencia artificial, compresión de información, sensores térmicos, etc.

Estas grandes posibilidades permiten tener un amplio espectro de aplicación pero, a su vez, requieren del Ingeniero de Seguridad un alto conocimiento de las posibilidades técnicas y su correcta aplicación ante cualquier proyecto que se pueda encontrar. Sin duda se trata de uno de los capítulos de Controles Técnicos con una mayor carga técnica que va desde la evaluación de condiciones ópticas hasta las posibilidades de la inteligencia artificial.

Las nuevas tecnologías de analítica de vídeo e inteligencia artificial han convertido a los sistemas de circuito cerrado de televisión en sistemas interpretadores de la escena, lo que implica que la labor del ingeniero de seguridad no sólo es el diseño e instalación sino que también la correcta utilización y configuración de algoritmos de detección aplicados a escenarios concretos.

La tecnología de videovigilancia es crucial en la detección y evaluación de riesgos en tiempo real pero también en la investigación forense ya que supone en muchos casos información crítica ante posibles actuaciones judiciales. Ello hace que sea una herramienta crucial para los departamentos de seguridad, requiriendo al Ingeniero de Seguridad el tener una capacitación profunda para conseguir el correcto alineamiento entre requerimientos específicos del proyecto y la gran variedad de tecnología disponible.

6.9 Protección contra incendios

La Protección contra incendios cuenta con un amplio repertorio de capacitaciones y certificaciones específicas por lo que no se pretende realizar una capacitación profunda al respecto. Para el alcance de esta formación, en este capítulo se explicará brevemente las diferentes tecnologías de detección de fuego y extinción de incendios y sus implicaciones

con los sistemas de seguridad que son el objeto troncal de la formación del Ingeniero de Seguridad.

6.10 Equipamiento de Centros de Control

En muchas ocasiones los centros de control son los elementos de un sistema de seguridad sobre los que menos énfasis se realiza, pero sin embargo se tratan del núcleo principal y desde el cual se debe hacer un uso y aprovechamiento óptimo de los controles técnicos desplegados. Contar con un equipamiento adecuado es importante pero en el ámbito del centro de control se deben asegurar que los procedimientos de gestión de alarmas de detección, evaluación y respuesta ante los diferentes riesgos o eventos que se producen son correctamente gestionados.

Esto implica conocer los medios técnicos de integración de sistemas y visualización de información, pero también de sistemas lógicos y de la correcta configuración del sistema para cumplir con los procedimientos de gestión definidos.

6.11 Comunicaciones

Un sistema de seguridad puede tener una extensión reducida como puede ser una vivienda o puede ser un sistema global interconectado. En todos los casos los sistemas de comunicación entre los diferentes componentes son cruciales. Dentro de las tareas de diseño por parte del Ingeniero de Seguridad se requiere un diseño, dimensionamiento, puesta en marcha y gestión óptima del sistema de comunicación subyacente. Además de asegurar el funcionamiento se tendrá que responder a requerimientos de ciberseguridad en las comunicaciones, alta disponibilidad y protección de la información puesto que las comunicaciones son un objetivo claro de ciberataques además de ser una infraestructura muy sensible a fallos o accidentes que provoquen un posible corte o fallo del sistema general. El Ingeniero de Seguridad deberá dominar conocimientos técnicos suficientes para poder plantear un sistema de comunicaciones y contrastarlo con interlocutores como administradores de sistemas o directores de tecnologías de la información.

6.12 Tecnologías de respuesta a la detección de otras amenazas (drones y robótica en general)

Las tecnologías de seguridad son grandes receptores de las principales tendencias tecnológicas y los principales avances son la robótica en general y con mayor desarrollo a día de hoy los drones en particular. Son tecnologías que pueden ser usadas de manera activa por las organizaciones de seguridad como por ejemplo un dron para acudir a inspeccionar una zona remota en caso de salto de alarma pero también son necesarias contramedidas tecnológicas ante el uso malicioso de estas tecnologías.

