



# **DECÁLOGO DE PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA**



## UN PAÍS NO PUEDE EXISTIR SIN SU INFRAESTRUCTURA, NUESTRA VIDA DEPENDE DE LA MISMA

Desarrollar una política nacional para proteger y garantizar las infraestructuras nacionales críticas, requiere:

- Identificar la amenaza: físicas y ciber
- Desarrollar políticas legislativas
- Desplegar comisiones y realizar el plan

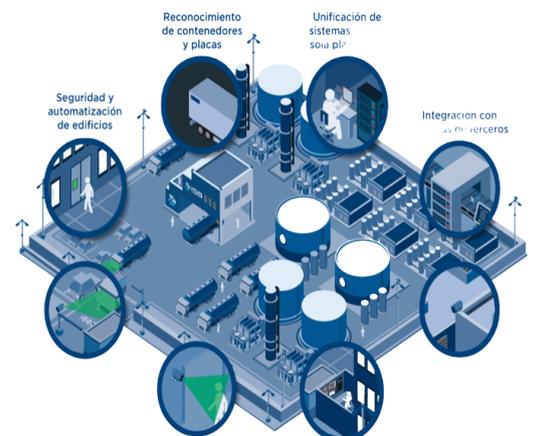
## DECÁLOGO DE PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA

El objetivo fundamental de la protección física en las instalaciones críticas es mantener un ambiente seguro para el personal que allí labora. Así como también los activos, la continuidad operacional y la seguridad de la información. Esto se logra identificando plenamente los riesgos operativos de la instalación.

Por ello se ha pensado en estos diez elementos como línea guía de la protección de la seguridad física.

## ¿QUÉ ES UNA INFRAESTRUCTURA CRÍTICA?

“Son sistemas que se consideran esenciales y los servicios que prestan son vitales para las operaciones cotidianas, la economía, la seguridad y el bienestar general de las sociedades modernas”. Así quedaron definidos por la directiva europea 2008/114/CE del 8 de diciembre de 2008.



# DIEZ ELEMENTOS COMO LÍNEA GUÍA DE LA PROTECCIÓN DE LA SEGURIDAD FÍSICA

## 1. ADMINISTRACIÓN DE RIESGOS

La Gestión de Riesgos es un elemento de gestión estratégica de los programas de seguridad, que vincula las prácticas de seguridad de una organización con su misión y objetivos, utilizando los principios de gestión de riesgos establecidos y aceptados globalmente.



## 2. PROTECCIÓN EN PROFUNDIDAD

Las medidas de protección deberán estar orientadas a prevenir los accesos no autorizados a las instalaciones. Deben disuadir, detectar y demorar cualquier intento de acceso no autorizado, incluyendo capas que hagan más difícil el accionar del adversario.



## 3. CONOCIMIENTO DEL ENTORNO

Los entornos corporativos son internos y externos. En ambos ambientes el analista de seguridad física deberá conocer a la perfección sus variaciones.



#### **4. ENTENDER LA SEGURIDAD FÍSICA COMO PARTE DEL PROCESO**

Las medidas de protección por sí solas no proporcionarán la protección adecuada, deberán ser un balance entre Personas, procedimientos y tecnología, a fin de poder dar balance a la solución de la seguridad.

#### **5. LOS MEDIOS DE PROTECCIÓN EMPLEADOS NO SÓLO DEBEN SER EFICACES, TAMBIÉN DEBEN PARECERLO**

Con esto se busca persuadir a los delincuentes. De lo contrario, pueden acarrear severos problemas comprometiendo la seguridad de la instalación.

