GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN Y ESTUDIOS

GUÍA DE BUENAS PRÁCTICAS

PLAN DE SEGURIDAD DEL OPERADOR (PSO)

CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

GUÍA DE BUENAS PRÁCTICAS

PLAN DE SEGURIDAD DEL OPERADOR (PSO)

ÍNDICE

1. INTRODUCCIÓN

1.1 BASE LEGAL

El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada cuyo funcionamiento es indispensable y no permiten soluciones alternativas: las denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir la destrucción, interrupción o perturbación que perjudiquen la prestación de los servicios esenciales a la ciudadanía y asegure la continuidad de los mismos.

En este sentido, la Ley 8/2011, de 28 de abril por el que se establecen medidas para la protección de las infraestructuras críticas tiene como objeto el establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, impulsando además la colaboración e implicación de los organismos y empresas gestoras y propietarias (operadores críticos) de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados tanto físicos como lógicos, que puedan afectar a la prestación de los servicios esenciales.

Dicha Ley tiene su desarrollo mediante el Real Decreto 704/2011 de 20 de mayo, por el que aprueba el Reglamento de medidas para la protección de las infraestructuras críticas.

Del art. 13 de esta Ley se derivan una serie de compromisos para los operadores públicos y privados, entre los que se encuentran la elaboración de un Plan de Seguridad del Operador (en adelante PSO) y Planes de Protección Específicos (en adelante PPE).

Respecto a los contenidos del PSO, según se recoge en el artículo 22.4 del Real Decreto 704/2011, el Secretario de Estado de Seguridad estableció, a través del CNPIC, mediante Resolución de 8 de septiembre de 2015, los contenidos mínimos con los que debe contar todo PSO, así como el modelo en el que basar la elaboración de los mismos.

1.2 OBJETIVO DE ESTE DOCUMENTO

Con el presente documento se pretende orientar a aquellos operadores designados como críticos en la elaboración de su PSO, sirviendo como complemento a las Resoluciones del Secretario de Estado de Seguridad sobre Contenidos Mínimos del PSO. 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 la Resolución mencionada previamente.

En esta guía se incluyen una serie de Anexos (ejemplos, relación de estándares y buenas prácticas, etc.) que podrán ser de ayuda a los operadores críticos para la confección de alguno de los puntos de los contenidos mínimos del Plan de Seguridad del Operador.

1.3 PROTECCIÓN DE LA INFORMACIÓN

Tras la aprobación del PSO, su grado de clasificación será de **Difusión Limitada**, debiendo el Operador Crítico (en adelante OC) 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, para la Protección de la Información clasificada con grado de difusión limitada entre las que cabe destacar[1]:

- Seguridad documental
  - OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.
- Seguridad en el personal
  - OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.
- Seguridad física
  - OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.
  - OR-ASIP-01-02.03 – 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/

- Seguridad de los sistemas de información y comunicaciones
  - OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR Y MARCO DE GOBIERNO

2.1 POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR

El marco normativo de cualquier organización estará compuesto, habitualmente, por un conjunto de políticas de alto nivel, normas o estándares de desarrollo y procedimientos operativos o instrucciones de trabajo. La Política de Seguridad[2] a la que se refiere el PSO se trata del documento de mayor nivel de este conjunto mencionado que debería reunir una serie de requisitos que detallaremos a continuación.

Esta Política de Seguridad puede adoptar formas diversas, todas ellas, igualmente válidas: Documento en papel, manifestación en la Intranet de la Organización y, en general, cualquier soporte que permita comprobar los aspectos recogidos en los apartados siguientes.

2.1.1 Objeto

El objeto de la Política marca de manera fundamental todo el desarrollo posterior del cuerpo normativo, la organización de la función y las actividades relacionadas con la seguridad, así como, de manera muy clara, qué indicadores se utilizarán para medir la eficacia y eficiencia de las medidas implantadas. Este objeto es la estrategia de la función de seguridad, por lo que debería recoger cuál es su misión y su visión en el contexto de la estrategia global de la organización, aunque también podría adoptar otras formas (declaración de objetivos, etc.).

Normalmente, la estrategia de seguridad reflejará la intención de la organización de cumplir sus objetivos a largo plazo minimizando los riesgos, cumpliendo las normas de seguridad que le sean aplicables y previniendo y anticipando los incidentes que pudieran afectar a dichos objetivos organizativos. Dado que la seguridad absoluta no es factible, es lógico que se asuma en el objeto que van a existir incidentes y que se realizará una gestión de los mismos que permita minimizar su impacto en la consecución de los objetivos de la organización.

[2] Ver Anexo 1, apartado 7.1

El objeto de la política debería resaltar la protección de las infraestructuras críticas (IICC) especialmente frente a ataques deliberados. Dado que este tipo de amenazas presentan un perfil de baja probabilidad y alto impacto, su protección no responde a los parámetros habituales de eficacia y eficiencia. Por lo tanto, se debería recoger en esta política para la protección de las IICC qué criterios se aplicarán para responder adecuadamente a la materialización de estas amenazas de alto impacto de forma que se minimice el daño sobre las personas, el medio o el servicio esencial que se provee.

2.1.2 Ámbito o alcance

La Política de Seguridad puede tener un alcance limitado en distintos ejes: geográficos (países, regiones…), ámbitos de aplicación (físico, lógico…), organizativos (unidades, filiales…), etc.

Lógicamente, cada operador puede decidir cuál es la mejor forma para organizarse y no existen, a priori, modelos mejores o peores. En cualquier caso, para que la política de seguridad sea relevante para el PSO debería incluir en su alcance los servicios esenciales y las IICC operadas por la organización.

Los requisitos que existen en este sentido es que la(s) política(s) de seguridad debe(n) cubrir exhaustivamente todas las IICC operadas por la organización incluyendo la protección de las personas, los procesos y la tecnología (enfoque integral de la seguridad).

En relación con el alcance de la política, se debería prestar atención especial a aspectos tales como los siguientes:

- Consideración integral de la seguridad incluyendo los aspectos lógicos y físicos.
- Inclusión, tanto de los sistemas de información TIC de gestión, como de los sistemas de información para el control de los procesos industriales.
- Aplicación a los servicios esenciales y a las localizaciones y ubicaciones consideradas como críticas.
- Inclusión de las relaciones de dependencia como, por ejemplo, las empresas filiales que operen los servicios esenciales y las IICC.

2.1.3 Compromiso de la alta dirección

El compromiso de la Alta Dirección es un factor esencial para garantizar la aplicación de medidas de seguridad en una organización, por lo que debería implicarse, desde el inicio, en el propio proceso de definición de la Política.

Dicho compromiso puede adoptar formas diversas, pero normalmente, el más habitual es la sanción por el máximo órgano directivo de la Política de Seguridad que se va a aplicar, idealmente, con la firma del documento.

