sedian

Seguridad Digital
de Andalucía

Real Decreto-Ley 12/2018, de seguridad de las redes y sistemas de información y Ley 8/2011, de Protección de Infraestructuras Críticas

Junta de Andalucía

Índice.

1. Introducción.

Real Decreto-ley de seguridad de las redes y sistemas de información (Real Decreto-ley 12/2018)

- En el ámbito europeo, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems)

1. Introducción.

Real Decreto-ley de seguridad de las redes y sistemas de información (Real Decreto-ley 12/2018)

- Esta norma integra requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y **requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.**

1. Introducción.

Ley de Protección de Infraestructuras Críticas (Ley 8/2011, de 28 de abril)

- Para la protección de las infraestructuras críticas se hace imprescindible, por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra sociedad y, por otro, **diseñar una estrategia** que será desarrollada durante la ponencia **incluyendo medidas de prevención y protección eficaces contra las posibles amenazas.**

2. Real Decreto-ley de seguridad de las redes y sistemas de información (Real Decreto-ley 12/2018).

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad

2.2 Responsable de Seguridad (CISO), Roles y Responsabilidades

2.3 Gestión de incidentes de seguridad

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad.

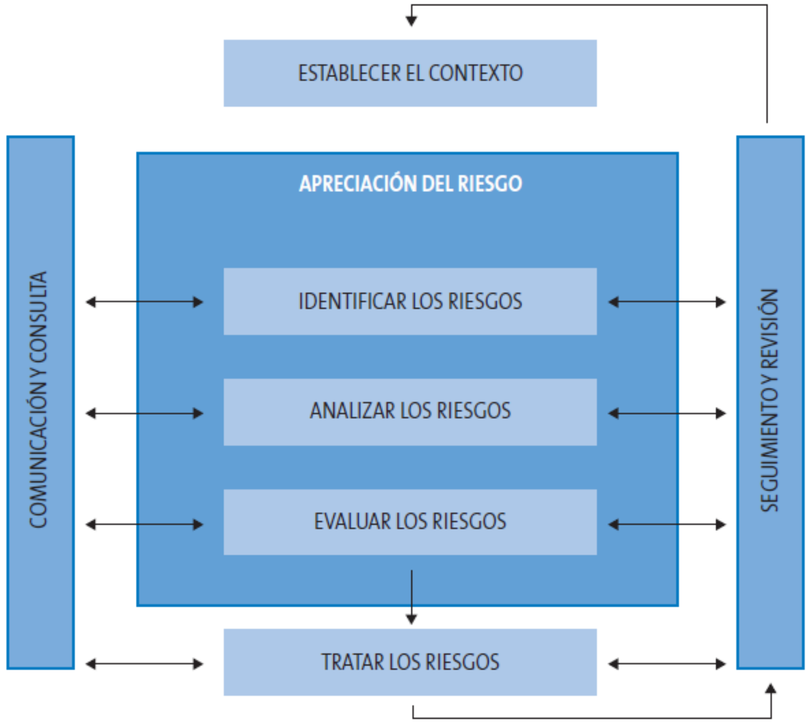
Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las **medidas técnicas y de organización** adecuadas y proporcionadas **para gestionar los riesgos** que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios.

Las medidas a considerar, como mínimo, deben cubrir los siguientes aspectos:

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad.

a) **Análisis y gestión de riesgos.**
b) **Gestión de riesgos de terceros** o proveedores
c) **Catálogo de medidas de seguridad**, organizativas, tecnológicas y físicas.
d) **Gestión del personal** y profesionalidad.
e) **Adquisición de productos o servicios de seguridad.**
f) **Detección y gestión de incidentes.**
g) **Planes de recuperación** y aseguramiento de la **continuidad** de las operaciones.
h) **Mejora continua.**
i) **Interconexión de sistemas.**
j) **Registro de la actividad de los usuarios.**

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad. Gestión de Riesgos.



- Distribución de malware.
- Configuración de malware.
- Robo.
- Sabotaje.
- Interrupciones.
- DoS (Denegación de servicio).
- Acceso no autorizado a información.
- Modificación no autorizada de información.
- Fuga de Información.
- *Phishing.*
- *Proveedor Comprometido*

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad. Ej. Catálogo de medidas de Seguridad.

