GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

GUÍA DE BUENAS PRÁCTICAS

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

PLAN DE PROTECCION ESPECÍFICO (PPE)

1. INTRODUCCIÓN

1.1 BASE LEGAL

Según establece la Ley 08/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico se integrará como agente del sistema de protección de infraestructuras críticas, debiendo cumplir con una serie de responsabilidades recogidas en su artículo 13. De acuerdo con en el punto 1, letra "d", del citado artículo, el operador deberá elaborar un Plan de Protección Específico (en adelante PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor.

El Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, a través del cual se da desarrollo reglamentario a la Ley 08/2011, en su capítulo IV del Título III sobre los *Instrumentos de Planificación*, establece aquellos aspectos relativos a la elaboración, finalidad y contenido de dichos planes, formas de revisión y actualización, autoridades encargadas de su aplicación y seguimiento y compatibilidad con otros planes ya existentes.

En este sentido, y conforme al artículo 25.5 de dicho Real Decreto, el Secretario de Estado de Seguridad estableció, mediante Resolución de fecha 15 de noviembre de 2011 y su modificación con Resolución de fecha 29 de noviembre de 2011, los Contenidos Mínimos con los que debe contar todo PPE, así como el modelo en el que fundamentar su estructura y compleción.

En el PPE, el Operador Crítico (en adelante OC) público o privado recogerá de forma ***práctica*** los siguientes aspectos y criterios incluidos en su Plan de Seguridad del Operador (en adelante PSO), que afectan de manera específica a esa instalación:

- Aspectos relativos a su política general de seguridad.
- Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica.
- Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como lógicas, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

1.2 OBJETIVO DE ESTE DOCUMENTO

Con el presente documento se pretende orientar a aquellos operadores designados como críticos en la elaboración de sus PPEs, sirviendo como complemento a las Resoluciones del Secretario de Estado de Seguridad sobre Contenidos Mínimos del PPE. Por lo tanto, se trata de un documento de carácter voluntario que no incluye requisitos adicionales a los establecidos por la legislación vigente o por las Resoluciones mencionadas previamente. Para facilitar la aplicación de estas buenas prácticas se han incluido diferentes ejemplos en este documento.

En esta guía se incluyen una serie de Anexos (detalle de medidas organizativas o gestión, operacionales o procedimentales, protección o técnicas, etc.) que podrán ser referentes de ayuda a los operadores críticos para la confección de alguno de los puntos de los contenidos mínimos del PPE.

1.3 PROTECCIÓN DE LA INFORMACIÓN

Tras la aprobación del PPE, su grado de clasificación será, como se sabe, de Difusión Limitada, debiendo el Operador Crítico definir sus procedimientos de gestión y tratamiento de la información conforme a unos estándares de seguridad que garanticen una adecuada y eficaz protección de dicha información.

Para ello, el OC tomará como referencia las orientaciones dictadas por la Autoridad Nacional de Seguridad, entre las que cabe destacar[1]:

- Seguridad documental
  - OR-ASIP-04-01.03 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.
- Seguridad en el personal
  - OR-ASIP-02-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.
- Seguridad física
  - OR-ASIP-01-01.02 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.
  - OR-ASIP-01-02.02 – Orientaciones para la Constitución de Zonas de Acceso Restringido.

[1] Los documentos mencionados pueden consultarse en la dirección: http://www.cni.es/es/ons/documentacion/normativa/

2. ASPECTOS ORGANIZATIVOS

2.1 DELEGADOS DE SEGURIDAD DE LAS INFRAESTRUCTURAS CRÍTICAS

El operador aportará la información solicitada en este apartado conforme a lo establecido en el documento de contenidos mínimos del PPE, siendo recomendable también informar de los mecanismos de contingencia y continuidad adoptados para garantizar la comunicación con el Delegado de Seguridad en caso de incidentes o que dicha persona se vea afectada por cualquier tipo de suceso adverso que no le permitan estar accesible, así como los canales de coordinación existentes con los distintos actores afectados (incluyendo FFCCS y CNPIC).

En cuanto a la formación que deberá reflejar, en función del Plan de Formación, debería incluir aspectos tanto técnicos, como de gestión en el ámbito de la seguridad y, en sus dos dimensiones más tradicionales (física y lógica). Sería recomendable incluir la formación que ha recibido de acuerdo con lo previsto en el Plan de Formación recogido en el PSO.

2.2 MECANISMOS DE COORDINACIÓN

Para clarificar los mecanismos de coordinación establecidos en relación a la IC conforme a lo establecido en el documento de contenidos mínimos del PPE, se recomienda identificar, en primer lugar, todos aquellos interlocutores con los que se debe establecer relación en el ámbito de la protección de las IICC, tanto dentro como fuera de la propia infraestructura.

A continuación, se debería recoger para cada uno de ellos, tanto el mecanismo de comunicación principal como el secundario para casos de contingencias (canales que deberían ser probados periódicamente, como es lógico).

Asimismo, se deberían reflejar también las reuniones, comités, protocolos y cualquier otro mecanismo que se emplee para la coordinación con dichos organismos / roles, así como los procedimientos de actuación previstos ante las distintas situaciones críticas o extraordinarias con el objetivo de minimizar el impacto de estas eventualidades.

Finalmente, sería conveniente desarrollar planes de comunicación para mantener informados de las novedades a cada uno de los niveles de responsabilidad y funcionalidad entre los distintos actores.

2.3 MECANISMOS Y RESPONSABLES DE APROBACIÓN

Al igual que para otros tipos de políticas y procedimientos se debería recoger el procedimiento que se utiliza para la aprobación del propio PPE, es decir:

- Quién es el responsable de su aprobación.
- Quién es el responsable de su revisión y actualización si fuera necesario.
- Cuáles son los pasos para su aprobación y a quién se comunican las modificaciones en el plan (incluyendo cualquier tercero afectado por dichas modificaciones).
- Periodicidad con la que se revisa el Plan (que debe cumplir, en cualquier caso, con los requisitos legales establecidos) y fecha de la última revisión.
- Aspectos que serán objeto de revisión.
- Registros generados por el procedimiento de revisión que permitirán comprobar que el Plan ha sido revisado, aunque no se haya traducido en modificaciones del plan (reuniones, actas del Comité correspondiente, estudios y análisis realizados, actualizaciones de los análisis de riesgos, etc.).

3. DESCRIPCIÓN DE LA INFRAESTRUCTURA CRÍTICA

3.1 DATOS GENERALES

El Operador Crítico, a modo de introducción de la Infraestructura Crítica, debería incluir al menos la información de contexto suficiente para describir los siguientes aspectos:

- Información de carácter estratégico.
  - ✓ Descripción del servicio esencial que soporta y ámbito geográfico del mismo.
  - ✓ Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.
    - Del mismo sector.
    - De otros sectores.
  - ✓ Descripción de sus funciones y de su relación con los servicios esenciales soportados.

- Información de carácter general.
  - ✓ Denominación y tipo de instalación.
  - ✓ Descripción general de la infraestructura a proteger.
  - ✓ Propiedad y gestión de la Infraestructura Crítica.

- Localización física y estructura de la infraestructura a proteger.
  - ✓ Ubicación geográfica de la infraestructura.

- ✓ Planos generales de la infraestructura con referencia a todos los elementos, así como su ubicación relativa y absoluta.
- ✓ Fotografías relevantes de la infraestructura y los elementos que la componen.
- ✓ Componentes (Edificios/Instalaciones/etc.).

- Sistemas TIC y arquitectura.
  - ✓ Mapa de red y comunicaciones.
  - ✓ Mapa de sistemas y servicios.
  - ✓ Sistemas de control.

