



AUTORIDAD NACIONAL DE SEGURIDAD DELEGADA
Oficina Nacional de Seguridad



**ORIENTACIONES PARA PLAN DE PROTECCIÓN
DE UNA ZONA DE ACCESO RESTRINGIDO**

05.05.2008

OR-ASIP-01-01.02

**ORIENTACIONES
PARA EL
PLAN DE PROTECCIÓN
DE UNA
ZONA DE ACCESO RESTRINGIDO**

ÍNDICE

1.	INTRODUCCIÓN.....	3
2.	OBJETO DEL PLAN DE PROTECCIÓN.....	3
3.	VIGENCIA, ACTUALIZACIÓN Y RESPONSABILIDADES.....	4
4.	CLASIFICACIÓN DEL PLAN DE PROTECCIÓN.....	5
5.	ELABORACIÓN DEL PLAN DE PROTECCIÓN.....	5
5.1.	GENERALIDADES	5
5.2.	PLAN DE ACONDICIONAMIENTO	5
5.2.1.	Nociones Generales.....	5
5.2.2.	Esquema Propuesto de Plan de Acondicionamiento	6
5.3.	PLAN DE SEGURIDAD.....	6
5.3.1.	Nociones Generales.....	6
5.3.2.	Esquema Propuesto de Plan de Seguridad	7
5.4.	PLAN DE EMERGENCIA	7
5.4.1.	Nociones Generales.....	7
5.4.2.	Esquema Propuesto de Plan de Emergencia	8
	ANEXO I – MODELO DE PLAN DE ACONDICIONAMIENTO	1
	ANEXO II – MODELO DE PLAN DE SEGURIDAD	1
	ANEXO III – MODELO DE PLAN DE EMERGENCIA	1

1. INTRODUCCIÓN

En las Normas de la **Autoridad Nacional para la Protección de la Información Clasificada**, especialmente la norma **NS/03 sobre Seguridad Física**, se establecen los criterios para la constitución de una Zona de Acceso Restringido (ZAR), siendo fundamental la elaboración del Plan de Protección.

Como se indica en la citada norma NS/03, bajo la denominación general de **Plan de Protección** se engloban tres documentos diferenciados:

- El Plan de Acondicionamiento.
- El Plan de Seguridad.
- El Plan de Emergencia.

Estos documentos son de obligada confección, como parte fundamental del expediente de acreditación de una ZAR, en la que se vaya a manejar o almacenar Información Clasificada.

Esta ZAR puede corresponder a las instalaciones y estructura de seguridad de un Órgano de Control (Subregistro, Punto de Control, Servicio de Protección o Cuenta de Cifra) o de una Zona de Seguridad que alberga un CECOM, una Sala de Operaciones, u otra función similar, que implica el manejo o almacenamiento de Información Clasificada en la misma.

2. OBJETO DEL PLAN DE PROTECCIÓN

Con el Plan de Protección se pretende dejar evidencia objetiva de que las medidas de seguridad implantadas, tanto de Seguridad Física, como de Seguridad en el Personal y de la Información, junto con los procedimientos organizativos de seguridad, de obligado cumplimiento, constituyen un entorno de seguridad definido, estudiado y adaptado a la normativa vigente, que permite el manejo o almacenamiento seguro de la Información Clasificada.

Son también objeto de dicho Plan:

- Constituir la normativa de seguridad del Órgano de Control o Zona de Seguridad, a través de la cual, los responsables de la seguridad y los usuarios, conozcan sus obligaciones en dicha materia, dentro de su ámbito de aplicación.
- Constituir un documento básico en los relevos de responsabilidades de seguridad, al definir y asegurar el cumplimiento de unas mismas medidas de seguridad, con independencia del personal destinado en cada momento.
- Constituir un documento básico para la formación de seguridad del personal destinado en el Órgano de Control o Zona de Seguridad.
- Constituir la guía de referencia para las inspecciones, tanto de apertura como de correcto desempeño.

3. VIGENCIA, ACTUALIZACIÓN Y RESPONSABILIDADES

Es recomendable su confección en formato electrónico, para facilitar su posterior actualización. En este sentido, es fundamental que, en todo momento, el Plan de Protección refleje de forma completa la situación real de la seguridad, no siendo de ninguna utilidad si no se actualizan los cambios que se vayan produciendo y que afecten a la misma.