Además de este aspecto formal, el compromiso de la Dirección tiene otras formas de reflejarse en relación a la seguridad:

- Aspectos organizativos:
  Si existe un compromiso de la Dirección con la seguridad, la función responsable de la misma debería ser independiente de la operación / producción de manera que se pudiera producir un sano conflicto de intereses entre operatividad y seguridad. Por ejemplo, el responsable de seguridad de la información no dependería del responsable de sistemas de información.
  Por otra parte, la Dirección fomentaría y participaría en los Comités / Grupos de Trabajo que se establecieran para una adecuada toma de decisiones y gestión de la seguridad en conjunto con las áreas productivas y de soporte de la organización.
- Dotación de recursos:
  La Dirección aportaría los medios suficientes, dentro de las posibilidades de la organización, para implementar, operar y mantener los mecanismos de seguridad que se definan en línea con el objeto de la función de seguridad.
- Concienciación:
  La Dirección apoyaría, participaría e impulsaría las actividades relacionadas con la sensibilización en materia de seguridad para los empleados y usuarios externos implicados en la seguridad, en particular, de las infraestructuras críticas.
- Relaciones con terceros:
  La Dirección facilitaría el establecimiento de relaciones con otras organizaciones, privadas o públicas, que contribuyan a la seguridad (CERTs, FFCCS, etc.).

2.1.4 Carácter integral de la seguridad

Con independencia de cómo se organice la seguridad en otros ámbitos del operador, es esencial abordar la protección de las IICC con un enfoque integral (es decir, tener una visión única de las amenazas físicas y cibernéticas sobre las mismas y diseñar e implementar una estrategia de protección que integre medidas físicas, informáticas, operativas y del personal).

Este enfoque integral no presupone que se deba implementar una organización única de seguridad (aunque sería recomendable pues simplificaría los procesos de integración)

sino que deberían existir mecanismos para abordar una protección con un enfoque integral (de hecho, una organización unificada de seguridad no garantiza que no persista un enfoque dual de la protección).

En este sentido, el operador deberá indicar las medidas que garantizan este enfoque integral como, por ejemplo:

- Existencia de una organización unificada con objetivos, procesos y medios unificados.
- Procedimientos de trabajo (reuniones, elaboración de procedimientos, mecanismos de monitorización conjuntos…) enfocados a dotarse de una visión global.
- Existencia de órganos de coordinación.

2.1.5 Actualización

La Política de Seguridad debe ser un documento vivo que recoja las variaciones del entorno, de las infraestructuras y, también, del propio operador.

Por tanto, la organización debería indiciar los mecanismos de actualización de dicha política lo que, normalmente, se debería traducir en un procedimiento de revisión bienal (en línea con lo establecido en el RD) que establezca la responsabilidad para la realización de dicha revisión, los aspectos a analizar, los mecanismos de propuesta de modificaciones, así como la aprobación, publicación y difusión de los cambios (incluyendo, para el ámbito de la protección de las IICC, la pertinente comunicación con el CNPIC).

Dado que existe la posibilidad de que el proceso de revisión concluya sin cambios, el procedimiento existente debería generar las evidencias necesarias para poder verificar que la revisión ha tenido lugar (actas de reuniones, punto en el orden del día del Comité de Seguridad, etc.), aunque finalmente no hubiera generado modificaciones en la Política.

2.2 MARCO DE GOBIERNO DE SEGURIDAD

2.2.1 Organización de Seguridad y Comunicación

La Dirección de la Organización deberá formalizar los nombramientos del responsable y delegado/s de seguridad de acuerdo a sus procedimientos internos. La función de

seguridad, en particular, debería permitir dar cobertura de manera transversal a toda la Organización, para que se puedan cumplir los requerimientos establecidos.

Además de la documentación que se debería aportar sobre la organización de la seguridad, básicamente, organigrama general del operador, donde se identifique la estructura de seguridad corporativa y un organigrama específico de la función de seguridad donde se pueda comprobar el nivel jerárquico de los distintos roles y los comités existentes en materia de seguridad, existen dos aspectos que también deberían ser considerados.

Por una parte, el operador debería reflejar cómo la organización propuesta permite suficientemente la aplicación y el cumplimiento de la Política. En este sentido, hay que considerar que existen funciones dentro de las organizaciones que colaboran en la implantación de medidas de seguridad, como por ejemplo, la función de auditoría interna que, en muchas organizaciones, tienen una responsabilidad clara en asegurar que se cumplen las políticas internas y los marcos normativos de aplicación a la organización. Por este motivo, se debería considerar su inclusión en los organigramas mencionados anteriormente.

Por otra parte, existen herramientas que pueden ayudar a demostrar la suficiencia requerida. Por ejemplo, se pueden utilizar matrices RACI[3] para la clarificación de roles y responsabilidades dado que permiten reflejar, precisamente, quién se responsabiliza y encarga de cada tarea en una organización. Estas matrices se construyen indicando las distintas responsabilidades que existen (en este caso, se trataría de tareas relacionadas con la aplicación y comprobación de la Política de Seguridad) en filas y, en columnas, las funciones (los puestos) que existen dentro de la organización. Finalmente, las intersecciones se utilizan para indicar, donde aplique, el rol de una función en la ejecución de una determinada tarea. Los roles que se utilizan son los que dan nombre a la matriz (por su inicial en inglés):

- R – Responsable (responsable)
- A – Autorizador (accountable)
- C – Consultado (consulted)
- I – Informado (informed)

Para construir dichas matrices hay que considerar algunas reglas muy simples:

- Solo puede existir una ‘A’ (un autorizador) por cada tarea / responsabilidad.

[3] Ver Anexo 1, apartado 7.2.

- Pueden dejarse celdas en blanco, indicando que determinada función no interviene en la ejecución de una tarea.
- Todos los actores deben aprobar la matriz RACI que se elabore.

Finalmente, en caso de que se subcontraten algunas tareas en un tercero, en primer lugar, dicho tercero debería figurar en la matriz RACI con su correspondiente rol para las tareas asignadas y, por otra parte, se deberían indicar los compromisos existentes.

Normalmente, la manera más adecuada de recoger esta información es en el contrato de prestación de servicios aunque existen otras opciones:

- Puede existir un catálogo de servicios que recoja el encargo al proveedor o proveedores.
- Para los compromisos existentes, se pueden utilizar acuerdos de nivel de servicio como mecanismos de control y seguimiento del desempeño del proveedor (métricas que deberían incluir también elementos de seguridad).

En cualquier caso, el operador debería recoger los mecanismos que utiliza para controlar el cumplimiento de los compromisos existentes con el proveedor y, en particular, cómo gestiona la subcontratación de tareas por el propio proveedor y la notificación de incidentes.

En el caso de que exista un Comité de Seguridad dentro de la Organización de Seguridad, sería recomendable que, al menos un miembro o representante de la Dirección, perteneciera a dicho Comité, de forma que las decisiones que se adopten en él, cuenten implícitamente con el respaldo de la Dirección.