3.2 ACTIVOS / ELEMENTOS

Se debería realizar una descripción de los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son y detallando las dependencias existentes entre ellos. La información que se podría incluir al menos sería la enumerada a continuación:

- Medios materiales y recursos necesarios para la prestación del servicio esencial.
  - ✓ Componentes de la Infraestructura Crítica.
  - ✓ Ubicación de los centros de procesamiento de datos (CPD) que gestionan los diferentes elementos que conforman la Infraestructura Crítica.
  - ✓ Sistemas informáticos (hardware y software) utilizados.
    - Relación de sistemas (HW/SW).
    - Versiones.
    - Redes de comunicaciones que se utilizan para dicha IC. Tipos.

- Medios personales para la prestación del servicio esencial.
  - ✓ Tipología.
  - ✓ Volumen.

- Relación de la IC con los servicios esenciales prestados por el operador.

- Servicios críticos que son necesarios para el funcionamiento de dicha IC (emergencias, abastecimiento, etc.).

- Usuarios finales de los servicios prestados por la IC (particulares, empresas, Sector público…).

3.3 INTERDEPENDENCIAS

Se debería realizar una descripción y el motivo que origina las posibles interdependencias entre servicios esenciales e infraestructuras críticas propias, así como, con las de otros operadores dentro del mismo sector o diferente, que deban ser consideradas en el análisis de riesgos en el marco global de la organización. En este sentido hay que tener en cuenta el análisis de riesgo del marco global de la organización así como el modo en que afectan al servicio, analizando las posibles dependencias de entrada, de salida y de proceso, sin olvidar tanto el ámbito interno como externo a la organización de la dependencia. Algunos ejemplos de interdependencias serían:

- Entre los servicios esenciales: Del propio operador y/o otros Operadores nacionales o extranjeros del mismo o distinto sector.
- Entre infraestructuras: Del propio operador y/o otros Operadores nacionales o extranjeros del mismo o distinto sector.
- Con sus proveedores dentro de la cadena de suministros.
- Etc.

4. RESULTADOS DEL ANÁLISIS DE RIESGOS

4.1 AMENAZAS CONSIDERADAS

Para el análisis de riesgos a realizar se podrían tomar como punto de partida diferentes tipologías de amenazas que están definidas en diferentes catálogos existentes o referentes a nivel nacional o internacional.

En ese sentido, se deben analizar las principales amenazas que pudieran tener un origen intencionado por parte de terceras partes diferentes a los propios operadores y que pudieran afectar a los activos de tipo lógico como de tipo físico.

Los OC y resto de agentes con un interés legítimo podrán dirigirse al CNPIC para obtener una modelización típica de amenazas que podrá ser utilizada a modo de guía para la realización de esta actividad.

4.2 MEDIDAS EXISTENTES

Se entiende por medidas de seguridad, las medidas de protección de los activos. Estas medidas podrán ser, permanentes, temporales y graduales.

En las secciones siguientes se proporcionan recomendaciones y ejemplos generales a partir de los cuales se podría estructurar la seguridad integral de los servicios esenciales

y las infraestructuras críticas de las que ellos dependen. La lista de ejemplos proporcionada no es exhaustiva, pero puede servir de punto de partida para organizar las necesidades de protección del entorno concreto de protección para el que sean aplicables.

El Operador deberá describir las medidas de seguridad integral actualmente implantadas en línea con el análisis de riesgos realizado. Se recomienda seguir una organización de las medidas en tres niveles:

- Medidas organizativas o de gestión
- Medidas operacionales o procedimentales
- Medidas de protección o técnicas.

En general las medidas a implementar, o implementadas, deberán ser acordes con la Legislación vigente y aplicable, tanto en lo que respecta a la documentación exigible, como a la instalación y mantenimiento.

4.2.1 Organizativas o de gestión

Todas las organizaciones tienen una función, misión o negocio, que determina sus objetivos (qué hay que conseguir) y estrategias (cómo hay que conseguirlo). Es por ello que la seguridad integral de una organización debería alinearse para garantizar la consecución de los mismos.

Las medidas organizativas son el conjunto de medidas de seguridad embebidas en los procesos y estructuras organizativas existentes en la organización y cuyo objetivo principal es gestionar la complejidad de los procesos de gestión de la seguridad y dar respuesta a los riesgos, condicionantes normativos y regulatorios del entorno.

En el Anexo I (apartado 7.1) se incluye información adicional sobre las siguientes medidas organizativas o de gestión que se pueden establecer:

- Definición de un cuerpo normativo
- Organización de la seguridad
  - ✓ Comité de Seguridad y Crisis
  - ✓ Establecimiento de roles
  - ✓ Gestión de cambios
  - ✓ Gestión de la calidad y de la documentación
- Medios Humanos y seguridad del personal
  - ✓ Formación y Concienciación
  - ✓ Protección del personal.

4.2.2 Operacionales o procedimentales

Derivados del cuerpo normativo establecido en la organización, las buenas prácticas recomiendan la documentación del conjunto indispensable de procedimientos operacionales o procedimentales con su alcance concreto que permita realizar una gestión integral del proceso de seguridad y la adecuada gestión de los controles implantados. Todo ello con el objetivo de lograr la eficacia y la eficiencia de los mismos acorde con los riesgos contemplados y la racionalidad y proporcionalidad de la protección requerida.

En el Anexo (apartado 7.2) se describen los procedimientos de alto nivel que engloban la tipología de controles que son aconsejables acordes con las buenas prácticas de seguridad. En concreto, en dicho anexo se incluye información sobre los siguientes:

- Procedimientos de gestión de activos
- Gestión de la formación y la concienciación
- Gestión de la continuidad
- Supervisión continua y monitorización
- Gestión de accesos
- Gestión de evacuación y emergencias
- Gestión de la información
- Gestión de la respuesta, incidentes y escalado
  - ✓ Procedimiento para la catalogación de incidentes
  - ✓ Procedimiento para el escalado de incidentes
  - ✓ Procedimiento para la respuesta a incidentes
- Gestión del conocimiento
- Revisión.

4.2.3 De protección o técnicas

Las medidas de protección o técnicas hacen referencia a aquellos conjuntos de controles de carácter técnico necesariamente implantados en la organización para conseguir un nivel de riesgo aceptable. La forma más recomendable de implementación es mediante el establecimiento de medidas automatizadas que permitan crear registros de evidencias fiables.

A continuación, de forma no exhaustiva, se proporciona un conjunto de ejemplos de alto nivel de controles y medidas agrupadas conforme a lo que consideramos criterios prácticos: facilidad de lectura, catalogación y naturaleza de las medidas. Estas agrupaciones de controles tienen por objeto el facilitar su inclusión en un ciclo de gestión continua de la seguridad que permita mayor eficacia y eficiencia en la implementación y mantenimiento de la seguridad. Ello no quita que algunas de las medidas pudieran ser

clasificadas en más de un grupo. No obstante, el objetivo es facilitar su identificación y comprensión de forma general para, conforme a las necesidades, aplicar medidas más concretas derivadas o relacionadas con las mismas. Por ejemplo, si se indica de forma general medidas de control de perímetro de seguridad hay varios grupos de medidas que pueden ser implantados conforme a las necesidades de defensa en profundidad: hipotéticamente conforme a los riesgos sería necesario implementar una valla, un volumétrico y una cámara de video vigilancia; adicionalmente para la protección del perímetro lógico sería necesaria la segmentación de la red, la creación de una DMZ, la aplicación de reglas de firewall y de sistemas de detección de intrusiones, etc.