Dado que este Plan constituye la referencia para la concesión del correspondiente Certificado de Acreditación de Local de la Zona de Acceso Restringido, expedido por la Oficina Nacional de Seguridad (ONS), se deberá tener en cuenta que, en tanto no haya expirado, sólo tendrá validez mientras siga siendo fiel reflejo de la situación real en materia de seguridad.

La responsabilidad final de la seguridad en cada Departamento, Organismo o Dependencia, es siempre del Jefe del mismo. No obstante, por delegación y mediante nombramiento, la responsabilidad ante dicho Jefe y la responsabilidad funcional dentro de la infraestructura de protección de la Información Clasificada, recaen en el Jefe de Seguridad del Órgano de Control, y por último en el Responsable de Seguridad de la ZAR (si fuera distinto).

Este último es responsable de la confección del Plan de Protección, así como de su implantación y de asegurar su cumplimiento.

En función de la especial idiosincrasia del Departamento, Organismo o Dependencia en el que esté encuadrado, el Responsable de Seguridad podrá ser el encargado directo del estudio, diseño e implementación de dicho Plan, o podrán estar centralizados dichos trabajos en Unidades, Grupos o Equipos especializados en dicha materia. En ningún caso el Responsable de Seguridad de la ZAR podrá delegar o transferir su responsabilidad en el producto final, salvo relevo de funciones.

El Plan de Protección sólo tendrá validez, y producirá los efectos oportunos, tras su aprobación por la ONS. Previamente a la remisión a la ONS del Plan de Protección, dentro del proceso de apertura o acreditación, se requerirá que la ZAR sea inspeccionada por el Jefe de Seguridad del Órgano de Control superior del que dependa funcionalmente en materia de seguridad, y que éste emita certificado de cumplimiento de la normativa de seguridad pertinente. Si esta inspección no resulta positiva, se adoptarán las medidas correctoras necesarias para solventarlas, requiriendo una inspección y certificación posteriores.

Independientemente de lo anterior, el Jefe del Departamento, Organismo o Dependencia del que dependa, o al que sirva, el Órgano de Control o Zona de Seguridad cuyas instalaciones y estructura de seguridad se han de acreditar, en base a sus responsabilidades podrá igualmente inspeccionar los mismos y refrendar con su firma el Plan de Protección. Este trámite no tendrá ningún efecto vinculante, respecto al proceso, en la ONS, para quien sólo serán relevantes los pasos seguidos dentro de la escala funcional (infraestructura de protección de la Información Clasificada).

En ningún caso se remitirán a la ONS expedientes de solicitud de acreditación de ZAR, cuyo Plan de Protección y, por ende, las medidas de seguridad adoptadas, no cumplan la normativa existente. En la medida en que cada escalón cumpla con sus cometidos y atienda a sus responsabilidades en materia de seguridad, los procesos serán más efectivos y rápidos, evitando la devolución de expedientes por incumplimientos.

4. CLASIFICACIÓN DEL PLAN DE PROTECCIÓN

Se tratará de evitar un exceso de clasificación de seguridad de los planes. Se estima suficiente una clasificación de nivel CONFIDENCIAL, toda vez que en ningún caso se va a aportar (sólo mencionar su existencia) el Plan Global de Seguridad de la Base, Acuartelamiento, Centro o Instalaciones, sino de una zona concreta. Con ello se facilita y agiliza la gestión del proceso.

5. ELABORACIÓN DEL PLAN DE PROTECCIÓN

5.1. Generalidades

Al objeto de normalizar los procesos y facilitar su análisis y aprobación, se recomienda seguir los esquemas o modelos de documentos que más adelante se proponen para cada uno de los planes a presentar.

Los documentos mencionados a continuación deben adaptarse a las características específicas de cada caso particular. La casuística puede incluir desde locales ubicados en edificios de oficinas, en un entorno urbano, hasta buques de guerra en alta mar, y el manejo en los mismos desde documentos en papel, a información almacenada en redes informáticas.

5.2. Plan de Acondicionamiento

5.2.1. Nociones Generales

Este documento constituye un cuerpo específico separado del resto de documentos que componen el Plan de Protección.

Su objeto es describir los sucesivos entornos de seguridad existentes, las características físicas y las medidas técnicas adoptadas, que permiten alcanzar un nivel de protección suficiente. No debe incluir, en ningún caso, procedimientos, normas o medidas organizativas, que son objeto de los otros planes.