2.2.1.1 Responsable de Seguridad y Enlace / Delegado de Seguridad[4]

El operador debe aportar la información solicitada en este apartado y adicionalmente, también podría informar de los mecanismos de contingencia y continuidad adoptados para garantizar la comunicación con el Responsable de Seguridad y Enlace en caso de incidentes o que dicha persona se vea afectada por cualquier tipo de suceso adverso que no le permitan estar accesible.

[4] Ver Anexo 1, apartado 7.3

2.2.2 Formación y Concienciación

El plan de Formación y Concienciación aportado por el operador debería estar alineado con el objeto de la Política de Seguridad. Dicho plan, deberá recoger la información solicitada además de la información habitual de cualquier plan de este tipo:

- Duración. Normalmente los planes de formación y concienciación se realizan a lo largo de períodos plurianuales.
- Objetivos. Es decir, las mejoras en la capacitación y concienciación que se persigue obtener con la ejecución del plan.
- Público objetivo. Clasificación y segmentación de la audiencia a la que se dirige el plan. En este punto sería importante considerar los colectivos implicados en la protección de los servicios esenciales, tanto directa como indirectamente, y con independencia de que se trate de personal propio o subcontratado.
- Medios - Mensajes. Para cada uno de los públicos objetivos anteriormente identificados, se debería reflejar el mensaje que se le desea transmitir, así como el medio que se utilizará para hacérselo llegar (formaciones presenciales, vídeos, cursos online, boletines periódicos, sección específica en la Intranet, campañas de comunicación interna…).
- Seguimiento. Es decir, los mecanismos de evaluación que se utilizarían para comprobar que las acciones que se han emprendido contribuyen a la consecución de los objetivos marcados por el plan (como, por ejemplo, métricas de adecuación y aprovechamiento, política de firma de los asistentes, celebración de pruebas de aprovechamiento, etc.). Asimismo, se podría incluir quién se encarga de recoger la información, la metodología que utilizará, la periodicidad de las acciones, así como las acciones correctivas previstas.
- Actualización. Como todo plan, el Plan de Formación y Concienciación tiene una duración temporal, por lo que debería ser actualizado periódicamente para revisar sus objetivos, mensajes, etc. El Plan debería incluir el procedimiento de revisión utilizado: responsable, elementos a revisar y mecanismo de aprobación y publicación y difusión de los cambios al mismo.

En relación a la concienciación de los usuarios no hay que olvidar que no sólo los cursos y los elementos de difusión tienen un efecto sobre el nivel de concienciación de las personas, los elementos punitivos también tienen efecto sobre nuestras pautas de comportamiento, por lo que, los planes de concienciación también pueden incluir elementos como:

- Procedimientos sancionadores en caso de incumplimiento de la Política de Seguridad.
- Difusión de sanciones, incidentes… relacionados con la seguridad.
- Publicación de información relativa a controles de monitorización implantados.

Por último, no se debería olvidar la necesidad de compromiso de la Dirección mediante la disposición de los medios y recursos necesarios, pero también con muestras de apoyo público y notorio que ayudarán a desarrollar y garantizar el éxito de los planes establecidos.

2.2.3 Modelo de gestión aplicado

El modelo de gestión de la seguridad empleado por la organización para asegurar la aplicación y cumplimiento de la Política de Seguridad incluye todos los elementos típicos de estos esquemas normalmente asociados a un ciclo de mejora continua PDCA (*Plan – Do – Check – Act*) o ciclo de Deming con la particularidad, de que deberían considerar de manera concreta la protección de las IICC:

- Establecer el Sistema de Gestión (Planificar)
  - Establecer los objetivos y la política del sistema.
  - Crear los procesos y procedimientos necesarios para una adecuada gestión del riesgo.
  - Crear los mecanismos para el alineamiento de los objetivos del sistema con los objetivos del negocio.
- Implantar y operar el Sistema de Gestión y sus distintos componentes (Hacer)
  - Políticas y procedimientos.
  - Controles.
  - Procesos.
- Monitorizar y revisar el Sistema de Gestión (Comprobar)
  - Evaluar y, cuando sea posible, medir el funcionamiento de los procesos respecto a lo definido en la política y los objetivos del sistema.
  - Notificar los resultados de la evaluación a la Dirección para su revisión.
  - Realizar acciones preventivas.
  - Abordar acciones correctivas a partir de los resultados de revisiones y auditorías internas.

Por lo que respecta a las propias medidas de seguridad, además del sistema de gestión anterior, deben cubrir todos los momentos en que son necesarias. Por ejemplo, se podrían clasificar en las siguientes categorías:

- Prevención y Detección
  - Responsabilidad sobre la seguridad.
  - Análisis y gestión de riesgos.
- Protección y Defensa
  - Controles de la Dirección.
  - Adquisición / aprovisionamiento de sistemas e infraestructuras.
- Alertas y Auditorias: Evaluación y cumplimiento normativo.
- Medición y mejora continua.
- Coordinación y Respuesta: Relación entre la gestión de la seguridad y el resto de la organización.

En este contexto, es de especial importancia todo lo relacionado con los mecanismos de seguimiento de implantación de medidas de seguridad, así como, las métricas de eficacia y eficiencia que se utilicen, sin el menoscabo de otros mecanismos de control como los llevados a cabo por las áreas de auditoría interna y/o cumplimiento. Por este motivo, la función de auditoría debería incluir en su planificación de trabajos, revisiones relacionadas con la protección de las IICC en todas sus dimensiones y sin olvidar elementos, como el software de control industrial.

En esta misma línea, la consideración de la seguridad desde el inicio en la adquisición y el aprovisionamiento de nuevos sistemas e infraestructuras sería esencial para evitar errores derivados del diseño de las mismas. De esta forma, antes de que cualquier sistema o infraestructura esté operativa se debería verificar que cumple los requisitos de seguridad necesarios en función del Plan de Seguridad adoptado por la organización.

2.2.4 Comunicación

Para que haya un intercambio de información eficaz entre el CNPIC y el propio operador en todos aquellos aspectos relativos al ámbito de la Protección de Infraestructuras Críticas es importante que por parte de operador se diseñen los oportunos procedimientos para realizar de forma efectiva dicha comunicación. Así, el operador deberá incluir los siguientes procedimientos y aquellos otros que estime oportunos, a saber:

Comunicación al CNPIC:

- De aquellos incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de alguna de las infraestructuras de la que el operador es gestor y/o

propietario, conforme al protocolo de comunicación de incidentes PIC elaborado por este Centro y puesto a disposición de los operadores críticos.

- De aquellas variaciones de carácter organizativo, de planificación o estructural que se produzcan en el seno del propio operador y que afecten de alguna manera a las infraestructuras críticas objeto de protección (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

Comunicación al CERTSI:

- A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes del operador crítico y la disponibilidad de los servicios que presta. Todo ello, conforme al protocolo de comunicación de incidentes PIC elaborado por el CNPIC y puesto a disposición de los operadores críticos.