Para organizar un ciclo de gestión continua de la seguridad las agrupaciones propuestas, son las siguientes:

- Prevención y Detección
- Vigilancia y Monitorización
- Coordinación y Respuesta
- Continuidad y Contingencia.

En el Anexo I (apartado 7.3) se incluye información adicional sobre cada uno de los tipos de medidas que se pueden aplicar en cada caso.

4.3 VALORACIÓN DE RIESGOS

A partir de la selección de las diferentes medidas de seguridad que hayan sido implantadas se procederá a estimar el riesgo residual al que se encuentra expuesta una infraestructura. Para poder proceder a dicha estimación se deberá tener en consideración el grado de implantación de cada una de esas medidas de seguridad, es decir, habría que evaluar si:

- Están correctamente implantadas
- Están operativas
- Están procedimentadas
- Están bajo un sistema de gestión y mejora continua
- Son objeto de pruebas regulares para verificar su correcto funcionamiento y que el personal encargado de usarlas está formado en sus funciones y responde en los tiempos previstos.

Para determinar el cálculo final de los riesgos a los que se encuentra expuesta la infraestructura se deberían tomar en consideración las probabilidades que existen de que el conjunto de amenazas identificadas puedan llegar a afectar a la infraestructura, así como el potencial impacto que podrían provocar. A partir de ese cálculo se debería

contemplar la reducción del riesgo a partir de las medidas de seguridad que se hayan podido implantar, ya sea por la reducción en las probabilidades de que llegaran a suceder o bien por la reducción del impacto que provocaría esa determinada amenaza en el supuesto que se materializara.

Se deben diferenciar en este análisis los diferentes escenarios de la IC, así como, en su caso, los diferentes horarios de su funcionamiento (instalación ocupada o no, etc.).

En cualquier caso, dado el enfoque de protección de los servicios esenciales que se persigue, deberá prestarse especial atención a las amenazas de alto impacto y baja probabilidad que pudieran afectar al servicio esencial y dotarse de las medidas de protección pertinentes.

Con el objetivo de mostrar la información de la valoración de riesgos realizada se podrían elaborar dos tablas similares a las siguientes que resumen los principales datos del análisis:

1. Para los activos con niveles de riesgo altos o muy altos

Activos	Amenaza	Riesgo intrínseco			Controles existentes	Riesgo residual		
		Probabilidad	Impacto	Riesgo		Probabilidad	Impacto	Riesgo

2. Para los activos con niveles de impacto altos o muy altos

Activos	Amenaza	Riesgo intrínseco		Controles existentes	Riesgo residual	
		Probabilidad	Riesgo		Probabilidad	Riesgo

La interpretación de la información recogida en las tablas previas es la siguiente:

- Activo. Elemento / componente de la infraestructura crítica.
- Amenaza. Suceso que puede afectar al funcionamiento o a la disponibilidad del activo y, por tanto, del servicio esencial.
- Riesgo intrínseco. Análisis realizado con carácter previo a la aplicación de medidas de seguridad.
  - ✓ Probabilidad. Posibilidad de que la amenaza se materialice sobre el activo.
  - ✓ Impacto. Estimación de las consecuencias de la ocurrencia de la amenaza (está ligado al valor del activo).
  - ✓ Riesgo. Resultado de la combinación de los valores previos de probabilidad e impacto.

- Controles existentes. Medidas de seguridad que se aplican en la actualidad y que reducen, bien la probabilidad, bien el impacto.
- Riesgo residual. Análisis realizado considerando ya los controles aplicados. Por lo tanto, deberán ser valores inferiores a los intrínsecos.
  - ✓ Probabilidad. Posibilidad de que la amenaza se materialice considerando las medidas de seguridad existentes (solo las medidas preventivas reducen la probabilidad).
  - ✓ Impacto. Estimación de las consecuencias de la ocurrencia de la amenaza, considerando las medidas de seguridad aplicadas (solo las medidas de detección y las correctivas reducen el impacto).
  - ✓ Riesgo. Resultado de los valores de probabilidad e impacto residuales previos.

5. PLAN DE ACCIÓN PROPUESTO

El Plan de Acción consiste en la planificación completa para la implementación de las medidas de seguridad identificadas en el análisis de riesgos de la infraestructura crítica como necesarias para complementar las existentes en la actualidad, de forma que puedan establecerse unos hitos y fechas para su implementación.

El Plan de Acción se constituye en un número de acciones dónde se agruparían las medidas de seguridad de índole organizativa, operacional y técnica, que se deberían implantar, monitorizar y gestionar para afrontar los riesgos detectados.

El Plan de Acción es parte del PPE y debería ser implementado en el plazo máximo de tres años. Su revisión se debería realizar basándose siempre en un análisis de riesgos previo.

El Plan de Acción se debería recoger los siguientes requisitos:

- Priorizar las acciones, en base al nivel de riesgo asociado, atendiendo a las posibles dependencias existentes entre ellas.
- Estructurar las distintas medidas de seguridad, asociándolas en base a su finalidad y naturaleza, en acciones que resulten acotadas y viables.
- Asignar responsabilidades en la implantación de las acciones.
- Realizar una planificación completa y detallada donde se incluya la estimación sobre las inversiones y los plazos necesarios para su implantación.
- Establecer un mecanismo de seguimiento por medio de métricas que permita conocer el estado de las acciones.

A cada medida de seguridad resultante del análisis de riesgos, el Operador Crítico debería asignarle un nivel de prioridad de cara a la reducción del riesgo que la implantación de esta medida de seguridad provocaría en la evaluación general de los riesgos que afectan a la Infraestructura Crítica.

En base al nivel de prioridad asignado a una determinada medida de seguridad, el Operador Crítico podría priorizar la implantación de las medidas en forma de acciones.

5.1 ACCIONES

Las acciones abarcan un conjunto de medidas de seguridad que se deberán implementar conjuntamente.

El Operador Crítico podría definir, para cada acción, los siguientes datos:

- Identificación de la Acción: Consiste en un código único y un nombre descriptivo para la acción.
- Objetivos: Especificación, incluyendo ámbito y alcance, de la finalidad hacia la que se orienta el conjunto de medidas de seguridad que componen la acción y la reducción del riesgo esperado a la implantación de ésta.
- Descripción: Resumen de los contenidos e implicaciones de la acción de manera descriptiva.
- Responsable: Identifica el departamento o persona al cargo de la ejecución de la acción.
- Dependencias: Refleja las posibles relaciones existentes entre otras acciones y la que se desarrolla.
- Activos: Activos sobre los que se aplica la acción.
    - ✓ Identificador del Activo: Consiste en un código único y un nombre descriptivo para el activo.
    - ✓ Tipología del Activo: Define la tipología del activo sobre el que se aplica la acción. Ésta podría ser, por ejemplo:
        - Instalaciones de la IC necesarias para la prestación del servicio esencial. (Código: INS).
        - Sistemas informáticos, ya sean hardware o software. (Código: SI).
        - Redes de comunicaciones que se utilicen en dicha IC. (Código: RED).
        - Personas que explotan u operan con los activos anteriormente citados. (Código: PER).
        - Proveedores críticos que son necesarios para el funcionamiento de la IC. (Código: PRO).

- ✓ Responsable del Activo: Responsable a cargo del activo sobre el cual se aplica la acción.

- Listado de las medidas de seguridad: Recoge las distintas medidas de seguridad agrupadas como parte integrante de la acción. el responsable de dicha medida de seguridad y su tipología.
- Inversión estimada: Estimación de coste de la acción, basado en la experiencia en presupuestos para acciones previas, análogas y en entornos similares. Se adjuntará además un breve desglose del esfuerzo en recursos estimado, así como las tecnologías y soluciones que se han tenido en consideración.
- Estimación temporal: Fecha en la que está previsto que se desarrollará la acción.
- Mecanismos de coordinación y seguimiento: Mecanismos que se aplicarán para la coordinación y seguimiento en la ejecución de la acción sobre uno o varios activos.