La seguridad, normalmente se constituye y explica en profundidad, en diferentes entornos sucesivos, desde el perímetro exterior de la Base, Acuartelamiento, Edificio o Centro, hasta llegar al recinto final del Órgano de Control o Zona de Seguridad.

Se explicarán las medidas constructivas adoptadas en este último para adecuarlo a la normativa vigente en Seguridad Física, así como una descripción detallada de los medios de seguridad adicionales instalados (caja fuerte, sistemas de detección de intrusión, puertas blindadas, rejas, sistema de control de accesos, sensores de movimiento, sistema de detección de incendios, apantallamiento TEMPEST). No debe ser una mera enumeración de medios, sino una relación detallada, con indicación de características físicas, seguridad aportada, disposición y, en general, cualquier otro dato que aporte información necesaria.

Los planos originales acotados con especificación de detalles, tales como: grosor paredes, locales anexos, materiales construcción, ubicación de puertas, ventanas, rejas, sensores,

equipos, cajas fuertes, cámaras TV, constituyen un excelente medio de información adicional, y se considera prácticamente obligatoria su inclusión.

En caso de disponer de las especificaciones técnicas de los sistemas, medios y materiales empleados, así como de datos de homologación o normativa UNE que cumplan, será de considerable utilidad su inclusión. En determinados casos, esta información puede ser imprescindible para la aprobación del Plan y acreditación del local o área.

Se deberá cumplir la normativa vigente por la que se rige en cada caso

5.2.2. Esquema Propuesto de Plan de Acondicionamiento

Se propone el indicado en el Anexo I.

5.3. Plan de Seguridad

5.3.1. Nociones Generales

Este documento constituye un cuerpo específico separado del resto de documentos que componen el Plan de Protección.

Su objeto es describir las medidas organizativas de seguridad, es decir, los procedimientos de control, gestión, trabajo, guarda, salvaguarda, etcétera, establecidos en el Órgano de Control o Zona de Seguridad para, en conjunción con las medidas de Seguridad Física existentes (explicadas en el Plan de Acondicionamiento), permitir y garantizar la protección de la Información Clasificada y su adecuado manejo, en condiciones de trabajo habituales.

Para cada medida de Seguridad Física indicada en el Plan de Acondicionamiento, se explicará en el Plan de Seguridad el procedimiento de organización correspondiente, para su correcta explotación. Por ejemplo, si en el Plan de Acondicionamiento se define la existencia de una combinación en la caja fuerte, de características X, en el Plan de Seguridad se explicará el procedimiento para su correcta utilización, indicando la periodicidad y motivos de cambios de combinación, la gestión y registro de dichos cambios, la responsabilidad de realizarlos, la comprobación de funcionalidad, la verificación diaria de su uso, la gestión y salvaguarda de claves de combinación, etc.

Asimismo, allí donde exista una vulnerabilidad en la seguridad, que no sea cubierta por una medida de Seguridad Física, el Plan de Seguridad explicará la medida organizativa adoptada para reducir el riesgo existente. Por ejemplo, si no existe, y así se menciona en el Plan de Acondicionamiento, un sistema de detección de intrusión (detectores de presencia), el Plan de Seguridad puede mencionar la existencia de un servicio de personal que cubre la seguridad del Órgano de Control o Zona de Seguridad las 24 horas del día, con presencia continua.

Quiere todo esto significar que existe una relación directa entre ambos planes, pero cada uno cubre unas facetas o aspectos diferentes de la seguridad, complementándose mutuamente.

Cuanto más completo sea el Plan de Seguridad, menos quedará a la improvisación, y más sencilla será la aprobación de los planes. Es en este plan donde se explica en detalle el modelo de seguridad adoptado y se justifica su fortaleza ante posibles amenazas o vulnerabilidades existentes, por ello debe ser exhaustivo, aunque no por ello complicado.

5.3.2. Esquema Propuesto de Plan de Seguridad

Se propone el indicado en el Anexo II.

5.4. Plan de Emergencia

5.4.1. Nociones Generales

Este documento constituye un cuerpo específico separado del resto de documentos que componen el Plan de Protección.

Su objeto es describir las medidas organizativas de seguridad a adoptar o seguir para mantener la protección de la Información Clasificada ante contingencias de tipo extraordinario que puedan afectar a la misma.