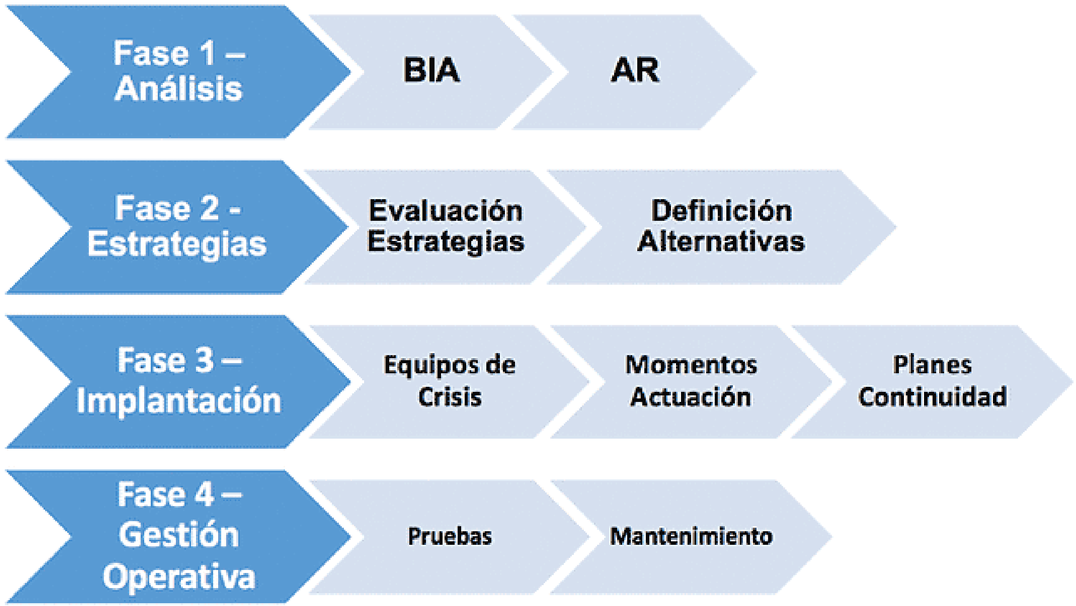
ISO 27001

Anexo A: 14 Dominios, 35 objetivos de control y 114 controles

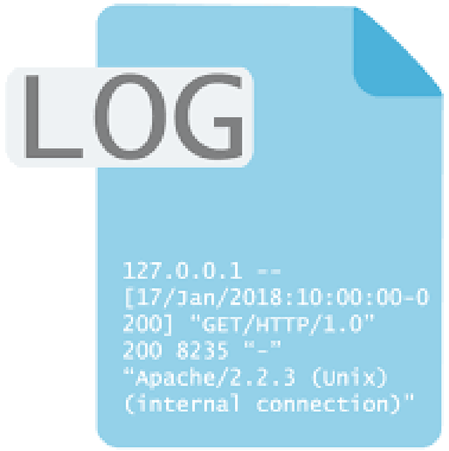
- A.5 Políticas de seguridad de la información
- A.6 Organización de la seguridad de la información
- A.7 Seguridad relativa a los recursos humanos
- A.8 Gestión de activos
- A.9 Control de acceso
- A.10 Criptografía
- A.11 Seguridad física y del entorno
- A.12 Seguridad de las operaciones
- A.13 Seguridad de las comunicaciones
- A.14 Adquisición, desarrollo y mantenimiento de sistemas de información
- A.15 Relación con proveedores
- A.16 Gestión de incidentes de seguridad de la información
- A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- A.18 Cumplimiento

Catálogo de controles de la ISO 27001

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad. Continuidad.



2.1 Medidas para el cumplimiento de las obligaciones de Seguridad. Registro de Actividades.



EJEMPLO DE NIVEL DE EFECTIVIDAD DE REGISTRO DE ACTIVIDAD

Nivel BAJO
Se activarán los registros de actividad en los servidores.

Nivel MEDIO
Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO
Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.

2.1 Medidas para el cumplimiento de las obligaciones de Seguridad.

Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica, en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes.

Sin perjuicio de lo anterior, podrán tenerse en cuenta otros estándares reconocidos internacionalmente.

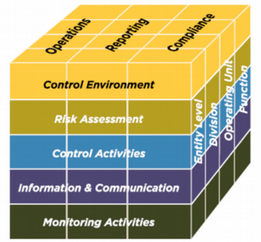
ens Esquema Nacional de Seguridad

ISO

27001
22301
20000-1
31000
27005
...