Tabla 1. Ejemplo de ficha de activo

IDENTIFICADOR DE LA ACCIÓN:		
CÓDIGO ÚNICO NOMBRE DESCRIPTIVO		
OBJETIVO:		
ESPECIFICACIÓN DE LA FINALIDAD DE LA ACCIÓN.		
DESCRIPCIÓN:		
DESCRIPCIÓN DE LA ACCIÓN.		
RESPONSABLE:		
RESPONSABLE DE LA ACCIÓN.		
DEPENDENCIAS CON OTRAS ACCIONES:		
ACCIONES CON LAS QUE ÉSTA GUARDA RELACIÓN.		
Activos		
Identificador:	Responsable:	Tipología:
Identificador del Activo 1 (Código y Nombre Descriptivo)	Responsable del Activo 1	INS / SI / RED / PER / PRO
Identificador del Activo 2	Responsable del Activo 2	INS / SI / RED / PER / PRO
Medidas de Seguridad		
Identificador:	Responsable:	Tipología y Carácter
Medida de seguridad 1.	Responsable de la medida de seguridad 1.	Organizativa / Operacional / Técnica Permanente / Gradual
Medida de seguridad 2.	Responsable de la medida de seguridad 2.	Organizativa / Operacional / Técnica Permanente / Gradual
MECANISMOS DE COORDINACIÓN Y SEGUIMIENTO:		
MECANISMOS PARA LA ACCIÓN.		
INVERSIÓN:	ESTIMACIÓN TEMPORAL:	
ESTIMACIÓN DEL COSTE DE LA ACCIÓN.		

5.2 MEDIDAS DE SEGURIDAD

La consecución de una acción va ligada a la aplicación ordenada de una o múltiples medidas de seguridad que pueden interrelacionarse. Las medidas de seguridad pueden segmentarse en tareas atómicas que conducen a la consecución de la medida de seguridad.

Para la definición apropiada de las medidas de seguridad se podrían definir los siguientes datos:

- Identificación de la medida de seguridad: Consistente en un código único y un nombre descriptivo de la medida de seguridad.
- Descripción: Resume los contenidos e implicaciones de la medida de seguridad de manera descriptiva.
- Responsable: Identifica el departamento o persona al cargo de la ejecución de la medida de seguridad.
- Identificación de la Acción: Muestra la acción en la que se engloba la medida de seguridad.
- Criticidad: Marca el nivel de importancia de la medida de seguridad. La ejecución de una medida de seguridad de nivel de criticidad más alto tendrá un mayor impacto en la gestión de riesgos.
- Carácter: El carácter distingue entre medida de seguridad permanente o gradual.
  - ✓ Permanente: Medida de seguridad que se aplica en cualquier circunstancia.
  - ✓ Gradual: Se activará en función de los distintos niveles de amenaza. Se deberá indicar las circunstancias de activación.
- Tipología: La tipología de la medida de seguridad será relativa a las siguientes.
  - ✓ Organizativas o de Gestión.
  - ✓ Operacionales o Procedimentales.
  - ✓ De Protección o Técnicas.
- Activos: Activos sobre los que se aplica la medida de seguridad.
  - ✓ Identificador: Consiste en un código único y un nombre descriptivo del activo.
  - ✓ Responsable: Responsable a cargo del activo sobre el cual se aplica la medida de seguridad.
  - ✓ Tipología: Define la tipología del activo:
    - Instalaciones de la IC necesarias para la prestación del servicio esencial. (Código: INS).
    - Sistemas informáticos, ya sean hardware o software. (Código: SI).
    - Redes de comunicaciones que se utilicen en dicha IC. (Código: RED).
    - Personas que explotan u operan con los activos anteriormente citados. (Código: PER).

- Proveedores críticos que son necesarios para el funcionamiento de la IC. (Código: PRO).

- Listado de tareas: Recoge las diferentes tareas unitarias a desarrollar que podrían considerarse necesarias, si bien no suficientes, para la consecución de la medida de seguridad. Así como una descripción de dicha tarea.

- **Tabla 2. Ejemplo de Medida de seguridad**

IDENTIFICADOR DE LA MEDIDA DE SEGURIDAD:		
CÓDIGO ÚNICO NOMBRE DESCRIPTIVO		
DESCRIPCIÓN:		
DESCRIPCIÓN DE LA MEDIDA DE SEGURIDAD.		
RESPONSABLE		
RESPONSABLE DE LA MEDIDA DE SEGURIDAD.		
ACCIÓN:		
IDENTIFICADOR DE LA ACCIÓN QUE ENGLOBA ESTA MEDIDA DE SEGURIDAD.		
CRITICIDAD:	CARÁCTER:	TIPOLOGÍA:
NIVEL DE CRITICIDAD.	☐PERMANENTE ☐ TEMPORAL / GRADUAL NIVEL DE AMENAZA INDICA EL NIVEL DE AMENAZA O CIRCUNSTANCIA PARA LA ACTIVACIÓN DE LA MEDIDA TEMPORAL O GRADUAL.	ORGANIZATIVA O DE GESTIÓN / OPERACIONAL O PROCEDIMENTAL / DE PROTECCIÓN O TÉCNICA.
Activos		
Identificador:	Responsable:	Tipología:
Identificador del Activo 1 (Código y Nombre Descriptivo)	Responsable del Activo 1	INS / SI / RED / PER / PRO
Identificador del Activo 2	Responsable del Activo 2	INS / SI / RED / PER / PRO
TAREAS:		
Tarea 1: Descripción de la tarea 1. Tarea 2: Descripción de la tarea 2.		

6. DOCUMENTACIÓN COMPLEMENTARIA

El Operador Crítico incorporará como Anexo la planimetría general de la instalación, así como, aquellos otros planos que incorporen la ubicación de las medidas de seguridad implementadas. A su vez, se podrá adjuntar aquella otra información que se pueda generar de los diferentes apartados de este documento.

Se hará una breve referencia a todos aquellos planes de diferente tipo (emergencia, autoprotección, etc.), que afecte a la instalación con el fin de establecer una adecuada coordinación entre ellos, así como, todo aquella normativa y buenas prácticas que regulen el buen funcionamiento del servicio esencial prestado por esa infraestructura y los motivos por los cuales le son de aplicación.

Las normativas a incluir comprenden tanto las de rangos nacionales, autonómicos, europeos e internacionales, como las sectoriales, relativos:

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Información en cualquiera de sus ámbitos.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

-----oo00oo-----

7. ANEXO I. DETALLE DE MEDIDAS DE SEGURIDAD

7.1 DETALLE DE MEDIDAS ORGANIZATIVAS O DE GESTIÓN

7.1.1 Cuerpo normativo definido

Es aconsejable establecer los procesos de seguridad para que den cabida al cumplimiento normativo, voluntario y regulatorio que afecta a la organización y sus activos. Por eso es conveniente Identificarlo controles de seguridad derivados de la normativa identificada en el PSO y las normativas o reglamentaciones aplicables al PPE.
Generalmente suelen ser aplicables los siguientes conjuntos de procesos en la definición y estructuración del cuerpo normativo:

- Relación con normativa interna y corporativa.
- Seguridad Física.
- Protección civil.
- Seguridad Ambiental.
- Seguridad Personal.
- Seguridad Autoprotección y Prevención de Riesgos Laborales.
- Seguridad Lógica y de la información.