El Plan de Emergencia se activará cuando las medidas contempladas en el Plan de Acondicionamiento y en el Plan de Seguridad, sean insuficientes para garantizar el nivel mínimo de seguridad permitido, motivado por una circunstancia no ordinaria. Son ejemplos de tipos de emergencia que se pueden considerar, entre otros posibles, los siguientes:

- Incendio
- Amenaza de bomba
- Disturbios, manifestaciones violentas u otro tipo de graves alteraciones del orden público:
- Ataque terrorista
- Con explosivos
- Con armas químicas / bacteriológicas
- Con armamento convencional
- Guerra o estado de alerta máxima
- Hundimiento (del buque)
- Terremoto
- Inundacion
- Otro tipo de desastres naturales (tornado, tifón, helada severa, maremoto)
- Fallo total de suministro eléctrico, de duración no asumible por los sistemas alternativos de energía.

En cada uno de los supuestos que se contemplen deben indicarse las diferentes actuaciones posibles, en función de las circunstancias (dentro de la jornada laboral, fuera de la jornada laboral, en caso de una combinación de más de una de las situaciones anteriores, etcétera).

Su estructura normalmente se organizará en base a las diferentes circunstancias extraordinarias que puedan producirse, debiendo aportar soluciones que, en algún caso, también tendrán carácter de excepcionalidad.

Son circunstancias extraordinarias las citadas arriba (incendio o inundación, desastres naturales, inestabilidad social, etcétera), y son soluciones excepcionales la destrucción de la documentación clasificada, o el traslado de la misma a otra zona segura.

5.4.2. Esquema Propuesto de Plan de Emergencia

Se propone el indicado en el Anexo III.

ANEXO I – MODELO DE PLAN DE ACONDICIONAMIENTO

PLAN DE ACONDICIONAMIENTO

1. OBJETO

(Definir la finalidad del plan, y la identificación/definición exacta del Órgano de Control o Zona de Seguridad al que se refiere)

2. SITUACIÓN

(Explicar la localización física del Órgano de Control o Zona de Seguridad dentro del Edificio, Acuartelamiento, Base, Centro, etcétera, en que se encuentre. Si es preciso y relevante, se indicará la situación en el entorno exterior – ciudad, terreno colindante -)

3. PLANOS

(Referencia de los planos, que se incorporarán como anexos al plan; se incluirán los generales de entorno, Base, Zona, Edificio y Planta, con indicación de la situación en los mismos del Órgano de Control o Zona de Seguridad, y se incluirán los planos de detalle de este último, en planta y alzado, con indicación detallada de los elementos relevantes para la seguridad, tanto del propio local, como de los elementos de seguridad adicionales instalados y del mobiliario de seguridad. En este sentido es importante reflejar la situación de sensores, lectores, cámaras CCTV, cajas y armarios de seguridad, destructora de papel, fotocopiadora, mobiliario habitual, disparadores de extinción, etcétera)

4. ENTORNO GLOBAL DE SEGURIDAD

(Se refiere al perímetro o perímetros de seguridad exteriores, que es necesario sobrepasar para llegar a la propia Zona de Acceso Restringido. Se compone de elementos de seguridad tales como elementos estructurales de protección - vallas, iluminación de seguridad, detectores de presencia y paso, circuitos cerrados de TV perimétricos, etc.-, control general de accesos y de identificación, guardias de seguridad, patrullas y fuerzas de reacción)

4.1. Perímetro de Seguridad

(Descripción de altura, construcción, material utilizado y las características empleadas para incrementar su efectividad, así como los elementos instalados en la parte superior del mismo.)

4.2. Sistemas de Detección de Intrusión en el Perímetro (PIDS)

4.2.1. Descripción

(Tipo: barrera de infrarrojos, microondas, campo electromagnético, cable microfónico, tensión mecánica, detector de vibraciones, etc.) funcionamiento, características generales, mantenimiento)

4.2.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en los detectores: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

4.3. Iluminación de Seguridad

4.3.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

4.3.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

4.4. Circuito Cerrado de Televisión (CCTV)

4.4.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

4.4.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en el circuito: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

4.5. Control de Acceso

4.5.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

4.5.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en los detectores: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etc., e indicación del modo de transmisión de alarmas)

4.6. Sistema de Identificación Personal

4.6.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

(En el uso de pases, estos deberán reunir las siguientes características: Llevar un número de serie. Portar identificaciones sucintas que permitan la identificación, especialmente firma y fotografía del titular. No mencionar ni el nombre de la organización a la que permite el acceso ni la habilitación de seguridad del titular. Serán portados de forma bien visible dentro de las zonas de seguridad, con el fin de que el titular pueda ser reconocido e identificado. Se utilizarán códigos de colores o símbolos diferentes para identificar al personal según el nivel de seguridad y necesidad de conocer.)