NIST

COBIT 5
AN ISACA® FRAMEWORK



2.2 Responsable de Seguridad (CISO), Roles y Responsabilidades. Competencias.

PUNTOS CLAVE DEL RESPONSABLE DE SEGURIDAD

- MEDIDAS TÉCNICAS Y ORGANIZATIVAS
- GESTIÓN DE RIESGOS
- NOTIFICACIÓN DE INCIDENTES
- COMPETENCIAS

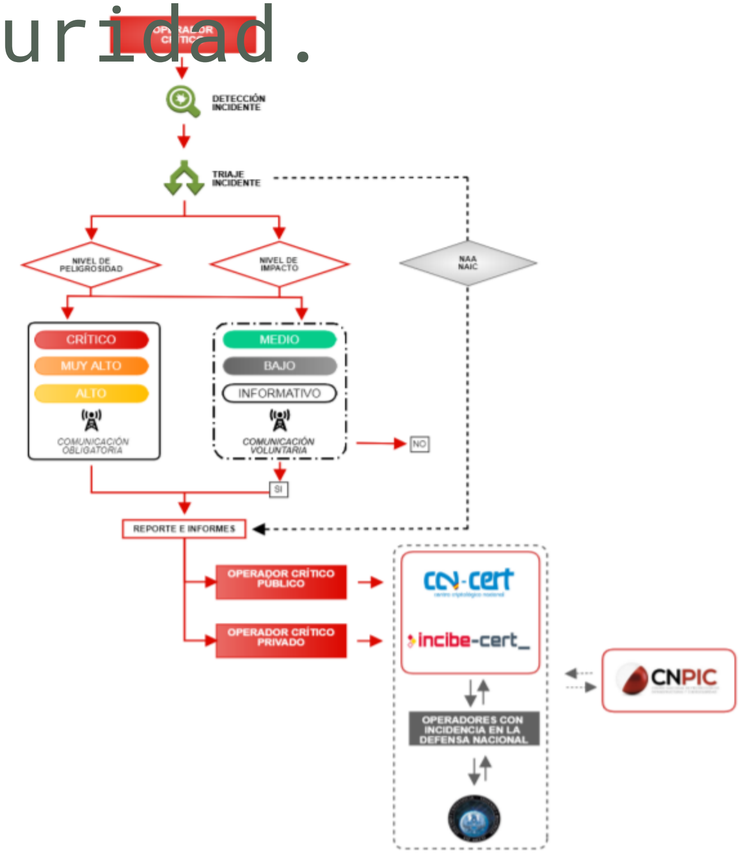
2.3 Gestión de incidentes de seguridad.

Obligaciones de notificación de incidentes de los operadores de servicios esenciales

Los operadores de servicios esenciales notificarán a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios**, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto,**

2.3 Gestión de incidentes de seguridad.

La siguiente imagen se pueden observar los flujogramas informativos en los que se detalla el proceso de notificación y gestión de un incidente y el proceso de respuesta operativa ante la comunicación de un ciberincidente acaecido en las redes o sistemas de información que soportan los servicios esenciales prestados por las infraestructuras de un operador.