El Ingeniero de Seguridad debe conocer las diferentes medidas técnicas aplicables en los diferentes escenarios así como su coordinación con el resto de Controles técnicos. Siendo una de las áreas más novedosas todavía existen ámbitos de desarrollo

tecnológico en evolución con lo que la capacidad de adaptación y resolución de problemas propia del Ingeniero va a ser requerida en la aplicación de estas tecnologías. Igualmente son ámbitos con normativas recientes y en pleno desarrollo que exigirán una adaptación a circunstancias y ámbitos de aplicación cambiantes.

6.13 Referencias

Protección de Activos - Seguridad Física, 2014. ASIS International

Manual de Seguridad Electrónica, GET, Jesús Felipe García Cubillo

7 Materias del Área de Infraestructuras

7.1 Construcción de sala de control

Con frecuencia el Ingeniero de Seguridad ha de diseñar una sala de control desde donde se gobiernen los sistemas de seguridad propios de su Compañía o de un cliente, por lo que se requiere conocer la normativa al respecto y determinar todos los elementos y requerimientos a tener en cuenta en la sala.

Por tanto, se han de calcular: superficies necesarias, compartimentación y blindajes, emplazamiento, y sus comunicaciones, mobiliario con su ergonomía y dotación de medios de seguridad intrínsecos de la sala, tales como control de accesos y visitas, detección de intrusión, videovigilancia, protección contra incendios y medios de comunicación.

Para el aprendizaje en la construcción de salas de control, se han de estudiar cada una de las características físicas y de seguridad definitorias y, en base a este conocimiento, se describirán y analizarán una serie de ejemplos, para así poder realizar ejercicios sobre edificios ficticios, valorándose los diferentes cálculos indicados en el párrafo anterior. De este modo, se podrá afrontar la construcción de una sala real.

7.2 Dotación de equipos de operación

En la sala de control, aparte de su contexto y condiciones mínimas necesarias, incluidas en el punto anterior, han de situarse en su mobiliario los elementos de centralización y operación del sistema global de seguridad controlado desde la sala: de detección de intrusión, control de accesos de personas, vehículos y materiales, videovigilancia, protección contra incendios, recepción de señales, verificación de alarma y comunicaciones interiores y exteriores.

De cada subsistema de seguridad se tendrán en cuenta los elementos necesarios de centralización y operación, así como los integradores entre los mismos.

Para la formación en el diseño de la dotación de equipos, se han de conocer en detalle todos los subsistemas de seguridad, que a su vez deben ser integrables entre sí. Por tanto, el aprendizaje sobre la dotación de los equipos de operación de las salas de control se ha de realizar tras el del conocimiento suficiente sobre los diferentes subsistemas de seguridad. Con este conocimiento, se realizarán una serie de ejemplos, tras los cuales ya se estará en disposición de realizar ejercicios evaluables al respecto.

7.3 Suministro eléctrico

El suministro eléctrico es esencial para la funcionalidad de todo sistema de seguridad y así queda recogido en la normativa de aplicación. Además, no sólo es necesaria una fuente primaria de corriente alterna, sino que suele ser necesaria una segunda fuente, en caso de fallo o interrupción de la principal, por medio de equipos de alimentación con baterías o de sistemas de alimentación ininterrumpida (SAI o UPS en denominación en lengua inglesa).

La formación en esta materia ha de incidir en que el suministro eléctrico principal ha de coordinarse con los demás servicios eléctricos del recinto, edificio o complejo, de forma que esté suficientemente independiente y seguro, así como las posibles fuentes secundarias alternativas.

Para diseñar el suministro eléctrico se han de conocer los datos y situación de los equipos de seguridad que necesiten alimentación eléctrica, de forma que así se pueda realizar el adecuado cableado de alimentación entre ellos y las fuentes que sean necesarias. Para ello, serán necesarios los adecuados conocimientos de Electrotecnia.

7.4 Consumos eléctricos y caídas de tensión

El requisito fundamental para que el suministro eléctrico, definido en el apartado anterior, sea coherente, es que la red de cableado de alimentación entre equipos y fuentes sea suficientemente sobrada respecto a intensidades máximas admisibles y caídas de tensión.

