GOBIERNO DE ESPAÑA
MINISTERIO DE POLÍTICA TERRITORIAL Y FUNCIÓN PÚBLICA

CCN
centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 844

## ANEXO I: PREGUNTAS FRECUENTES (FAQ)


Octubre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.10.17 12:49:33 +02'00'



NIPO: 083-19-023-3

Fecha de Edición: octubre 2019

# PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El 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 (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# Índice

## 1. PREGUNTAS GENERALES DE USO DE LA HERRAMIENTA INES

1. **Pregunta. ¿Por qué no puedo ver el cuadro de mando?**
   Respuesta. Para que el cuadro de mando se active es necesario que el nivel de rellenado de la herramienta **supere el 50% y que estén registrados los valores máximos de cada dimensión de seguridad** en la pestaña de "Categorización de los sistemas", con el fin de que haya la suficiente cantidad de información como para que se pueda generar un número significativo de indicadores y sus comparaciones.
2. **Pregunta. ¿Por qué no puedo generar el informe de resultados?**
   Respuesta. Para que se genere el informe de resultados es necesario que el nivel de rellenado de la herramienta **supere el 50% y que estén registrados los valores máximos de cada dimensión de seguridad** en la pestaña de "Categorización de los sistemas", con el fin de que haya la suficiente cantidad de información como para que se pueda generar un número significativo de indicadores y sus comparaciones.
3. **Pregunta. ¿Por qué no puedo editar los datos?**
   Respuesta. Está en una ficha de una campaña anterior, no tiene permisos de escritura o es supervisor de dicha ficha. Tiene que acceder - en el menú lateral izquierdo - a la ficha de la cual su rol sea "Operador" o a una ficha del año en curso y que disponga de permisos de escritura. Recuerde que en la campaña actual no se permite editar los datos de la sección **" Datos Generales".**
4. **Pregunta. ¿Por qué no se guardan los datos que he introducido?**
   Respuesta. Los datos que ha introducido no son correctos, te aparecerá un mensaje en la zona superior derecha indicando el motivo del error.
5. **Pregunta. ¿Qué indica la campana situada en la barra de navegación del menú superior derecho?**
   Respuesta. Dicha campana muestra las alertas existentes para el usuario. Muestran mensajes tales como la fecha de cierre de campaña o si el organismo se encuentra o no supervisado, entre otros.
6. **Pregunta. ¿Cómo puedo visualizar y/o insertar comentarios?**
   Respuesta. Para poder insertar un comentario en una cuestión determinada, deberá pulsar el icono situado a la derecha de la cuestión siempre y cuando ésta se encuentre habilitada. Tras rellenar el comentario, al igual que en la campaña anterior, el texto se guardará de forma automática.
   Si por el contrario desea mostrar todos los comentarios de la pestaña, bastará con pulsar el botón "Mostrar todos los comentarios" situado bajo el botón de las FAQ. Dicho botón, puede mostrar y ocultar los comentarios sin necesidad de hacer clic en cada comentario de forma individual.

## 2. IDENTIFICACIÓN DEL ORGANISMO

7. **Pregunta. ¿Si soy un organismo de autonómico o estatal, debo indicar la provincia y/o comunidad autónoma en la que se encuentra mi sede central?**

   Respuesta. No. Los organismos estatales no deben completar el dato de comunidad autónoma ni el de provincia, y los organismos autonómicos no deben completar el dato de la provincia. Dichas preguntas permanecerán desactivadas, en función de la respuesta a la cuestión del "Tipo de organismo".

8. **Pregunta. ¿Qué es el DIR3 y cómo debería rellenarlo?**

   Respuesta: El código DIR3, del Directorio Común de Unidades Orgánicas y Oficinas, es un identificador único de cada organismo, unificado y común a toda la Administración, cuyo objetivo es simplificar el mantenimiento de la información y la identificación de los organismos.

   Este código alfanumérico de 9 caracteres identifica el tipo de organismo, así como la existencia o no, de organismos dependientes y/o la dependencia del organismo propio con respecto a otro.