3. RELACIÓN DE SERVICIOS ESENCIALES PRESTADOS POR EL OPERADOR CRÍTICO

El principal objetivo es que el operador pueda realizar una presentación y breve descripción de la compañía o grupo al que pertenece dicho operador, pudiendo tenerse en cuenta aspectos como:

- Razón Social y matriz.
- Desglose de la estructura societaria.
- Desglose de la composición accionarial y grado de participación.
- Sedes principales y ubicación geográfica.
- Sector/es al que pertenece en función de la actividad desarrollada.
- Subsector/es para cada actividad desarrollada.
- Actividad desarrollada.
- Proveedores necesarios para la prestación de los servicios esenciales identificados (incluyendo información como, por ejemplo, nombre de los proveedores y tipo de suministros prestados).
- Clientes finales de los servicios prestados identificado/s como esencial/es (incluyendo información como, por ejemplo, países, administraciones, empresas, particulares, etc.).

3.1 IDENTIFICACIÓN DE LOS SERVICIOS ESENCIALES

El OC debe realizar una breve descripción de los servicios esenciales prestados a la ciudadanía en relación al concepto de servicio esencial recogido en el Art. 2 a) de la Ley, dentro del sector o subsector estratégico en el que se encuentra incluido. Para ello, podría aportar información como la siguiente:

- Identificación de los servicios y áreas de actividad que son o pueden ser esenciales para los ciudadanos.
- Tipología de los activos o infraestructuras críticas sobre las que descansa dicho servicio o área de actividad.
- Medios materiales, personales y recursos de los que dispone para la prestación del servicio.
- Ubicación geográfica en la que se presta el servicio identificado como esencial, (por ejemplo: país, comunidad autónoma, ciudad, etc.), identificando localidades y estimación del volumen de población en su área de influencia.
- Empresas con las que comparte la ubicación geográfica.

3.2 MANTENIMIENTO DEL INVENTARIO DE SERVICIOS ESENCIALES

Se debería realizar una descripción del procedimiento de mantenimiento del inventario de los servicios identificados como esenciales como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece. Se deberían describir las formas y procedimientos de identificación, mantenimiento, revisión y actualización, así como el órgano responsable encargado de los mismos. En dicho mantenimiento se debería tener en cuenta al menos:

- El ajuste de cartera de servicios, fusiones, adquisiciones, ventas de activos...
- La internalización de procesos operativos.
- Los periodos establecidos en el Plan conforme al punto 1.4 incluido en la guía de contenidos mínimos del PSO (la legislación establece períodos de actualización bienales o cuando se produzcan cambios significativos).

3.3 ESTUDIO Y CONSECUENCIAS DE LA INTERRUPCIÓN DEL SERVICIO ESENCIAL

El estudio de consecuencias que debe llevar a cabo el OC, debe realizarse conforme a lo que se entiende en la legislación por “interrupción” que excede a la simple indisponibilidad del servicio ya que considera la *“no disponibilidad del servicio esencial*

[…] motivado por alguna alteración o interrupción en el tiempo o una destrucción parcial o total de las infraestructuras que gestionan dicho servicio".

Se debería realizar un análisis de los resultados del estudio de las consecuencias que supondría la interrupción y no disponibilidad para cada uno de los servicios identificados como esenciales en caso de:

- Alteración de su función.
- Interrupción en el tiempo.
- Destrucción parcial o total de la infraestructura que gestiona el servicio.
- Etc.

Adicionalmente, se debería identificar claramente, para cada uno de los casos, la siguiente información:

- Extensión geográfica y número de personas que pueden verse afectadas.
- Efectos en el tiempo.
- Impacto económico.
- Impacto medioambiental.
- Impacto en la vida y salud de las personas.
- Efecto sobre operadores y servicios esenciales dependientes.
- Existencia de alternativas de prestación del servicio esencial o mecanismos de contingencia proporcionados por el propio operador y nivel de degradación que conllevan.

3.4 INTERDEPENDENCIAS

Se debería realizar una descripción de las posibles interdependencias entre servicios esenciales e infraestructuras críticas que los soportan, así como con las de otros operadores dentro del mismo sector o diferente, que deban ser consideradas en el análisis de riesgos. Algunos ejemplos de interdependencias a considerar serían los siguientes:

- Entre las propias instalaciones o servicios del operador.
- Con operadores del mismo sector.
- Con operadores de distintos sectores.
- Con operadores de otros países, del mismo sector o no
- Con sus proveedores de servicios dentro de la cadena de suministros.

- Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del Operador.
- Con servicios esenciales prestados por otros operadores del mismo sector con una breve explicación del motivo que origina dichas interdependencias.
- Con servicios esenciales prestados a otros operadores de distinto sector.
- Con servicios esenciales prestados por operadores de otros países.
- Etc.

4. METODOLOGÍA DE ANÁLISIS DE RIESGOS

El operador debe contar con una metodología de análisis de riesgos que permita identificar y gestionar los principales riesgos a los que se encuentran expuestos los servicios críticos derivados de cada operador.

4.1 DESCRIPCIÓN DE LA METODOLOGÍA DE ANÁLISIS

Cualquiera de las metodologías internacionalmente reconocidas que los operadores quieran utilizar para la identificación y posterior gestión de sus riesgos debería tomar en consideración, al menos, las fases incluidas en los apartados siguientes.

Un aspecto fundamental de las metodologías de análisis de riesgos es que los distintos valores que se utilizan y las estimaciones de los diferentes parámetros (vulnerabilidad, impacto…) sean repetibles y con un mismo criterio a lo largo del tiempo para poder obtener valores comparables.

4.2 IDENTIFICACIÓN Y VALORACIÓN DE LOS ACTIVOS QUE SOPORTAN LOS SERVICIOS ESENCIALES

El nivel de detalle debería cubrir, al menos, lo siguiente:

- Servicios prestados; pudiéndose agrupar por clases uniformes a efectos de impacto en terceros.
- Dependencias de elementos que están redundados de forma que, en principio, no serían críticos para la prestación de los servicios, pero que se convertirían en críticos si fallara alguno de ellos.

- Dependencias de servicios de terceros, indicando la dependencia entre servicios y la posible complementariedad cuando un servicio puede reemplazar a otro (plan de contingencia).
- Instalaciones físicas, en particular edificios, recintos y canalizaciones susceptibles de ataques o incidentes.
- Equipos de personas con roles críticos.
- Sistemas de información de soporte, como sistema, sin entrar en componentes salvo que alguno sea singular.
- Sistemas de control industrial de instalaciones (Sistemas SCADA).

La valoración de los activos estriba, principalmente, en la estimación de las consecuencias derivadas de la interrupción del servicio. Desde el punto de vista de los criterios para realizar esta valoración se deberá tener en consideración lo establecido por la ley 8/2011 en lo relativo a "criterios horizontales de criticidad".