Se incidirá especialmente en que cada tramo de cableado se dimensionará con la debida suficiencia respecto a intensidad máxima admisible y a caída de tensión, de forma que lo sea respecto a la más desfavorable de las dos. Para estos cálculos se han de aplicar las debidas fórmulas de Electrotecnia.

La evaluación de este tema se hará tras realizar ejemplos genéricos y casos prácticos, con diferentes tipos de configuraciones y fuentes de alimentación.

7.5 Redes de datos

Los Sistemas de Seguridad actualmente se soportan mediante una red de datos informática, tanto desde el punto de vista de topología de sus conexiones, como de las características inherentes a las redes: protocolos de comunicaciones, cableados específicos, electrónica de red, etc.

Ineludiblemente, por lo tanto, el Ingeniero de Seguridad ha de conocer los conceptos que permitan proyectar, instalar y mantener las redes de datos que forman parte del Sistema de Seguridad.

Entre las materias a incluir a este respecto, se deben tener en cuenta las siguientes:

- Proyectos e instalaciones de redes de datos
- Gestión de las redes de datos

- Sistemas operativos
- Bases de datos y su gestión

7.6 Ciberseguridad de los Sistemas de Seguridad

La propia existencia de un Sistema Informático (red de datos, sistema operativo del mercado, conexiones con el exterior, etc.) sobre el que se sustenta el Sistema de Seguridad, implica la posibilidad de sufrir ciberataques, interiores o exteriores, que comprometan el funcionamiento del Sistema de Seguridad, la integridad, confidencialidad y disponibilidad de sus datos e, incluso, el que el Sistema sirva de vehículo para realizar ataques ciber a otros Sistemas Informáticos del propietario del Sistema de Seguridad.

Las materias a conocer por el Ingeniero de Seguridad deben incluir:

- Cortafuegos de red y de aplicación.
- Sistemas de prevención de intrusión.
- Pasarelas y diodos de acceso.
- Sistemas de control de acceso a la red.
- Seguridad de redes inalámbricas.
- Bastionado de sistemas y puntos de acceso.
- Actualización de sistemas y aplicaciones.
- Control de acceso lógico.
- Prevención de fugas de información (DLP/IRM).

7.7 Cableados

En las infraestructuras físicas de las instalaciones de seguridad tanto la alimentación eléctrica como la transmisión de datos se realiza mediante cableados, pudiendo sólo esta última ser parcialmente por algún medio alternativo. En los dos apartados anteriores ya se ha descrito el cableado de alimentación y sus peculiaridades. Mientras el cableado de alimentación es siempre de un mismo tipo, variando sólo la sección del mismo, de acuerdo con la intensidad y caída de tensión, el cableado de datos es variopinto, en general de mucho menores secciones que el de alimentación, pero pudiendo contener sus mangueras desde un solo hilo hasta una enorme cantidad y variedad de cables.

En un sistema de seguridad el cálculo del cableado de alimentación es global, sin embargo en el de datos hay que ir diseñando su cableado específico subsistema a subsistema, porque cada uno suele tener unas necesidades diferentes e incluso en un solo subsistema puede ser diferente dependiendo de qué equipos contenga. Incluso equipos similares de diferentes Compañías pueden requerir cableados distintos, de acuerdo con lo que prescriba el fabricante.

Los tipos y características de los cableados posibles son las que se indican en el Reglamento Electrotécnico de Baja Tensión.

Hay que realizar un gran número de ejercicios del cableado de distintos sistemas de seguridad para estar en disposición de evaluar y aplicar con garantías los conocimientos adquiridos.

Se deberá incluir en esta materia los conocimientos necesarios para los cableados que utilizan fibra óptica, así como su dimensionado, criterios de selección y fases de su instalación y certificación.

7.8 Envolventes (Armarios y Racks)

En la infraestructura física de las instalaciones de seguridad hay generalmente una serie de elementos auxiliares, aunque por otra parte esenciales, que se encuentran dispersos por la instalación, tales como fuentes de alimentación, cuadros eléctricos, concentradores de datos, repartidores / amplificadores de señales, conversores de diferentes tipos, … etc., que deben agruparse y protegerse en una serie de alojamientos protegidos, tales como armarios y racks.