   Debe rellenar esta pregunta con su código DIR3, si lo desconoce consúltelo en el portal de administración electrónica www.administracionelectronica.gob.es

9. **Pregunta. ¿Cómo debo interpretar el concepto de sistema de información?**

   Respuesta. Se debe interpretar como un único sistema de información al conjunto de servidores, aplicaciones, middleware, bases de datos e infraestructuras utilizados para la prestación de uno o más servicios electrónicos. Ejemplos habituales de sistemas de información que se consideran de forma individual son la sede electrónica, la plataforma de contabilidad, el conjunto de sistemas que se utilizan para la contratación electrónica, etc.

10. **Pregunta. ¿Es normal tener muchos sistemas de información?**

    Respuesta. Dado que el concepto de sistema de información no tiene una interpretación muy concisa, el número de sistemas de información identificados por cada organismo es muy variable.

    No obstante, se suele dar una pauta: si el organismo tiene sistemas de información relativamente nuevos, el número de sistemas de información suele ser más bajo, ya que se utilizan la misma infraestructura y plataformas transversales sobre las que se implementan muchos servicios pero que acaban dependiendo de tantos elementos comunes que no se pueden distinguir muchos sistemas de información aislados.

    Si los sistemas de información son más antiguos, los servicios suelen ser más independientes, lo que suele provocar arquitecturas más verticales y por lo tanto un mayor número resultante de sistemas de información.

11. **Pregunta. ¿Cómo relleno el número de sistemas de información?**

    Respuesta. El número de sistemas de información se debe extraer del análisis de riesgos y/o del alcance del proceso de seguridad.

**12. Pregunta. ¿Cómo debo interpretar el dato de número total de usuarios?**

Respuesta. Se debe interpretar considerando al personal interno del organismo, tanto propio como subcontratado, sin considerar a los receptores de los servicios electrónicos prestados (ciudadanos, personas jurídicas, alumnos, etc.). Otra forma de interpretarlo sería considerar todos los usuarios registrados en el directorio del organismo como personal propio o subcontratado o por el número de cuentas en el sistema, asumiendo que el número de cuentas por persona es prácticamente uno, aunque los administradores de seguridad además dispongan de otras cuentas de servicio.

## 3. CATEGORIZACIÓN DE LOS SISTEMAS

**13. Pregunta. ¿Cómo relleno el dato de nivel máximo de las dimensiones de seguridad (Disponibilidad / Autenticidad /Integridad / Confidencialidad / Trazabilidad)?**

Respuesta. Tienes que revisar todos tus activos esenciales (activos de tipo información y/o de tipo servicio) y/o todos tus sistemas de información, e indicar el valor máximo de entre todos ellos para dichas dimensiones de seguridad. Ver guía CCN-STIC-803 Valoración de los sistemas.

**14. Pregunta. ¿Qué debo hacer si no tengo ningún sistema de alguna categoría?**

Respuesta. Se deberá indicar en la sección de Identificación del Organismo (marcando con '0' en el número de sistemas), de este modo verá deshabilitadas las opciones de registro de datos para esa categoría en todas las solapas en las que la información sea registrada de forma individual por categoría de sistema.

**15. Pregunta. Diferencia entre "No aplica" y "No definido"**

Respuesta. La cumplimentación de los niveles de seguridad asociados a cada categoría de sistema es de carácter obligatorio. Si se marca el valor "No definido" para alguna de las categorías, se considerará que no se ha asignado nivel de seguridad y, por tanto, no se calculará el Indicador de Cumplimiento, no se podrá generar el informe individual, no se podrá mostrar el cuadro de mandos, ni se incluirán los datos en el Informe Anual de Seguridad.

Si se marca el valor "No aplica" en alguna de las dimensiones de seguridad para alguna categoría en concreto, las medidas de seguridad que sólo afecten a dicha dimensión no serán tenidas en cuenta, ni en el cálculo del Indicador de Madurez ni en el del Indicador de Cumplimiento.