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

4.3 IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS

A partir del listado de activos identificados, se debería realizar la identificación de amenazas que pudieran llegar a afectar a estos activos con el fin de tratar de cubrir el mayor número de potenciales situaciones de riesgo.

Para realizar esta identificación se recomienda establecer una taxonomía con un código que identifique a cada tipo de amenaza y contar con una estructura jerárquica que pueda ser refinada según sea necesario,

Ante cada posible amenaza que se considere, se debería establecer una escala de probabilidad de ocurrencia, a efectos de realizar el posterior análisis (ya sea este cualitativo o cuantitativo).

Los OC y resto de agentes deberán tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado.

4.4 VALORACIÓN Y GESTIÓN DE RIESGOS

El objetivo de esta actividad es la identificación de las combinaciones de activos y amenazas que puedan afectar la prestación de los servicios críticos, precisándose dichas consecuencias, en general y especialmente sobre la disponibilidad de los servicios.

Para cumplir con este objetivo, sería necesario estimar el impacto potencial que provocaría la materialización de cada amenaza sobre los activos identificados por el operador. El impacto potencial mide el posible daño, independientemente de que sea más o menos probable. Simplemente, se determina si es posible.

Es posible que haya que definir niveles degradados de servicio que, sin prestar la calidad exigible en condiciones normales, faciliten un nivel de 'supervivencia'.

A partir de esta estimación se calculará el riesgo potencial como resultado de la combinación del impacto potencial con la probabilidad de que la amenaza se materialice en incidente o un ataque.

De la totalidad de riesgos potenciales que se hayan identificado, será necesario proceder a la gestión de los mismos. Dicha gestión consiste en la identificación de las medidas de seguridad que reduzcan los riesgos potenciales. Serán de especial interés los controles en caso de incidentes. Los riesgos resultantes de la aplicación de estas medidas de control determinarán los riesgos residuales a los que está expuesto cada operador.

En particular, dada la naturaleza de las amenazas de origen intencionado, el operador debe indicar el tratamiento que va a dar a las amenazas de baja probabilidad y alto impacto (en cualquiera de sus dimensiones de valoración). En este sentido, debería indicar la combinación de medidas de seguridad que va a aplicar para prevenir, detectar o actuar en caso de que se materialice alguna de dichas amenazas, como, por ejemplo:

- Sistema de detección de alerta temprana.
- Procedimientos de respuesta ante incidentes.
- Mecanismos de contingencia.
- Etc.

Sería recomendable, como parte de la metodología de análisis de riesgos, indicar la forma en la que se plasmarán los resultados de dicho análisis y que recoja la información esencial para la evaluación posterior del mismo por el CNPIC.

5. CRITERIOS DE APLICACIÓN DE MEDIDAS DE SEGURIDAD INTEGRAL[5]

Como buenas prácticas para la aplicación de medidas de seguridad integral, el Operador puede seleccionar las medidas de seguridad a implementar, por ejemplo, entre los estándares de seguridad reconocidos internacionalmente y en la legislación específica aplicable a su sector o con carácter general.

En el ámbito de la seguridad lógica se establece como buena práctica, realizar la selección de los controles de seguridad a implementar y gestionar de la ISO 27002:

- Definir la Política de Seguridad Corporativa
- Organización de la seguridad de la información
- Gestión de Activos
- Seguridad de los RRHH
- Gestión de las comunicaciones y operaciones
- Control de Acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes de seguridad
- Gestión de la continuidad del negocio
- Cumplimiento de la legislación aplicable
- Revisión y auditoría de sistema de gestión de la seguridad integral implantado.

En el ámbito de la seguridad física no existe normativa referente al catálogo de medidas de seguridad previo, pero se deberá seguir lo especificado por la legislación de

Seguridad Privada, especialmente lo recogido en la Orden Ministerial 316/2011 del Ministerio del Interior y su referencia a la normativa UNE/EN.

En este sentido, será especialmente útil seguir las recomendaciones de la norma UNE/CLC TS 50131-7 (Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7. Guía de aplicación).

Dado el enfoque integral que se pretende dar a las medidas de seguridad y conforme a la clasificación de medidas genérica establecida en el apartado 4.2 Medidas de Seguridad de la Guía de Contenidos Mínimos del PPE, sería recomendable reflejar los criterios de aplicación de las diferentes medidas recogidas en dicha clasificación y que reproducimos en la tabla siguiente con algunos detalles adicionales.

[5] En el apartado 8. Anexo 2 – Relación de Estándares y Mejores Prácticas se incluye una relación de documentación que puede ser utilizada como soporte para la identificación de medidas de seguridad integral.

Respecto a dichos criterios, resaltar una vez más que la prioridad debe ser aplicar dichas medidas en función del impacto que las amenazas puedan tener sobre los servicios esenciales (es decir, la probabilidad juega un papel secundario ya que el objetivo perseguido es la prevención y la protección de las infraestructuras críticas).

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

A continuación se muestra un registro de ejemplos de medidas de seguridad aplicadas a activos físicos y de seguridad de la información:

	ACTIVOS	
	FÍSICOS	SISTEMAS DE INFORMACIÓN
ORGANIZATIVAS O DE GESTIÓN		
Análisis de Riesgos	Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo	
Planificación	Identificación de objetivos y programación de las actividades para conseguirlos	
Definición de roles y responsabilidades	Asignación de responsabilidades en materia de seguridad	
Cuerpo normativo	Elaboración de políticas, estándares y procedimientos de seguridad	
Cumplimiento normativo	Identificación de normativa aplicable y cumplimiento con las mismas	
Certificación, acreditación y evaluación de seguridad	Revisiones periódicas de los sistemas para evaluar su nivel de seguridad	
OPERACIONALES O PROCEDIMENTALES		
Gestión de activos y de la configuración	Identificación de activos, control de inventario	
Formación y concienciación	Planes de formación y concienciación en seguridad	
Planes de Contingencias	Planes de Contingencias informáticas y físicas	
Supervisión continua	Evaluación / auditoría continua de los sistemas	
Seguridad del personal	Procesos de selección, régimen interno, procedimientos de cese	
Gestión de acceso - Gestión de usuarios	Altas, bajas y modificaciones	
Gestión de acceso - Control de accesos temporales	De personas, vehículos, etc.	Identificadores de usuario temporales de los sistemas (mantenimiento…)
Gestión de acceso - Control de entradas y salidas	Paquetería, correspondencia…	Soportes, equipos… e información (DLP, DRM…)
Procedimientos operacionales del personal de seguridad	Control de rondas de seguridad	N/A
Evacuación	Plan de evacuación	N/A
DE PROTECCIÓN O TÉCNICAS		
Medidas de prevención y detección		
Anti-intrusión	Seguridad física y electrónica perimetral, sistemas de detección perimetral	Firewalls, DMZs, IPSs, segmentación de redes, protección del puesto de trabajo, cifrado, VPNs
Control de accesos (incluye autenticación)	De personas, vehículos, paquetería y mercancías (medios humanos, tarjetas activas, lectores de tarjetas, lectores de matrículas, tornos, scanner, etc.)	Registro de usuarios, gestión de privilegios, gestión de claves secretas, revisión de derechos de acceso…, identificadores de usuario acceso a SSII
Instalación y configuración segura	Configuración segura de los equipos y sistemas con carácter previo a su entrada en operación, mantenimiento de los equipos y control de los cambios. Aseguramiento de las condiciones ambientales para su operación (temperatura, humedad…)	
Protección frente a malware	N/A*	Instalación de sistemas anti-virus, antispyware, etc.
Desarrollo seguro de aplicaciones	N/A*	Desarrollo basado en mejores prácticas, auditorías preproducción
Medidas de coordinación y monitorización		
Monitorización	Sistemas CCTV (cámaras, video vigilancia)	IDSs, sistemas de integridad de software y sistemas de monitorización y gestión de logs
Coordinación (gestión de incidencias)	Centro de Control, central de alarmas propia, sistemas de comunicación…	Creación de equipos de respuesta a incidentes (CSIRT), infraestructuras SOC