El estudio de armarios y racks, con sus componentes y accesorios, es sencillo, si bien lo complicado es determinar en una instalación todos los elementos auxiliares necesarios, por lo que habrá que incidir en la formación sobre las necesidades específicas en cada subsistema y así poder diseñar estas envolventes.

7.9 Canalizaciones

El cableado se protege mediante canalizaciones que, salvo excepciones muy concretas, serán exclusivas para el sistema de seguridad. En esta materia se describirán los tipos de canalizaciones y los criterios de su aplicación.

Los tipos y características de las canalizaciones posibles son las que se indican en el Reglamento Electrotécnico de Baja Tensión.

Se formará en que el diseño de las canalizaciones, de forma que se optimicen las distancias y las secciones, así como conducir los trazados por las zonas que tengan menos impacto estético.

Conviene realizar varios ejercicios de diseño de canalizaciones, en diversas topologías, para estar preparado para la evaluación y aplicación de los conocimientos al respecto.

7.10 Ayudas de obra civil

En la mayoría de las ocasiones las canalizaciones de las instalaciones de seguridad requieren hacer taladros o rozas en paramentos. La disposición de una sala de control adecuada también suele generar la realización / derribo de tabiques y retocar superficies de todo tipo: puertas, ventanas, suelos y techos. Los dos ejemplos anteriores, implican que en las instalaciones de seguridad surge la necesidad frecuente de ayudas de obra civil. Además, en una instalación de seguridad siempre se requieren remates de algún tipo entre albañilería, pintura, jardinería, carpintería o cerrajería.

Los trabajos de obra civil necesarios en las instalaciones de seguridad suelen ser por lo general bastante reiterativos y sencillos, por lo que el Ingeniero de Seguridad puede aprender enseguida todo lo concerniente con rapidez. En el caso de necesidades

específicas o de mucha complejidad, tales como blindajes, tendrá que recabar la ayuda o asesoramiento de personas o compañías especializadas.

7.11 Medios y maquinarias auxiliares de elevación, transporte, … etc.

Otra necesidad que surge en las instalaciones de seguridad son los medios auxiliares, tales como los de elevación y transporte. Los de elevación suelen necesitarse para el montaje de cámaras de TV, detectores de intrusión y otros posibles equipos, más sus canalizaciones en ubicaciones especiales como fachadas, terrazas o tejados, o bien si los techos de la instalación superan una cierta altura en algunos de sus habitáculos. Por su parte, los medios de transporte son necesarios en la mayoría de las instalaciones para la distribución de equipos, armarios, racks, cables, canalizaciones y accesorios.

Los medios auxiliares descritos suelen ser reiterativos y sencillos, al igual que para las ayudas de obra civil, pero en cualquier caso el Ingeniero de Seguridad. deberá tener un conocimiento general sobre su existencia y aplicación.

Es importante que se tenga en consideración la normativa de Riesgos Laborales para su uso

7.12 Referencias

Reglamento Electrotécnico de Baja Tensión, del Ministerio de Industria.

- Guías Técnicas de aplicación al Reglamento Electrotécnico de Baja Tensión, desarrolladas por el Ministerio de Ciencia y Tecnología.
- Normas Tecnológicas de la Edificación - Instalaciones, del Ministerio de Obras Públicas, Transporte y Medio Ambiente.
- Código Técnico de la Edificación.
- Normativa UNE de AENOR, referida a todos los campos que abarcan las instalaciones de seguridad.
- Normativa UNE de AENOR, referida a instalaciones de baja tensión (cableados, cuadros eléctricos, … etc.).
- Normativa UNE de AENOR, referidas a los centros de control y centros receptores de alarmas, especialmente UNE-EN 50518:2020 Y UNE-EN_ISO_11064;2001.
- Guía de buenas prácticas de Ciberseguridad en proyectos de Sistemas de Seguridad Física AEINSE 10/22