Para ello es necesario organizar de forma manejable, proporcionada y documentada toda la información sobre los controles y medidas de seguridad implementadas o que deberían serlo acorde al tratamiento de riesgos.
A alto nivel esta organización suele incluir:

- Políticas y estándares de Seguridad.
- Criterios de Seguridad.
- Procedimientos.
- Cumplimiento Normas y/o regulaciones de aplicación a la infraestructura crítica, así como identificación de su nivel de cumplimiento.
- Certificaciones, acreditaciones y evaluaciones de seguridad obtenidas para la infraestructura crítica.
- Planes de acción y mejora de la seguridad.
- Definición de roles y responsabilidades: Segregación de Tareas
- Jerarquía y responsabilidades de puestos de trabajo
- Relaciones con Terceros
- Gestión de la documentación y Estructura de dependencia y del proceso de elaboración y presentación de informes
- Gestión de Cambios.

7.1.2 Organización de la Seguridad

La organización de seguridad establece de forma general las estructuras organizativas adecuadas y las directrices de seguridad a tener en cuenta para la elaboración de los diferentes procesos que se desarrollan en las funciones de seguridad y los criterios aplicables a los mismos.

Una de las tareas principales de organizar la seguridad consiste en gestionar el factor humano, embebiendo en los procesos de seguridad todo lo referente a la gestión de las personas y las tareas directamente realizadas por las mismas.
Como ejemplo, entre los controles a tener en cuenta, podemos contemplarlos siguientes:

- Selección y Contratación del personal de Seguridad
- Los accesos de personas
- La vigilancia de la instalación
- Operación de los Sistemas de Seguridad
- Formación y entrenamiento
- Clasificación de la Información
- Acuerdos de confidencialidad
- Simulacros.

7.1.2.1 Comité de Seguridad y Crisis

Puesto que la seguridad es un proceso transversal a la organización las mejores prácticas para su gestión recomiendan la creación de un comité de seguridad y crisis con capacidad de priorizar y responsabilizarse de las acciones necesarias para la protección y continuidad de los servicios y la organización.

La mejor forma de progresar es colaborar. Es conveniente, la creación de grupos de trabajo en el que se permita una colaboración activa por parte de las personas encaminadas a eliminar las debilidades del sistema o establecer protocolos comunes de actuación frente a situaciones de crisis.

7.1.2.2 Establecimiento de Roles

El factor humano es el que realmente determina la efectividad de cualquier sistema de seguridad. Es por ello que debe existir un conjunto claro de funciones de seguridad y responsabilidades adecuadamente segregadas.

Es importante tener encuentra lo siguientes puntos a la hora de asignar responsabilidades:

- Asignar y documentar las responsabilidades.

- Documentar y definir claramente los niveles de autorización dentro del sistema.

7.1.2.3 Gestión de Cambios

La implantación del control de los cambios realizados en cualquier sistema, en especial los relacionados con la seguridad y las infraestructuras críticas, debería realizarse cómo mínimo mediante procedimientos formales (documentados) de control de cambios que contemple al menos:

- Evaluación de riesgos.
- Análisis de los efectos de los cambios.
- Especificación de los controles de seguridad necesarios.

Como recomendación de buenas prácticas es aconsejable la implementación automatizada de controles de cambios, de procedimientos de marcha atrás y la generación de los registros de auditorías pertinentes.

7.1.2.4 Gestión de la Calidad y Documentación

Es esencial una buena gestión de la documentación relacionada con los sistemas y ubicaciones de las infraestructuras críticas de las que dependen los servicios esenciales.

Específicamente las referencias y normas aplicables concretamente al servicio esencial deben estar identificadas para extraer de ellas los controles de seguridad específicos que son necesarios para la instalación / servicio.

Una buena gestión documental y de registros de la información relativa a la seguridad facilita el control y las actividades de monitorización y auditoría.

7.1.3 Medios Humanos y Seguridad del Personal

7.1.3.1 Formación y Concienciación

Partiendo de una estrategia planificada de formación: entrenamiento, reentrenamiento y concienciación, es conveniente sensibilizar y formar al personal, al menos, en las siguientes funciones:

- Sus roles y responsabilidades.
- Los conocimientos técnicos necesarios para el desempeño de su función.
- La sensibilización y conocimiento de las políticas y procedimientos establecidos.

7.1.3.2 Protección del Personal

El personal es el principal activo de toda organización. Las condiciones de salud, ambientales y seguridad personal son determinantes en todos los procesos de seguridad establecidos; por lo que es adecuado establecer protocolos de protección para aquellas personas cuya función dentro de la organización pueda suponer un alto riesgo en caso de compromiso de su seguridad.

7.2 DETALLE DE MEDIDAS OPERACIONALES O PROCEDIMENTALES

7.2.1 Procedimientos de gestión de activos

Una de las formas más eficientes de proteger las Infraestructuras críticas de un organización es mediante el modelado de la mismas tomando como base el servicio y/o los sistemas que la conforman.

Acorde con este modelo el punto de partida es la identificación de los activos que queremos proteger por lo que es conveniente contar con el inventario de los elementos integrantes. A la hora de clasificar los activos suele ser necesario establecer una serie de parámetros para poder determinar su nivel de y/o su agrupación en sectores o conjuntos de elementos. Como ejemplo de algunos parámetros a tener en cuenta podríamos destacar los siguientes:

- Impacto del incidente en activos que afecten al funcionamiento general del sistema.
- Impacto del problema en activos que afecten a los usuarios del sector.
- Impacto del problema en activos que afecten al resto de sectores.
- Capacidad de resolución del problema en un determinado activo.
- Tiempo estimado para la resolución del problema en un determinado activo.
- Posibilidad de propagación del problema en el mismo sector a través de un determinado activo.

- Coste de la resolución del problema o sustitución del activo.

Por ejemplo, los activos más críticos de un sector podrían ser los centros de control, ya que normalmente controlan el resto de elementos, pero habrá que tener en cuenta los distintos sectores, porque cada uno tendrá sus particularidades.

En una central nuclear puede que el subsistema encargado de su control directo sea el más crítico, ya que el daño que puede causar cualquier problema en el entorno puede ser incalculable.

Igualmente en subestaciones encargadas de proveer de energía a las distintas áreas geográficas también serán muy importantes, pero a medida que nos acercamos al destino final (usuario) la criticidad será menor, ya que deberían existir caminos redundantes a la hora de proveer al usuario final o una capacidad de reacción frente a contingencias más inmediatas.

Respecto a los sectores de telecomunicaciones, la posibilidad de establecer caminos secundarios a través de antenas y un control inmediato de las redes provocarían que los cortes de suministro no fuesen muy largos, siempre que se dispusiera de un servicio de acción rápido y eficiente.

Dentro de este apartado es conveniente contar con los procedimientos necesarios relacionados congestión y mantenimiento de activos, y de ser posible de forma automatizada:

- Procedimiento de inventariado (Identificación/Catalogación/Etc.)
- Activos físicos.
- Activos Digitales./Lógicos
- Procedimiento de gestión continúa de activos físicos y lógicos (Alta/Baja/Modificación).
- Etc.

7.2.2 Gestión de la Formación y Concienciación

La formación y concienciación se suele enfocar mediante dos vías de actuación principales:

- La capacitación para el desempeño de las funciones.
- La sensibilización para los puestos de trabajo y procesos operativos existentes.

En el primer caso se incluiría el cronograma aplicable, tanto interna como externamente, referido a los puntos siguientes:

- Evaluaciones
- Certificación
- Auditoria
- Simulación y Ejercicios
- Formación periódica
- Capacitación.