6. DOCUMENTACIÓN COMPLEMENTARIA

6.1 NORMATIVA, BUENAS PRÁCTICAS Y REGULATORIA

El operador recogerá en una breve referencia toda aquella normativa y buenas prácticas que regulen el buen funcionamiento de los servicios esenciales prestados por todas y cada una de sus infraestructuras, así como los motivos por los cuáles les son de aplicación.

Las normativas a incluir comprenden tanto las de rango nacional, autonómico, europeo e internacional, como las sectoriales, relativas a:

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

6.2 COORDINACIÓN CON OTROS PLANES

Se identificarán todos aquellos Planes diseñados por el operador relativos a diferentes aspectos como la continuidad de negocio, gestión del riesgo, respuesta, ciberseguridad, autoprotección, emergencias que puedan coordinarse con el Plan de Seguridad del Operador y los respectivos Planes de Protección Específicos, y que serían activados en el caso de fallo de los mecanismos de prevención una vez que se hubiera producido el incidente.

7. ANEXO 1: EJEMPLOS

7.1 POLÍTICA DE SEGURIDAD

7.1.1 Aprobación y entrada en vigor

Texto aprobado el día <día> de <mes> de <año> por <órgano que la aprueba>.

Esta Política se Seguridad Integral es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día <día> de <mes> de <año> por <órgano> qué lo aprobó.

7.1.2 Introducción

El normal funcionamiento de los servicios esenciales que <el operador crítico> presta a la ciudadanía descansa sobre una serie de infraestructuras cuyo funcionamiento es indispensable y no permite soluciones alternativas denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población, o con consecuencias catastróficas para las vidas de las personas o el medio ambiente.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas de seguridad definidas, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad es una parte integral de cada etapa del ciclo de vida del servicio esencial, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

7.1.3 Alcance

Esta política se aplica a todas las infraestructuras críticas del <el operador crítico> y a todos los miembros de la organización, sin excepciones.

7.1.4 Misión

Describir los objetivos de servicio del operador crítico.

7.1.5 Marco normativo

Listar leyes, reglamentos y otra normativa, nacional o internacional, a la que el operador crítico está sujeto.

7.1.6 Organización de la seguridad

7.1.6.1 Comités: Funciones y responsabilidades

El Comité de Seguridad Integral estará formado por <…>. Aquí aparecen cargos corporativos y designaciones de departamentos dentro del organismo cuando proceda.

El Secretario del Comité de Seguridad TIC será <…> y tendrá como funciones <…>.

El Secretario del Comité de seguridad Física será <…> y tendrá como funciones <…>.

El Comité de Seguridad Integral informará a <…>.

El Comité de Seguridad Integral tendrá las siguientes funciones: <…>.

7.1.6.2 Roles: Funciones y responsabilidades

Cuando proceda, se detallará el nombramiento de los Delegados de Seguridad y las funciones que les son delegadas.

Se detallarán igualmente las funciones del Responsable de Seguridad y Enlace.

7.1.6.3 Revisión

Será misión del Comité de Seguridad Integral la revisión de esta Política de Seguridad y la propuesta de revisión o mantenimiento de la misma.

La Política será aprobada por <órgano que la aprueba> y difundida para que la conozcan todas las partes afectadas.

7.1.7 Manejo de la información

<El operador crítico> trata datos de carácter personal. El <documento de seguridad> que se puede encontrar en <indicar la forma de localizar y acceder al documento de seguridad> recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de <el operador crítico> se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Por otra parte, la información relativa al Plan de Seguridad Integral será tratada y custodiada según se indica en los procedimientos específicos (acorde a la reglamentación que sea de aplicación en cada momento) conforme a su consideración como información de difusión limitada.

7.1.8 Gestión de riesgos

Todos los servicios sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año,
- cuando cambien los servicios prestados,
- cuando ocurra un incidente grave de seguridad,
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad Integral establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad Integral dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes servicios, promoviendo inversiones de carácter horizontal.

7.1.9 Prevención, detección, reacción y respuesta

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de acuerdo a la Ley de Protección de Infraestructuras Críticas.

7.1.9.1 Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información, los servicios, las vidas de las personas o el medio ambiente se vean

perjudicados por incidentes derivados de actos malintencionados. Para ello los departamentos deben implementar medidas de seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

7.1.9.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa a distintos niveles, por tanto, se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

7.1.9.3 Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros operadores críticos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.
- Ponerse en contacto con las Fuerzas y Cuerpos de Seguridad según los procedimientos específicos previstos.
- Establecer comunicación con los cuerpos de emergencias y protección civil.

7.1.9.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

7.1.10 Obligaciones del personal

Todos los miembros de <el operador crítico> tienen la obligación de conocer y cumplir esta Política de Seguridad Integral, siendo responsabilidad del Comité de Seguridad Integral disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de <el operador crítico> atenderán a una sesión de concienciación en materia de seguridad integral al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de <el organismo>, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de servicios esenciales recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

7.1.11 Terceras partes

Cuando <el operador crítico> preste servicios a otros <…> o maneje información de terceros <…>, se les hará partícipe de esta Política de Seguridad Integral, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad Integral y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando <el operador crítico> utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

7.1.12 Desarrollo de la política de seguridad integral

Esta Política de Seguridad Integral complementa las políticas de seguridad de <el operador crítico> en diferentes materias:

- Listar referencias a otras políticas en materia de seguridad.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet: URL e impresa en (LOCALIZACIÓN).