3. Ley de Protección de Infraestructuras Críticas (Ley 8/2011, de 28 de abril).

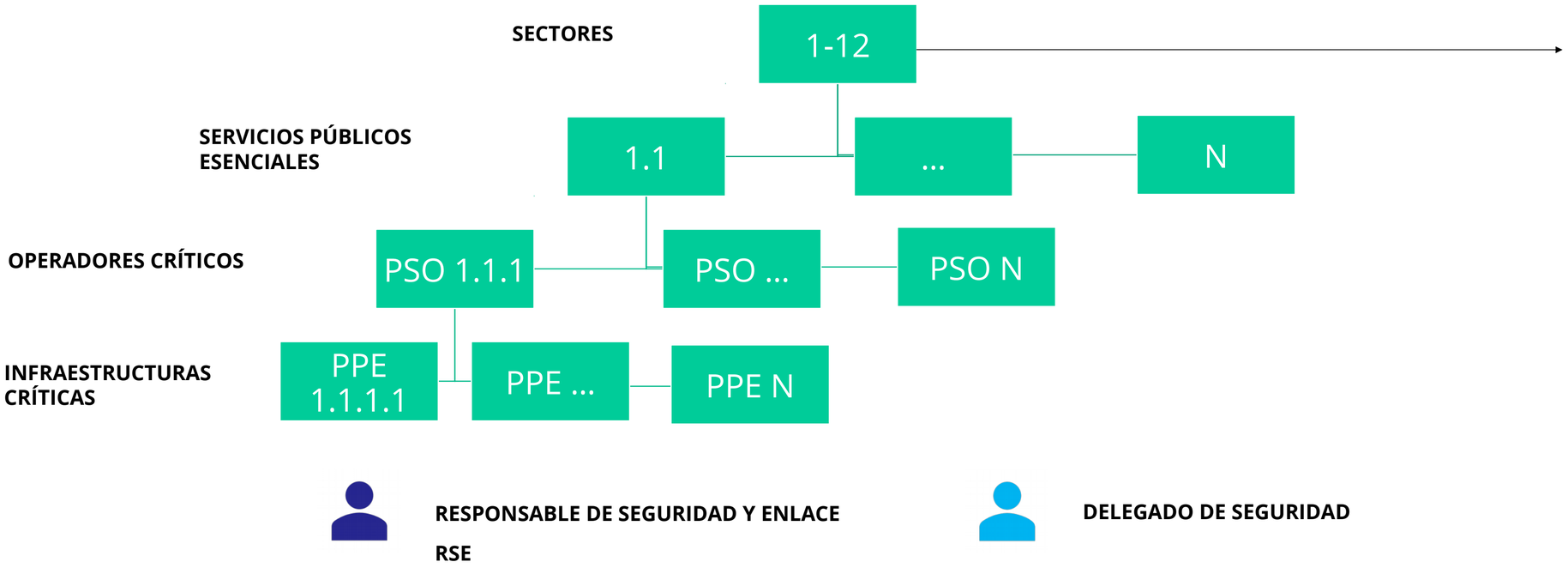
3.1 Conceptos de la LPIC

3.2 RSE y RSI. Responsable de Seguridad y Enlace y Delegado/s de Seguridad. Roles y Responsabilidades

3.3 PSO. Plan de Seguridad del Operador

3.4 PPE. Plan/es de Protección Específico/s

3.1 Conceptos de la LPIC.



- Genérico
- Industria Química
- Agua
- Tecnología información y Comunicaciones
- Alimentación
- Instalaciones Investigación
- Industria Nuclear
- Espacio
- Energía
- Transporte

3.2 RSE y RSI. Responsable de Seguridad y Enlace y Delegado/s de Seguridad. Roles y Responsabilidades.

RESPONSABLE DE SEGURIDAD Y ENLACE

- Representar al operador crítico ante la Secretaria de Estado de Seguridad:
  - En materias relativas a la seguridad de sus infraestructuras.
  - En lo relativo a los diferentes planes especificados en el Real Decreto.
- Canalizar las necesidades operativas e informativas que surjan entre el operador crítico y el CNPIC.

DELEGADO DE SEGURIDAD

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

3.3 PSO. Plan de Seguridad del Operador.

1. Finalidad

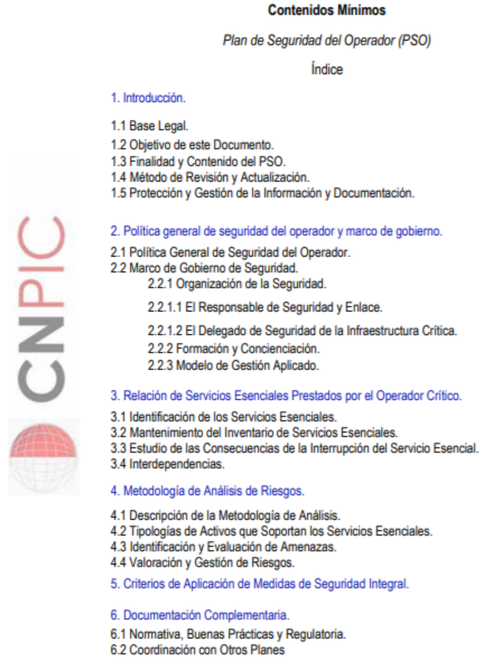
1. Política general de seguridad del operador y marco de gobierno

1. Relación de Servicios Esenciales Prestados por el Operador Crítico

1. Metodología de Análisis de Riesgos

1. Criterios de aplicación de medidas de Seguridad Integral

1. Documentación complementaria



Contenidos Mínimos

Plan de Seguridad del Operador (PSO)