En el segundo de los casos comprenderían todos aquellos procedimientos de formación, concienciación y capacitación (tanto general como específica) asociados a los planes definidos para:

- Empleados/Operarios
- Vigilantes de seguridad
- Proveedores, etc.

7.2.3 Gestión de la Continuidad

La continuidad de la actividad es uno de los objetivos generales de la seguridad.

Por tanto es aconsejable abarcar todos aquellos procedimientos que velan por la supervivencia y continuidad de la organización y los servicios prestados. En especial los planes y procedimientos de Contingencias y Recuperación en función de los escenarios derivados de los riesgos.

- Imposibilidad de acceso a algún edificio de un complejo industrial.
- Indisponibilidad de los sistemas de información que operan una infraestructura crítica
- Etc.

Dentro de las necesidades de la gestión de la continuidad podemos indicar los siguientes conjuntos de controles:

- Plan Continuidad del negocio
- Plan de continuidad y Plan de Contingencia
- Prueba, mantenimiento y reevaluación de los planes de continuidad
- Pruebas periódicas
- Respaldos
- Inclusión de seguridad en el proceso de gestión de continuidad de negocio.

7.2.4 Supervisión Continua y Monitorización

El objetivo de la monitorización y la supervisión continua suele ser doble: por un lado permitir la detección de las anomalías de comportamiento y su corrección y, por otro, servir como base para la adquisición de la información necesaria que permita el registro de la actividad y la toma de decisiones.

Este conjunto de procedimiento suelen abarcar todos aquellos procesos operativos para la monitorización y supervisión de los activos, los sistemas y las personas que los controlan. En especial todos aquellos que nos permitan recolectar la información necesaria para la medida y mejora de la gestión, los controles de seguridad, y la minimización del riesgo de los activos afectados.

De forma general se suelen controlar los siguientes grupos de activos:

- Activos Físicos de la infraestructura
- Activos Lógicos y/o de sistemas de operación.

7.2.5 Gestión de accesos

La gestión de accesos es sin duda la primera línea de defensa para la protección de los activos y suele englobar todos aquellos procedimientos operativos relacionados con el acceso a los sistemas y ubicaciones de la organización. Suele ser conveniente estructurar los accesos conforme a las buenas prácticas de zonificación y segmentación de seguridad para establecer parcelas de actuación que permitir una gestión más eficaz, eficiente y controlable. En especial deberían considerarse todos aquellos procedimientos y medidas que nos permitan manejar de forma eficaz y eficiente las identidades y sus accesos como por ejemplo:

- Accesos de usuarios y personas (altas / bajas / modificaciones), incluyendo accesos temporales.
- Acceso de vehículos, mercancías, correspondencia, soportes técnicos, equipamiento, etc. (entradas / salidas).
- Control de accesos temporales.
- Control de entradas y salidas.
- Control de rondas.
- Identificación de Seguridad (pases, tarjetas, etc.).
- Control de visitas.
- Control de llaves y combinaciones.

7.2.6 Gestión de Evacuación y Emergencia

Es conveniente prevenir y anticiparse a hechos que obliguen la ejecución de procedimientos de emergencia, incluidos aquellos en los que sea necesaria la evacuación

de las instalaciones. Fundamental mente en este apartado es útil establecer procedimientos para:

- Gestionar la evacuación de las personas
- Gestionarla coordinación con terceros
- La gestión y escalado de las emergencias.
- Protección y bastionado extraordinario de activos durante el estado de emergencia.

7.2.7 Gestión de la Información

En la sociedad actual la información suele ser el principal activo de una organización, por lo que es necesario aplicar normas y procedimientos para garantizar que la incorporación de cada nueva fuente de información desencadena el proceso de actualización y clasificación de la misma, retirando, de ser necesario, aquellas fuentes de información y/o clasificaciones pertinentes cuando ya no son aplicables o necesarias.

Normalmente la clasificación de la información es algo consustancial con la organización conforme a aquellas características como confidencialidad, disponibilidad, integridad o su trazabilidad conforme a la "necesidad de conocer"; por lo que es conveniente parametrizar y establece los niveles necesarios de uso.

Existen algunos criterios comúnmente utilizados para el marcaje y clasificación de la información, en los que a modo de ejemplo podemos mencionar:

1. Los criterios marcados por el *Traffic Light Protocol* (TLP), creado por el órgano CPNI del Reino Unido (Centro Nacional de Protección de Infraestructuras de Reino Unido), y ampliamente extendido en su implementación por parte grupos de trabajo interdepartamentales.

ROJO – De uso privado, para destinatarios concretos únicamente. En el contexto de una reunión, por ejemplo, la información de nivel ROJO se limita a aquellos presentes en la misma. En la mayoría de las circunstancias la información de nivel ROJO se comunicará de verbalmente o en persona.

AMBAR – Distribución limitada. Los destinatarios pueden compartir la información de nivel AMBAR con otros miembros de la organización, bajo el criterio de “necesidad de conocer”.

VERDE – De ámbito comunitario. La información manejada en esta categoría puede circular extensamente dentro de una comunidad específica. Sin embargo, la información no puede publicarse en Internet, ni salir fuera de la comunidad.

BLANCO – Información de uso no restringido. Sujeto a las reglas del copyright que puedan aplicar, la información de nivel BLANCO puede distribuirse libremente, sin restricciones.

2. Criterio de clasificación basados en clasificación establecida por la normativa vigente de aplicación para determinados organismos de las Administraciones Públicas, eso sí; suavizando quizá algunos de los requerimientos para ajustarlos al entorno y circunstancias concretas, a menos que sean legalmente exigibles. En últimos casos es necesario recordar puede ser exigible la habilitación de seguridad oportuna para poder tener acceso a la información. Como ejemplo de niveles en esta clasificación podemos mencionar los siguientes:

- Secreto
- Reservado
- Confidencial
- Difusión limitada
- Sin clasificar.

7.2.8 Gestión de la Respuesta, Incidentes y Escalado

En general, conviene articular una gestión de respuesta a incidentes graduada que permita responder eficaz y proporcionalmente a los eventos no deseados que impacten en la operativa normal de la organización. No hay que olvidar considerar el subconjunto específico relativo a incidentes que puedan comprometer la propia seguridad de los sistemas y procesos de seguridad.

A modo de ejemplo las sub-secciones siguientes indican los procedimientos mínimos que deberían considerarse.

7.2.8.1 Procedimiento para la catalogación de incidentes

Para poder desplegar y articular una respuesta eficaz y proporcionada a los riesgos derivados de un incidente es necesario catalogar los mismos de acuerdo a los riesgos detectados. Es necesario considerar el subconjunto específico relativo a incidentes que puedan comprometer la propia seguridad de los sistemas y procesos de seguridad. Cómo mínimo es aconsejable establecer:

- Niveles.
- Criticidad.
- Protección de las evidencias.

En lo referente a la elaboración de procedimientos de los niveles de seguridad tanto permanentes como excepcionales (temporales/provisionales) debe tenerse en cuenta las circunstancias especiales de origen operativo o de riesgo (amenaza) inminente con mención específica a situaciones de no operatividad parcial (relevante) o total de los sistemas de seguridad.

7.2.8.2 Procedimiento para el escalado de incidentes

Este conjunto de procedimientos permite definir la graduación, responsabilidades y necesidades de información y el flujo de la misma que debe establecerse para la toma de decisiones y la gestión del conocimiento. Cómo mínimo es aconsejable establecer medios para:

- Comunicación
- Seguimiento.