7.2 MATRIZ RACI

	CEO - Chief Executive Officer	Comité de Seguridad	CIO - Chief Information Officer	CSO - Chief Security Officer	Recursos Humanos	Áreas de negocio
Elaboración de política de Seguridad	A	C	I	R		
Ejecución del Plan de Formación y Concienciación		I		A	R	
Elaboración y mantenimiento de análisis de riesgos	I	A		R		C
Elaboración Plan de Tratamiento del Riesgo	A	I		R		C

7.3 DESIGNACIÓN DE RESPONSABLES

Responsable de Seguridad y Enlace

<Nombre organización> designa a <nombre y apellidos> como responsable de seguridad y enlace. Este responsable podrá ser sustituido por <nombre y apellidos>.

Los datos de los asignados son:

	Responsable	Sustituto
Nombre		
Dirección		
Teléfonos		
Email		
Número de la tarjeta identificativa de Director de Seguridad expedida por el Ministerio del Interior.		
Referencia o copia del nombramiento.		

El responsable, y en su defecto el sustituto, tendrán las siguientes funciones:

- Representar al operador crítico ante la Secretaria de Estado de Seguridad

  - En materia relativas a la seguridad de sus infraestructuras

  - En materia relacionada con los diferentes planes especificados en el real decreto

- Canalizar las necesidades operativas e informativas que surjan.

FIRMA

Delegados de Seguridad de las Infraestructuras Críticas.

<Nombre organización> designa para cada infraestructura los siguientes responsables y su correspondiente sustituto.

Los datos de los delegados y sus sustitutos son:

Infraestructuras		Responsable	Sustituto
Infraestructura X	Nombre		
	Dirección		
	Teléfonos		
	Email		
	Referencia o copia del nombramiento.		
Infraestructura Y	Nombre		
	Dirección		
	Teléfonos		
	Email		

El responsable, y en su defecto el sustituto, tendrán las siguientes funciones:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materia relativas a la seguridad de sus infraestructuras.
- Canalizar las necesidades operativas e informativas que surjan.

FIRMA

8. ANEXO 2: RELACIÓN DE ESTÁNDARES Y MEJORES PRÁCTICAS

A continuación se enumeran y describen una serie de estándares, guías y mejores prácticas que existen a nivel nacional e internacional.

8.1 ESTÁNDARES Y MEJORES PRÁCTICAS NACIONALES

8.1.1 Sistemas SCADA y Esquena Nacional de Seguridad[6]

La siguiente tabla recoge las diferentes guías de seguridad sobre sistemas de control industrial (SCADA), las guías relativas al Esquema Nacional de Seguridad, se encuentran en la dirección: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html. Estas guías han sido elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia del Ministerio de la Presidencia, y están dirigidas a las diferentes administraciones públicas.

SERIES	CCN-STIC	NOMBRE	VERSIÓN
	480	Seguridad en Sistemas SCADA	mar-10
	480A	Seguridad en Sistemas SCADA – Guía de buenas prácticas	feb-10
	480B	Seguridad en Sistemas SCADA – Comprender el riesgo del negocio	mar-10
	480C	Seguridad en Sistemas SCADA – Implementar una arquitectura segura	mar-10
	480D	Seguridad en Sistemas SCADA – Establecer capacidades de respuesta	mar-10
	480E	Seguridad en Sistemas SCADA – Mejorar la concienciación y las habilidades	ene-10
	480F	Seguridad en Sistemas SCADA – Gestionar el riesgo de terceros	mar-09
	480G	Seguridad en Sistemas SCADA – Afrontar proyectos	mar-09
	480H	Seguridad en Sistemas SCADA – Establecer una dirección permanente	mar-10

8.1.2 Seguridad Física

UNE-EN 50131-1:2008/A1:2010 Sistemas de alarma contra intrusión y atraco

Parte 1: Requisitos del sistema. Norma multi-parte específica de los sistemas de alarma

Proporciona una descripción general de los sistemas de Detección de Intrusión especificando los grados de Seguridad.

UNE/CLC TS 50.131.7 Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7. Guía de aplicación

Expone una guía para implementar correctamente un Sistema de Seguridad frente a Intrusión, indicando los pasos a seguir en el Proyecto, la Instalación, la puesta en marcha y el mantenimiento y explotación.

[6] Guías CCN-STIC relacionadas con sistemas SCADA: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/400-guias-generales.html
Guías CCN-STIC de la serie 800 relativas al Esquema Nacional de Seguridad: https://ccn-cert.cni.es/ens

8.1.3 Métricas e Indicadores

UNE 66175 Sistemas de gestión de la Calidad. Guía para la implantación de sistemas de indicadores

Esta norma facilita el establecimiento de indicadores y cuadros de mando, que contribuyen activamente a la medición de los fenómenos concernientes al funcionamiento de una organización y facilita la toma de decisiones. Así mismo explica la relación existente entre cuadros de mando, indicadores y objetivos.

8.2 ESTÁNDARES Y MEJORES PRÁCTICAS INTERNACIONALES

8.2.1 Gobernanza y Gestión de TI incluida la calidad y la cadena de suministro

ISO/IEC 20000 Information technology -- Service management

Es una norma multi-parte basado en ITIL (IT *Infrastructure Library*) para la gestión de los servicios prestados por IT. Es un conjunto de buenas prácticas aplicables a los sectores públicos y privados. Es posible la certificación, la formación acreditada y la utilización de herramientas para facilitar su implementación.

ISO/IEC 20000 Part 1:2005 *Information technology service management*. Describe los requerimientos de gestión de los servicios de IT frente a los cuales se puede certificar una organización.

ISO/IEC 20000 Part 2:2005 *Information technology service management*. *Code of Practice for Service Management*. Proporciona una guía práctica para los implementadores y un conjunto de buenas prácticas para la gestión de los servicios.

ISO/IEC 38500 -- Corporate governance of information technology - a standard for corporate governance of information technology

Proporciona los principios directrices a los responsables de las organizaciones para el uso aceptable, efectivo y eficiente de las Tecnologías de la Información en la organización. El estándar hace referencia a al proceso de gestión del gobierno de TI y las decisiones relativas a los servicios de información y comunicaciones de la organización.

ISO/IEC 13335 IT security management

Es una norma multi-parte que proporciona un conjunto de directrices para la gestión de la seguridad de TI, centrándose especialmente en controles técnicos de seguridad. Estas normas están siendo en parte sustituidas por la familia 270xx.

ISO 9003:2004 Software engineering - Guidelines for the application of ISO 9001:2000 to computer software

Contempla los aspectos de calidad desde el desarrollo, suministro, adquisición, operación y mantenimiento para software.

ISO/IEC 28000 Specification for security management systems for the supply chain

Su objetivo es mejorar la seguridad de la cadena de suministro mediante el análisis de los riesgos y los planes de reacción adecuados. Para ello, se requiere que la organización evalúe el entorno de seguridad en el que opera relativos a la financiación, manufactura, gestión de la información y las ubicaciones de embalaje almacenamiento, transporte y localización. De forma que determine si se implementan unas medidas de seguridad adecuadas y si ya existen otros requisitos reglamentarios que la organización cumpla.