Índice

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

3.4 PPE. Plan/es de Protección Específico/s.

1.Introducción

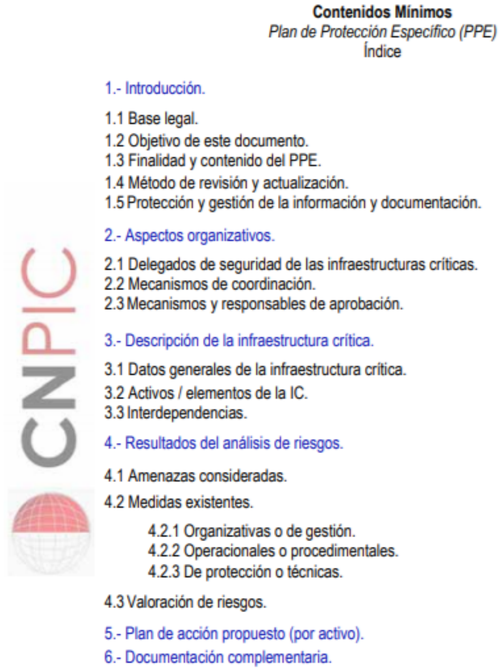
1.Aspectos Organizativos

1.Descripción de la Infraestructura Crítica

1.Resultado del Análisis de Riesgos

1.Plan de Acción propuesto (por activo)

1.Documentación complementaria



Contenidos Mínimos
Plan de Protección Específico (PPE)
Índice

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

3.5 PSO y PPE. Política y Metodología.

La política de Seguridad plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:
1.Los objetivos o misión de la organización.
2.El marco legal y regulatorio.
3. Los roles o funciones de seguridad,
4. La estructura del comité o los comités

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:
1.ACTIVOS
2.AMENAZAS
3.CONTROLES Y SU EFICACIA
4.ESTIMACIÓN DE IMPACTO
5.ESTIMACIÓN DE RIESGO, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

magerit
METHODOLOGY FOR INFORMATION SYSTEMS
RISK ANALYSIS AND MANAGEMENT

3.5 PSO y PPE. Resultados de Riesgos.

CONTROLES Y MEDIDAS
DE SEGURIDAD

GESTIÓN DE RIESGOS

Anexo. Gestión de incidentes de seguridad.

Nivel crítico:

– Afecta apreciablemente a la Seguridad Nacional.
– Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
– Afecta a una infraestructura crítica.
– Afecta a sistemas clasificados SECRETO.
– Afecta a más del 90 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.
– El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
– Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.
– Extensión geográfica supranacional.
– Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

Anexo. Gestión de incidentes de seguridad.

Nivel muy alto:

– Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
– Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
– Afecta a un servicio esencial.
– Afecta a sistemas clasificados RESERVADO.
– Afecta a más del 75 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.
– El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
– Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.
– Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias).
– Daños reputacionales a la imagen del país (marca España).
– Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Anexo. Gestión de incidentes de seguridad.

Nivel alto:

– Afecta a más del 50 % de los sistemas de la organización.
– Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.
– El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.
– Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.
– Extensión geográfica superior a 3 CC.AA.
– Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

2.3 Gestión de incidentes de seguridad – Anexo.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel crítico:
– APT.

Nivel muy alto:
– Distribución de malware.
– Configuración de malware.
– Robo.
– Sabotaje.
– Interrupciones.

Nivel alto:
– Pornografía infantil, contenido sexual o violento inadecuado.
– Sistema infectado.
– Servidor C&C (Mando y Control).
– Compromiso de aplicaciones.
– Compromiso de cuentas con privilegios.
– Ataque desconocido.
– DoS (Denegación de servicio).
– DDoS (Denegación distribuida de servicio).
– Acceso no autorizado a información.
– Modificación no autorizada de información.
– Pérdida de datos.
– *Phishing.*

2.3 Gestión de incidentes de seguridad – Anexo.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel medio:
– Discurso de odio.
– Ingeniería social.
– Explotación de vulnerabilidades conocidas.
– Intento de acceso con vulneración de credenciales.
– Compromiso de cuentas sin privilegios.
– Desconfiguración.
– Uso no autorizado de recursos.
– Derechos de autor.
– Suplantación.
– Criptografía débil.
– Amplificador DDoS.
– Servicios con acceso potencial no deseado.
– Revelación de información.
– Sistema vulnerable.

Nivel bajo:
– *Spam.*
– Escaneo de redes (*scanning*).
– Análisis de paquetes (*sniffing*).
– Otros.

sedian Seguridad Digital de Andalucía