7.2.8.3 Procedimiento para la respuesta a incidentes

En este apartado es adecuado tener en cuenta las relaciones con terceros y la colaboración a los Planes de Apoyo Operativos, en los que como operador de infraestructura crítica, se debe prestar apoyo a las Administraciones y organismos públicos implicados. Es conveniente articular previamente los escenarios de respuesta de modo que nos permitan realizar el análisis, resolución, cierre y aprendizaje de los mismos, para lo que debemos tener al menos en cuenta los siguientes entornos de operación:

- Interno
- Locales
- Externos
- Fuerzas y Cuerpos de Seguridad del Estado, autonómicas y locales.

7.2.9 Gestión del conocimiento

Es necesario articular la retroalimentación de las experiencias y situaciones acontecidas tanto propias como ajenas para realizar la incorporación de lecciones aprendidas de forma transversal a la gestión de la seguridad. La gestión del conocimiento nos permite aumentar el grado de certidumbre de las ocurrencias de eventos no deseados e identificar mejor la probabilidad de las amenazas al tiempo que nos prepara para ofrecer una respuesta más eficaz y proporcional a los incidentes.

Cómo mínimo es aconsejable establecer los siguientes procedimientos y mecanismos asociados necesarios:

- Recopilar el conocimiento
- Procesar y correlacionar el conocimiento

- Distribuir el conocimiento.

7.3 DETALLE DE MEDIDAS DE PROTECCIÓN O TÉCNICAS

7.3.1 Prevención y Detección

7.3.1.1 Protección multi-capa

Es útil para la defensa en general y ante la intrusión en particular aplicar un modelo de protección de acuerdo con el principio de "defensa en profundidad" en el que se aplican controles complementarios y superpuestos para lograr un mayor grado de protección.

Se deberían implementar las medidas necesarias de protección, detección y respuesta ante las intrusiones. Por ello es conveniente articular la compartimentación de zonas de protección conforme a las necesidades. Al menos es aconsejable considerar tres capas o zonas de protección, tanto en el mundo físico como en el lógico.

7.3.1.1.1 Zona Exterior o ante-perímetro

Vigilancia y Control de las zonas más externas al sistema o ubicación para detectar de forma proactiva posibles amenazas en las zonas circundantes al mismo. Es conveniente tener en cuenta los parámetros ambientales y sociales que pueden aumentar los riesgos y provocar incidentes que indirectamente afecten a la seguridad (huelgas, manifestaciones, vertidos, incendios, etc.….), cumpliendo siempre con la legislación vigente en este sentido.

7.3.1.1.2 Perímetro

Es recomendable controlar todo el perímetro de la organización, considerando éste tanto desde el punto de vista interior como exterior conforme a la segmentación en zonas de gestión.

A su vez, dentro de esta zonificación deberían considerarse zonas más generales de aquellas otras más vitales y/o importantes; monitorizando y registrando su actividad convenientemente para anticipar circunstancias de riesgo y anomalías.

7.3.1.1.3 Áreas Protegidas

Son las áreas en las que el acceso debe estar restringido incluso para usuarios internos según la necesidad de acceder. Serían áreas en las que, por su sensibilidad, pocas o muy pocas personas deberían tener acceso.

7.3.1.2 Control de acceso

Es elemental establecer controles y medidas de seguridad adecuados para la identificación, la restricción del acceso, el aseguramiento y monitorización del entorno de sistemas y ubicaciones bajo protección. El control de acceso debe fundamentarse en la "necesidad de conocer" y puede aplicarse de forma física y lógica a los sistemas y ubicaciones objeto de protección.

Algunos ejemplos de medidas de control de acceso aplicables podrían serlas siguientes:

- Como ejemplos de medidas y elementos de seguridad física y electrónica podemos indicar vallas, zonas de seguridad, cámaras de video vigilancia / CCTV, puertas y exclusas, cerraduras, lectores de matrículas, arcos de seguridad, tornos, etc.
- Cómo ejemplos de medidas y elementos de seguridad lógica relativos a los sistemas de información podemos indicar firewalls, DMZs; IPSs, segmentación y aislamiento de redes, cifrado, VPNs, elementos y medidas de control de acceso de usuarios (*tokens*, controles biométricos, etc.), medidas de instalación y configuración segura de elementos técnicos, herramientas de correlación de eventos y logs, etc.
- Otras medidas específicas acordes con los riesgos más particulares o concretos existentes.

7.3.1.2.1 Identificación y autenticación

Es necesario un sistema eficaz de identificación del personal, que facilite la categorización y diferenciación de los usuarios, la circulación y el acceso e impedir accesos no autorizados. Por ello se deben implementar medios técnicos y organizativos que permitan la identificación de personas, objetos y componentes.

Como ejemplo de medidas aplicables podemos destacar, las tarjetas de acceso, tarjetas de identificación, biometría, detección de metales, escáneres corporales, inventarios, etc.

Desde el punto de vista de la eficiencia, suele ser conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota.

7.3.1.2.2 Protección de áreas o zonas

La estructuración de las zonas interiores y exteriores de seguridad debe realizarse coherentemente para lograr el aseguramiento, vigilancia y monitorización de las mismas

en función de los riesgos sin olvidar aquellas zonas internas vitales cuyo compromiso puede producir un impacto altamente adverso en las personas, los procesos de negocio y los activos/ recursos de la organización.

Normalmente la creación de una división zonal de aquellos activos de mayor tamaño, alcance o complejidad favorece la gestión eficaz de las medidas y mecanismo implantado para su protección.

Cómo ejemplos de carácter general suelen tenerse en cuenta los siguientes elementos.

- Control de accesos tanto físicos como lógicos
- Áreas de acceso público, entrega y carga
- Asegurar oficinas, cuartos e instalaciones
- Control y contención de la intrusión
- Paramentos Horizontales y Verticales:
  - ✓ Muros, suelos, techos
  - ✓ Puertas, exclusas, y puertas de emergencia
  - ✓ Conductos
  - ✓ Ventanas
- Etc.

7.3.1.2.3 Control de Trabajo en Zonas Seguras

Uno de los elementos más importantes a controlar son la zonas seguras, fundamentalmente aquellas destinadas al control y supervisión de la seguridad.

Cómo ejemplos de carácter general suelen tenerse en cuenta los siguientes elementos:

- Control ambiental del entorno de la instalación: Iluminación de seguridad, operadores, etc.
- Vigilante de Seguridad o Recepcionista.
- Control de Acceso Automatizado.
- Control de Vehículos y mercancías.
- Circuito cerrado de televisión (CCTV).
- Protección contra incendios.
- Contenedores de seguridad, cajas fuertes, ficheros de claves, armarios blindados etc.
- Sistemas y elementos de respaldo.

7.3.2 Vigilancia y monitorización

7.3.2.1 Monitorización y alarma

Un componente importante de la seguridad se basa en el conocimiento y es por tanto aconsejable establecer todas aquellas medidas requeridas que conducen a la recolección de información, su correlación y la detección de desviaciones de lo que se considera normalidad.

Para ello es conveniente tener en cuenta los algunos elementos apropiados como:

- Centros de control de alarmas, centros de control de operaciones, centro de recepción y visionado de imágenes
- Equipos de vigilancia (turnos, rondas, dotación, etc.)
- Megafonía y radio
- Sistemas de detección y alarma de incendios.
- Sistemas de revisión de incidencias e incidentes
- Otros.

7.3.2.2 Seguridad del mantenimiento y activos de seguridad

La seguridad del mantenimiento consiste en prestar especial atención a todos los sistemas y ubicaciones y, en su caso, entornos no directamente relacionados con los activos a proteger; pero que por su naturaleza están imbricados en la estructura de la organización y/o son procesos básicos de mantenimiento del estado operativo de la organización.