4.7. Edificio

4.7.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

4.7.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en los detectores: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

4.8. Control de Acceso a Edificios

4.8.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

4.8.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en los detectores: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

5. ENTORNO LOCAL DE SEGURIDAD

(Viene referido a la seguridad inmediata e interior de la propia Zona de Acceso Restringido, por lo que incluye las medidas instaladas en las zonas adyacentes a la misma, en los propios paramentos y accesos, así como en el interior de la propia instalación, impidiendo el acceso a la Información Clasificada allí manejada)

(Se compone de elementos de seguridad tales como elementos estructurales de protección - paramentos de fortaleza adecuada, puertas blindadas, cerraduras de seguridad, etc. - , sistema de control de acceso, detectores de intrusión, cámaras CCTV, cajas y armarios de seguridad)

5.1. Local

5.1.1. Paramentos Horizontales y Verticales

(Descripción de muros, suelo, techo, falsos techos y existencia o no de ventanas o huecos en paramentos, del Local o Área, principalmente de los que constituyen el perímetro, con indicación de su constitución, grosor y fortaleza. Indicación de instalación de sistemas de insonorización)

5.1.2. Ventanas

5.1.3. Descripción

(Características físicas de las ventanas y marcos, con indicación de su constitución y fortaleza. Altura respecto al suelo exterior más próximo y accesibilidad desde el exterior. Visibilidad desde el exterior y elementos para impedir dicha visibilidad. Se hará una descripción para cada ventana cuando sea preciso)

5.1.4. Rejas

(Características físicas, constitución, grosor, paso entre barras, distancias, anclajes a pared, situación)

5.1.5. Sistema(s) de Apertura

(Descripción de los instalados en las ventanas, con sus características de seguridad, modelo, fortaleza)

5.1.6. Sistema(s) de Seguridad

(Descripción de los instalados en las ventanas, para impedir o detectar su apertura no autorizada, o la rotura de cristales, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

5.1.7. Huecos

5.1.8. Descripción

(Características físicas de los huecos, con indicación de su tamaño, forma, situación, accesibilidad desde el exterior. Altura respecto al suelo exterior más próximo. Se hará una descripción para cada ventana cuando sea preciso)

5.1.9. Rejas

(Características físicas, constitución, grosor, paso entre barras, distancias, anclajes a pared, situación)

5.1.10. Sistema(s) de Seguridad

(Descripción de los instalados en cada hueco, para impedir o detectar su paso no autorizada, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

5.2. Puertas de Seguridad

5.2.1. Descripción

(Características físicas de las puertas y marcos, con indicación de su constitución y fortaleza. Se hará una descripción para cada puerta existente)

5.2.2. Sistema(s) de Apertura

(Descripción de los instalados en las puertas, con sus características de seguridad, modelo, fortaleza)

5.2.3. Sistema(s) de Seguridad

(Descripción de los instalados en las puertas, para impedir o detectar su apertura no autorizada, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

5.3. Control de Acceso Local

5.3.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

5.3.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en el sistema de control de accesos: “antipass-back”, alarma antisabotaje, sensor de presencia en esclusas, conexión a sistema alternativo de energía, interfonos, etcétera, e indicación del modo de transmisión de alarmas)

5.4. Sistemas de Detección de Intrusión (IDS)

5.4.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

5.4.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en el sistema IDS: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

5.5. Detector(es) Sísmico(s)

5.5.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

5.5.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en los detectores: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

5.6. Sistema(s) de Circuito Cerrado de TV (CCTV)

5.6.1. Descripción

(Tipo, funcionamiento, características generales, mantenimiento)

5.6.2. Sistema(s) de Seguridad

(Elementos adicionales de seguridad implementados en el sistema CCTV: detección antisabotaje, sistema de autochequeo automático, interconexión con sistema IDS, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

5.7. Mobiliario de Seguridad

5.7.1. Cajas Fuertes, Armarios Blindados, Contenedores de Seguridad

5.7.2. Descripción

(Características físicas, con indicación de su constitución, peso, fortaleza y protección contra el agua y el fuego. Se hará una descripción para cada caja existente)