#### **6. DISEÑAR UN PROGRAMA DE CPTED**

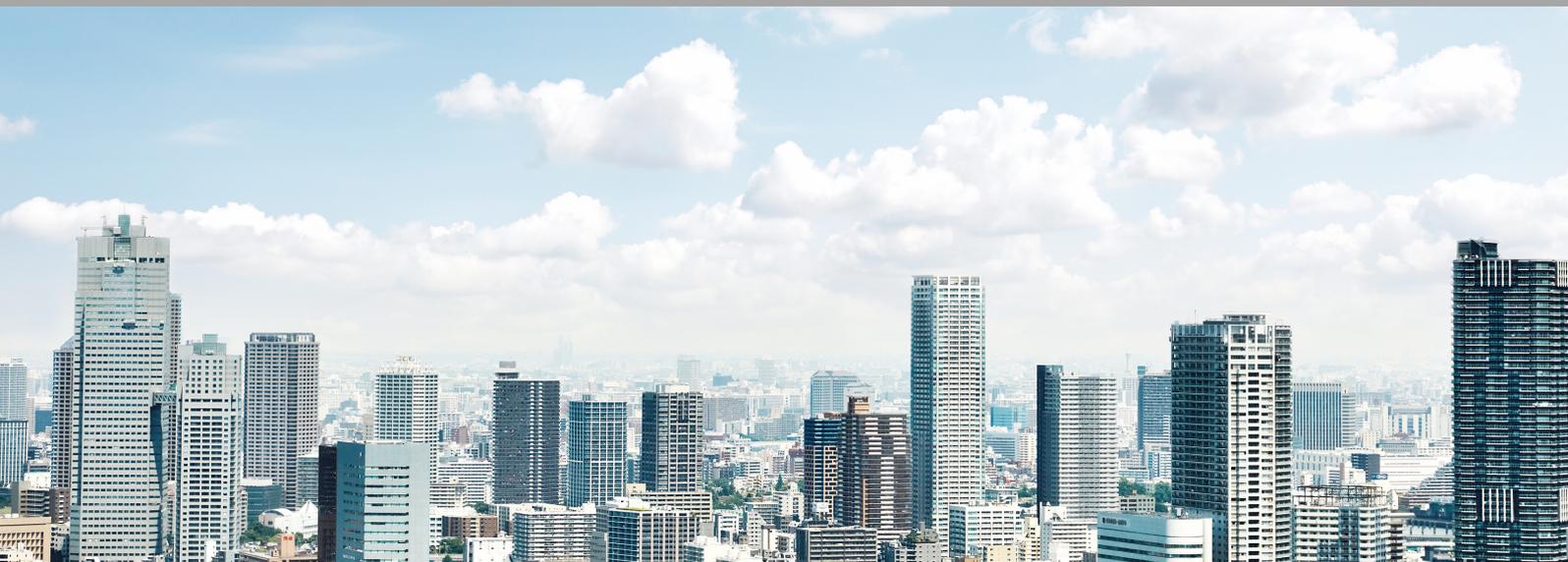
Cuando se involucra al medio ambiente en el diseño, aparte de hacer más amable el concepto de seguridad física generamos elementos de prevención muy efectivos que balancean los costos.

#### **7. CIBERSEGURIDAD**

Se refiere a la capacidad de proteger o defender el uso del ciberespacio de los ciberataques y garantizar que se alcancen y mantengan los objetivos de seguridad de la organización.

#### **8. DISEÑO DEL MODELO DE SEGURIDAD FÍSICA**

El diseño del Sistema de seguridad física busca garantizar que las amenazas y los riesgos que han sido identificados sean anticipados con medidas de seguridad eficientes que retrasen y favorezcan la respuesta ante la materialización de un riesgo.



## 9. CONTINUIDAD DE LAS OPERACIONES

La continuidad del negocio es un plan de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada, un desastre o un ataque, ya sea cibernético o de adversarios.



## 10. AUDITORIA DE SEGURIDAD

Es importante auditar la seguridad, desde sus procesos y procedimientos hasta la forma de prestar el servicio el personal a cargo. Por ello siempre se hace importante el cumplimiento de estándares por parte de los terceros prestadores del servicio. Es por ello que los estándares como el ISO 17788:2015 son referentes en las instalaciones críticas.



CEEYPP  
CENTRO DE ESTUDIOS EN  
ESTRATEGIA Y POLÍTICAS  
PÚBLICAS



**WhatsApp:** +54 9 11 2654-0867

**Web:** [www.ceeypp.com](http://www.ceeypp.com)

**Mail:** [info@ceeypp.com](mailto:info@ceeypp.com)