8.2.2 Seguridad de TI

ISO/IEC 27000:2009

Es la introducción y descripción de las normas de la familia 270xx.

ISO/IEC 27001:2005, Information security management systems — Requirements

Es el conjunto formal de especificaciones que describe el "*Information Security Management System* (ISMS)" (SGSI en español) contra el cual se puede certificar una organización.

ISO/IEC 27002:2005, Code of practice for information security management

Es el conjunto de buenas prácticas y controles aplicables a la gestión de la Seguridad de los sistemas de información.

ISO/IEC 27003, Information security management system implementation guidance

Guía facilitadora para la implantación de la ISO 27001. Describe el proceso de diseño y especificación del ISMS desde el inicio hasta la implementación final.

ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems

Este estándar sirve de guía a los cuerpos de certificación para especificar los procesos formales de certificación de los sistemas de gestión de la seguridad de la información como terceras partes implicadas en el proceso.

ISO/IEC 27007, Guidelines for information security management systems auditing

Norma directamente relacionada con la ISO 19011. Proporciona las directrices para las competencias de los acreditadores y auditores de sistemas ISMS y las necesidades de cumplimiento del estándar ISO/IEC 27001.

ISO 21827 Systems Security Engineering Capability Maturity Model (SSE CMM)

Describe las características esenciales del proceso de ingeniería de Seguridad que debe existir en una organización y recoge prácticas existentes en la industria.

8.2.3 Desastre y Recuperación

ISO/IEC 24762 Guidelines for information and communications technology disaster recovery services

Proporciona directrices para la provisión de servicios de recuperación de desastres para las tecnologías de la información y las comunicaciones (ICT DR) aplicable a servicios propios (*in house*) como externos (*outsourced*).

BS 25999 Business Continuity Management

Norma multi-parte Británica de la Gestión de Continuidad del Negocio. La parte primera establece los procesos, principios y terminología junto con un conjunto de buenas prácticas para todo el ciclo de vida de la gestión de la continuidad. La parte segunda proporciona las especificaciones formales frente a las cuales auditar el cumplimiento de las organizaciones. Se convertirá en la futura ISO 22301 *Societal security - Preparedness and continuity management systems – Requirements.*

ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity

Basado en la antigua BS 25777:2008 *Information and communications technology continuity management. Code of practice*. Proporciona directrices sobre los conceptos y principios que subyacen en los aspectos de la información y las comunicaciones en el aseguramiento de la continuidad de negocio. Este estándar abarca todos los eventos e incidentes y no sólo los relacionados con la seguridad de la información apoyándose en el concepto ICT *Readiness for Business Continuity* (IRBC).

ISO/PAS 22399 Societal security - Guideline for incident preparedness and operational continuity management

Proporciona directrices para desarrollar por parte de una organización sus propios criterios de rendimiento para la preparación de incidentes, la continuidad de las operaciones, y el diseño de un sistema de gestión permite a una organización medir su "resiliencia" de forma consistente.

8.2.4 Métricas e Indicadores

ISO/IEC 27004, Information security management — Measurement

Proporciona directrices sobre el desarrollo y uso de medidas y métricas para evaluar la efectividad de los controles establecidos y del propio ISMS implantado en la organización.

8.2.5 Auditoría y Control

ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing ISO 19011 Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental

Esta Norma Internacional proporciona orientación sobre la gestión de los programas de auditoría, la realización de auditorías internas o externas de sistemas de gestión de la calidad y/o ambiental, así como sobre la competencia y la evaluación de los auditores.

8.2.6 Gestión de Riesgos

ISO/IEC 27005:2008, Information security risk management

Proporcionar directrices para la gestión de riesgos en Seguridad TI y apoya el enfoque basado en riesgos de los conceptos propuestos por la ISO/IEC 27001 y ISO/IEC 27002.

ISO 31000 Risk management — Principles and guidelines

Esta norma sustituye a la AS/NZS 4360. Proporciona las directrices y principios para la implementación de una gestión de riesgos estableciendo como una organización debería entender su contexto específico en el que implementar la gestión de riesgos. Por tanto, la norma cubre la gestión de riesgos en un sentido amplio y no centrada específicamente en la seguridad de la información o los riesgos de IT.

ISO/IEC 31010 Risk management – Risk assessment techniques

Proporciona directrices para la selección y aplicación sistemática de técnicas para la evaluación de riesgos como una parte integral de la gestión de riesgos para que los gestores puedan entender los riesgos que pueden afectar los objetivos del negocio de forma que se puedan evaluar y proporcionar controles efectivos y adecuados para la mitigación de los mismos.

8.2.7 Seguridad Laboral

OHSAS 18001 Sistemas de gestión de la seguridad y salud en el trabajo

Especifica los requisitos para un sistema de gestión de la Seguridad y Salud en el Trabajo (SST), destinados a permitir que una organización controle sus riesgos de SST y mejore su desempeño protección de la SST.

8.2.8 Certificación y Acreditación

ISO/IEC 15408:2008 (Information technology -- Security techniques -- Evaluation criteria for IT security

Esta norma multi-parte describe los criterios comunes (CC) de evaluación para la seguridad de las tecnologías de información (IT). Los productos que evalúan contra esta norma logran un nivel definido de aseguramiento en cuanto a la capacidad de seguridad de la información se refiere. Este nivel de evaluación es reconocido por todos los miembros adheridos al acuerdo (arreglo) de *Common Criteria*.

ISO/IEC TR 19791:2010 Information technology – Security techniques – Security assessment of operational systems

Este informe técnico extiende la evaluación de productos establecida en la norma de ISO/IEC 15408 de *Common Criteria*, a los sistemas operacionales proporcionado las guías y criterios de evaluación de seguridad para estos sistemas al tener en cuenta el entorno del sistema operacional a evaluar así como la posibilidad de descomponer un

sistema operacional complejo en dominios de seguridad que pueden ser evaluados independientemente.

8.2.9 Coordinación y Respuesta

ISO/IEC 18043 Selection, deployment and operations of Intrusion Detection Systems (IDS)

Proporciona un guía para entender los beneficios y limitaciones de un IDS: como realizar la integración de las detección de intrusos en la organización, el desarrollo de una estrategia y plan de implementación para un IDS, cómo gestionar efectivamente las salidas, así como integrar el sistema IDS en las practicas de la organización teniendo en cuenta las necesidades legales y de privacidad que afectan a un IDS.

ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management

Los incidentes siempre van a ocurrir de una u otra forma debido a las imperfecciones e inefectividad de los controles preventivos. Por lo que la gestión efectiva de incidentes implica controles defectivos y correctivos designados para minimizar el impacto adverso y aprender las lecciones en términos de la mejora del ISMS, especialmente la implementación de controles preventivos más eficientes.

---oo0Ooo----