5.7.3. Sistema(s) de Apertura

(Descripción de los instalados en las puertas, con sus características de seguridad, modelo, fortaleza, número de combinaciones posibles, llaves)

5.7.4. Sistema(s) de Seguridad

(Descripción de los instalados, para impedir o detectar su apertura o traslado no autorizados, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

5.8. Sistemas de Destrucción

5.8.1. Destructoras de Papel

(Tipo, modelo, características de corte, capacidad)

5.8.2. Otros Elementos de Destrucción

(Tipo, modelo, características, capacidad – incluir sistemas de emergencia previstos)

5.9. Medios de Reproducción

(Tipo, modelo, almacenamiento en memoria, identificación de usuario. Se debe conocer si la máquina mantiene datos en memoria tras cada fotocopia realizada; debe configurarse para que no los mantenga, o establecer un procedimiento de borrado en el Plan de Seguridad).

5.10. Sistema Contra-incendios

(Tipo, características)

5.11. Sistema(s) Alternativo de Energía

(Descripción general del sistema y de su utilidad a nivel de la seguridad)

5.12. Otros Elementos de Seguridad Relevantes

(Es posible que existan otras medidas de seguridad instaladas, o llevadas a efecto, en la Zona de Acceso Restringido, de todos ellos se dará información en este apartado).

5.13. Sistema de Protección TEMPEST

5.13.1. Medidas TEMPEST

(Descripción de las medidas TEMPEST adoptadas en los locales y medios instalados)

5.13.2. Medición TEMPEST

(Si el Órgano de Control o Zona de Seguridad ha sido objeto de un medición TEMPEST, indicarlo, con expresión de quien lo ha realizado y los resultados de medición obtenidos – clasificación-)

ANEXO II – MODELO DE PLAN DE SEGURIDAD

PLAN DE SEGURIDAD

1. OBJETO

(Definir la finalidad del Plan de Seguridad. Nivel de clasificación superior de la información que va a ser protegida y manejada, y tipo – OTAN, UE -)

2. ÁMBITO DE APLICACIÓN

(Alcance del plan. Identificación/definición exacta del Órgano de Control o Zona de Seguridad y motivo por el que se constituye. Organismo, Departamento o Unidad al que se da servicio)

3. DEPENDENCIA

3.1.1. Dependencia de Mando

(Identificación del órgano superior, externo al Órgano de Control o Zona de Seguridad, del que se depende a efectos orgánicos o de mando)

3.1.2. Dependencia Funcional

(Identificación del órgano externo del que se depende funcionalmente respecto a protección de la Información Clasificada, dentro de la cadena de la infraestructura de protección)

4. PERSONAL DEL ÓRGANO DE CONTROL O ZONA DE SEGURIDAD

(Descripción de los puestos de trabajo existentes dentro del Órgano de Control o Zona de Seguridad, especialmente los que tengan responsabilidades superiores en seguridad –Jefe de Seguridad, Adjunto, Oficial de Control COSMIC o ATOMAL, etcétera -. No es precisa relación nominal, únicamente la descripción del puesto. En lugares con gran cantidad de personal, se indicará el número de personas por tipos de puestos o similares, destacando sólo los puestos relevantes. Sobre estas personas se llevará el control de acceso diario)

5. PROCEDIMIENTOS DE SEGURIDAD

5.1. Control de Personal

5.1.1. Gestión de Usuarios Autorizados

(Procedimiento para el control, altas y bajas, del personal destinado en el Órgano de Control o Zona de Seguridad o personal autorizado. Mantenimiento de listados. Identificación visual del personal. Procedimiento de gestión de habilitaciones personales de seguridad –HPS-. Posibles restricciones de acceso a la información para determinados puestos.)

5.1.2. Gestión de Personal de Limpieza y Mantenimiento

(Procedimiento para el control, altas y bajas. Mantenimiento de listados. Identificación visual del personal. Escolta. Necesidad de HPS.)

5.1.3. Horario de Trabajo

(Descripción del horario de trabajo, con indicación de tiempos con presencia o no de personal. Procedimiento para permanecer en zona fuera de horas de trabajo y restricciones al respecto. Personal presente las 24 horas. Servicios)

5.1.4. Formación del Personal

(Descripción del procedimiento para mantener la instrucción y concienciación del personal autorizado para acceso a la zona, en materia de seguridad en el manejo y protección de la documentación.)