Por ejemplo, se deberían asegurar las zonas y elementos de mantenimiento como cuadros de luces, llaves, cajas fuertes, elementos anti-incendios, dispositivos de alarma y seguridad, material y sustancias peligrosas, generadores, etc. que aunque no están directamente relacionados con los activos identificados del negocio; pero que su compromiso puede ser indicio o causa de un incidente de seguridad.

Como ejemplo de estos elementos podríamos considerar los siguientes:

- Subsistemas de Seguridad Electrónica
- Centralización y Control de Alarmas
- Mantenimiento del sistema de seguridad
- Mantenimiento de la infraestructura
- Mantenimiento de sistemas digitales críticos y comunicaciones
- Cableado, líneas de alimentación, etc.
- Sistema de comunicaciones de seguridad física

- Enlaces con los centros de control, puestos de vigilancia móviles o fijos
- Sistema de alimentación eléctrica, cableado, mantenimiento de equipos y reparaciones.

7.3.2.3 Auditoría y responsabilidad

La gestión de la seguridad y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos de seguridad), deberían someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad. Tras la misma, es aconsejable adoptar las acciones correctivas que correspondan para así mitigar los riesgos detectados, siempre bajo el bajo el marco de responsabilidad de la organización que permita corregir y dar cumplimiento a las insuficiencias detectadas en las mismas.

Es una buena práctica aconsejable establecer los controles de auditorías necesarios para determinar el grado de cumplimiento frente a las políticas y regulaciones establecidas, así como la eficacia y eficiencia de los controles de seguridad implantados; a la vez que se conciencia al personal sobre la responsabilidad de los procesos de los que forman parte.

De forma general el conjunto de auditorías a planificar suele ser de dos tipologías: de cumplimiento y técnicas. Las primeras se realizan frente a las regulaciones y normativas aplicables y la segunda frente a los requisitos documentados y comportamiento esperado de los sistemas auditados.

Como ejemplos de conjuntos de auditoría podemos destacar:

- Cumplimiento de normativa y legislación aplicable
- Eficacia de las medidas técnicas aplicadas
- Cumplimiento de los planes de acción acordados.

7.3.2.3.1 Gestión de registros

La gestión de conocimiento y la auditoría no es posible si no se registran evidencias de los hechos acontecidos; por lo que es necesario establecer una política de registros de evidencias acorde con las necesidades tanto de cumplimiento como conocimiento ligado a la eficacia y eficiencia de los procesos de seguridad.

Entre los elementos a controlar suele ser útil contar con:

- Gestión de registros en general.
- Registro de incidencias de seguridad.

- Registros de Avisos y Alertas.
- Registros o logs de auditoría.
- Protección de logs.
- Revisión de uso de sistemas.
- Logs de administradores y operadores.
- Logs de fallo del sistema.
- Etc.

7.3.2.3.2 Análisis forense

Se centra principalmente en conocer que ha sucedido tras un incidente estudiando los sucesos iniciadores que pueden dar lugar a la activación de determinadas medidas o actuaciones de seguridad. Ante cualquier incidente deberían aplicarse las técnicas metodológicas preestablecidas adecuadas para reconstruir los hechos, descubrir las relaciones entre ellos y comprender porque han sucedido con objeto de asimilar la lección aprendida. Por ejemplo, el método árbol de causas persigue evidenciar las relaciones entre los hechos que han contribuido en la producción de un incidente.

De forma general en cualquier análisis forense de unos hechos se deberían contemplar los siguientes puntos:

- Identificación y caracterización de los hechos
- Preservación de la evidencia
- Análisis y correlación de eventos para reconstruir la secuencia de hechos
- Informe, lecciones aprendidas y acciones de ser necesarias.

7.3.2.4 Métricas

Indicación de metodología de medición del desempeño de la Seguridad: qué tipo de objetivos se miden, qué forma de medirlos y qué procedimientos se disponen para su estudio y posterior propuestas de mejora.

7.3.3 Coordinación y respuesta

Ante la ocurrencia de un incidente de seguridad es necesaria una repuesta efectiva que permita lanzar acciones correctoras en tiempo y forma para contener o minimizar los daños que pudieran producirse.

La gestión adecuada de la respuesta y la información relativa a los incidentes de seguridad es esencial para cumplir con los parámetros normativos y regulatorios que sistematizan las evidencias necesarias para su estudio posterior.

Como ejemplo de elementos a tener en cuenta en la articulación de la coordinación y repuesta podríamos considerar los siguientes:

- Gestión de incidentes.
- Medida temporal y gradual.
- Repuesta ante incidentes y mitigación de ataques.
- Coordinación Internas.
- Comunicaciones externas: Criterios y Modelos de comunicación interna en caso de incidente comunicable.
- CNPIC.
- Administraciones y Ministerios.
- FFCCSE.
- ICS – CERT (*Industrial Control Systems Cyber Emergency Response Team*)
- CCN-CERT del CNI (Centro Nacional de Inteligencia) del Ministerio de la Presidencia.
- INTECO (Instituto Nacional de TEcnologías de la COmunicación) - INTECO (CERT) Centro de Respuesta a Incidentes de Seguridad, del Ministerio de Industria, Energía y Turismo.
- Servicios de Alertas de Proveedores.
- Etc.

7.3.3.1 Interrelación

En este punto se deberían tener en cuenta las interfaces bien sean suministradores o consumidores de las entradas y salidas de los procesos y/o servicios objeto de protección necesario entender a que aplican y su nivel de criticidad y/o los riesgos que suponen para los activos protegidos. Un punto clave es contar con documentación adecuada y veraz del intercambio mínimo necesario que se comparte o requiere entre los participantes.

Entre los puntos a tener en cuenta en este apartado podríamos destacar las necesidades técnicas y organizativas relativas a los siguientes elementos:

- Entorno ambiental.
- Entorno funcional.
- Servicios de los que depende.
- Servicios que dependen.
- Etc.

7.3.4 Continuidad y contingencia

La continuidad de una organización depende directamente de cumplir eficaz y eficientemente con la misión que se ha impuesto y la caracteriza; por ello, normalmente los servicios identificados como esenciales constituyen el punto central de su actividad. Es necesario dar continuidad a los mismos a pesar de las circunstancias y, cuando estas son adversas, se deberían prestar en condiciones mínimas aceptables y volver a la normalidad en cuanto sea posible. Por tanto es conveniente definir los controles necesarios que con una perspectiva de alcance adecuada a los servicios afectados permitan organizar los procesos de continuidad y contingencia aplicables según la granularidad necesaria.

Para lograr un conjunto mínimo de condiciones aceptables de continuidad suele ser útil contar con conjunto de elementos mínimos para desempeñar el servicio como por ejemplo los siguientes:

- La información y datos necesarios:
  - ✓ Respaldo de los datos.
  - ✓ Respaldo de las informaciones.
  - ✓ Respaldo de las dependencias externas e internas.
  - ✓ Respaldo del conocimiento.
- La infraestructura y las personas
  - ✓ Entornos alternativos.
  - ✓ Elementos de Respaldo y soporte.
  - ✓ Personas entrenadas y motivadas.
  - ✓ Capacidades alternativas del personal.
- Los planes y procedimientos para dar una respuesta en tiempo
  - ✓ Plan de contingencia y continuidad.
  - ✓ Prueba, mantenimiento y reevaluación de los planes.
  - ✓ Divulgación y formación de los planes.
  - ✓ Planes de Recuperación y reconstrucción.

-----oo00oo-----