5.1.5. Registro de entrada y salida aleatorios

(Se realizarán registros aleatorios a la entrada y a la salida concebidos para que actúen como elemento de disuasión para la introducción no autorizada de material o para la retirada no autorizada de Información Clasificada de una zona o de un edificio. Los registros de entrada y salida pueden convertirse en condición para la entrada a un lugar o edificio. Se colocará un aviso en el que se indique que se pueden realizar registros de entrada y de salida.)

5.2. Control de Acceso al Órgano de Control o Zona de Seguridad

5.2.1. Gestión de Usuarios

(Descripción detallada de procedimientos para alta y baja de usuarios, permisos necesarios, control de usuarios, listados, asignación de números de identificación personal, elaboración de tarjetas de acceso, dentro del sistema de control de accesos disponible)

5.2.2. Procedimiento de Acceso

(Descripción detallada del procedimiento a seguir por los usuarios autorizados, para acceder al Órgano de Control o Zona de Seguridad, con indicación explícita de la forma de evitar la mala práctica de que personas autorizadas permitan el acceso a otras, no quedando registrado su acceso. Explicar cómo se realiza la identificación del usuario. Acceso fuera de horario de trabajo y control de dichos accesos)

5.2.3. Gestión de Seguridad

(Descripción detallada del procedimiento de control y auditoría de accesos, responsabilidades en este aspecto, actuación ante pérdidas de tarjetas o revelación de número personal)

5.2.4. Visitas

(Descripción detallada del procedimiento de control de acceso para la visitas. Indicar si están permitidas o no, o en qué circunstancias se permiten. Existencia de Libro de Registro de Visitas y procedimiento para cumplimentarlo. Procedimiento de identificación y escolta de visitas)

5.3. Control de Llaves

(Descripción detallada del procedimiento para su manejo, control, sustitución, registro de cambios de cerraduras, actuación ante pérdidas, custodia durante y después del trabajo. Si existen diferencias, se indicará el procedimiento para cada llave que tenga un tratamiento diferente –normalmente no tendrá el mismo trato la llave de la puerta que la llave de la caja fuerte-)

5.4. Control de Claves de Combinación

(Descripción detallada del procedimiento para su manejo, control, sustitución, registro de cambios de claves y motivos, actuación ante pérdidas o comprometimientos, actuación por cambio de personal, custodia segura de claves para emergencias)

5.5. Activación Sistema IDS y Sensores

(Descripción detallada del procedimiento y horario, o eventos necesarios, para su activación/desactivación. Verificación diaria de funcionamiento. Posibles tiempos muertos sin cobertura. Activación a final de jornada. Desactivación a principio de jornada. Otras activaciones/desactivaciones)

5.6. Actuación ante Alarmas

5.6.1. Sistema de Recepción de Alarmas

(Descripción detallada del procedimiento para la transmisión y recepción de alarmas. Verificación diaria de funcionamiento)

5.6.2. Actuación ante Alarmas

(Actuación del Centro de Recepción de Alarmas. Procedimiento para la comunicación y actuación del personal implicado en la respuesta – guardia, fuerzas de reacción, responsables de seguridad. Tiempos de respuesta. Ensayos de alarma)

5.7. Guardia de Seguridad

(Descripción detallada de los apoyos en seguridad prestados, por el personal de guardia o servicio de vigilancia, que afectan directamente a la seguridad del Órgano de Control o Zona de Seguridad, en forma de rondas, inspecciones a fin de jornada, vigilancia exterior, etcétera)

5.8. Cortes de Energía

(Descripción detallada del procedimiento de actuación ante un corte de energía, en función de los sistemas alternativos existentes. Normas de protección especiales a adoptar en caso de fallos que afecten a los sistemas: sensores, IDS, control de accesos)

5.9. Control de la Documentación

5.9.1. Control Documental

(Descripción detallada de la forma en que se realiza el registro de entrada y salida, y la distribución de documentos. Movimiento y traslado de documentación clasificada. Tratamiento de mensajes. Tratamiento de documentos clasificados recibidos por canales no habituales. Copias de seguridad de los registros y almacenamiento de las mismas en local diferente)

5.9.2. Procedimiento de Almacenado

(Descripción detallada de la forma en que se almacena la Información Clasificada en los contenedores, cajas fuertes o armarios blindados. Criterios de almacenamiento. Separación en contenedores diferentes de la Información Clasificada de diferentes tipos –OTAN, UE -. Separación por niveles de clasificación)

5.9.3. Procedimiento de Acceso

(Descripción detallada del procedimiento de acceso a la documentación almacenada por parte del personal autorizado, distinguiendo entre el propio personal destinado en el Órgano de Control o Zona de Seguridad, y el que, sin estarlo, tiene la necesidad de conocer, está habilitado y es autorizado para acceder a dicha información. Existencia de salas de lectura. Criterios para que un usuario pueda retirar Información Clasificada y condiciones –bajo responsabilidad del Jefe de Seguridad y cumpliendo la normativa vigente-)

5.9.4. Procedimiento de Reproducción

(Descripción detallada del procedimiento de fotocopiado de documentos clasificados. Personal autorizado. Registro de copias)

5.9.5. Procedimiento de Destrucción

(Descripción detallada del procedimiento para la destrucción ordinaria de la Información Clasificada. Responsabilidades. Testigos)

5.10. Lista de Comprobación Diaria

(Lista detallada de las tareas diarias de comprobación que de forma automática, aunque con atención, deben realizarse al inicio y final de jornada para verificar que las condiciones de seguridad están establecidas y no ha habido ninguna violación de las mismas)

5.11. Informes de Violaciones o Comprometimientos

(Procedimientos y canales de comunicación de posibles comprometimientos de la Información Clasificada o de violaciones de la seguridad)

5.12. Otros Procedimientos de Seguridad Relevantes

(Se indicará cualesquiera otros que sean precisos para definir de forma exhaustiva la seguridad implantada, y que no tengan encaje en los puntos anteriores)

ANEXO III – MODELO DE PLAN DE EMERGENCIA

PLAN DE EMERGENCIA

1. OBJETO

(Definir la finalidad del Plan de Emergencia)

2. TIPOS DE EMERGENCIA

(Enumeración esquemática de los diferentes tipos de emergencia que se van a considerar en este plan. Se pueden clasificar por diferentes criterios, o combinaciones de varios:

- Tipo: incendio, inundación, acto terrorista, disturbios
- Continuidad: abandono del local, aumento de medidas de protección por imposibilidad de abandono.
- Consecuencias: material clasificado afectado, no afecta al material.)

3. PROCEDIMIENTOS GENERALES DE ACTUACIÓN

3.1. Actuación al producirse la Emergencia

3.1.1. En horario de Trabajo

(Procedimientos generales a seguir. Determinación del tipo de emergencia. Responsable de inicio de actuaciones. Guardado de la información. Cierre de contenedores. Evacuación del personal. Avisos. Teléfonos de emergencias)

3.1.2. Fuera de horario de Trabajo

(Procedimientos generales a seguir. Avisos necesarios. Actuación primera de los servicios de vigilancia. Responsabilidades. Criterios de acceso a la zona clasificada. Teléfonos de emergencias)

3.2. Actuaciones posteriores

3.2.1. Traslado de la Documentación Clasificada

(Criterios para adoptar la decisión del traslado. Responsabilidades. Prioridades. Procedimientos generales a seguir en caso de que se decida esta actuación. Instalaciones previstas. Itinerarios y planos de evacuación. Medios. Avisos. Recuentos. Actas del movimiento)

3.2.2. Destrucción de la Documentación Clasificada

(Procedimientos generales a seguir en caso de que se decida esta actuación. Responsabilidades. Criterios. Prioridades. Medios. Avisos. Lugares alternativos previstos para la destrucción masiva)

3.2.3. Evaluación de daños e informes

(Procedimiento para el recuento de la Información Clasificada, análisis de pérdidas, certificados de destrucción, informes de comprometimientos y pérdidas)

3.2.4. Vuelta a la situación inicial

(Procedimientos generales a seguir y requisitos a cumplir, una vez finalizada la situación de emergencia, para la vuelta a la situación inicial. Mecanismos de recuperación de la información. Condiciones de seguridad mínimos necesarios)

4. PROCEDIMIENTOS PARTICULARES DE ACTUACIÓN

(Descripción, para cada tipo de emergencia considerado, de las actuaciones, complementarias o más detalladas, que las generales indicadas anteriormente, que sería preciso ejecutar para asegurar la protección de la Información Clasificada)