El valor "No aplica" está destinado a identificar a aquellas medidas que por las características del sistema no tengan sentido su aplicación (independientemente de la relación de medidas que son de aplicación por cada categoría de sistema, según

Anexo II del RD 3/2010).

## 4. ANÁLISIS Y GESTIÓN DE RIESGOS

**16. Pregunta. ¿Cómo debo interpretar el concepto de activo esencial?**

Respuesta. Un activo esencial es todo aquél activo de tipo información y/o de tipo servicio en tu análisis de riesgos, que son aquellos activos cuyas dimensiones de seguridad han tenido que ser valoradas.

## 5. ACTIVIDADES ORGANIZATIVAS

**17. Pregunta. ¿Cómo debo interpretar el concepto de independencia del responsable de seguridad respecto del responsable del sistema?**

Respuesta. Se debe interpretar considerando que el rol de responsable de seguridad recae sobre una persona distinta a la que ostenta el rol de responsable de sistema. Además, el responsable de seguridad no debe depender del responsable del sistema, porque en este caso su función quedaría claramente mediatizada por su superior, impidiendo la adecuada toma de decisiones.

**18. Pregunta. ¿Cómo debo interpretar el concepto de normas/procedimientos de seguridad implantados?**

Respuesta. Se debe interpretar considerando sólo, del total de normas o procedimientos de seguridad previstos, los que ya han sido desarrollados, aprobados y difundidos.

**19. Pregunta. ¿Cómo debo calcular el porcentaje de normas/procedimientos de seguridad implantados?**

Respuesta. Se puede calcular o bien contabilizando el total de normas/procedimientos previstos y el número de normas/procedimientos implantados o bien realizando una estimación aproximada, plasmada en un número redondo, de acuerdo a las siguientes pautas:

| Porcentaje de avance (%) | Descripción del nivel |
|---|---|
| 0 | *No se ha iniciado la actividad.* |
| 10 | *La actividad está solamente iniciada*. |
| 50 | *La actividad está a medias*. |
| 80 | *La actividad está al 80%.* |
| 90 | *La actividad está prácticamente acabada.* |

| Porcentaje de avance (%) | Descripción del nivel |
|---|---|
| 100 | *La actividad está completa.* |

**Figura 1.- Escala de valoración de las actividades organizativas**

**20. Pregunta. Si ya he concluido la ejecución del plan de adecuación ¿Cómo debo responder a si se mantiene actualizado el plan de adecuación?**

Respuesta. Mantener actualizado el plan de adecuación no sólo supone llevar a cabo la adecuación inicial a las exigencias del ENS, sino también mantener actualizado el plan de acción necesario para gestionar adecuadamente los riesgos del organismo. Por lo tanto, mantener actualizado el plan de adecuación también se puede entender cómo mantener actualizado un Plan de Tratamiento o de Gestión de Riesgos, como consecuencia del correspondiente análisis de riesgos.

## 6. RECURSOS

**21. Pregunta. ¿Cómo debo interpretar el dato de número de administradores de seguridad?**

Respuesta. Se debe interpretar como el sumatorio del número de personas con permisos de administrador sobre la seguridad del sistema (ASS) o de algún componente del sistema (se incluyen tanto servidores como equipos de usuario final y los que administran productos de seguridad) y del número de personas con permisos de administrador de sistemas, si tienen control de administración sobre las funciones de seguridad del sistema. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios de seguridad, se imputarán también los recursos humanos indicados en el contrato de prestación de servicios.

No se consideran administradores de seguridad y por tanto se excluyen aquellas personas que dentro de una aplicación específica su rol es el de administrador solo y parcialmente de dicha aplicación (por ejemplo, controlando exclusivamente los cambios de claves de las cuentas de usuarios de su departamento, sin posibilidad de cambiar privilegios de acceso).

No se hará distinciones en función de la categoría de la persona.

A continuación, se detallan las actividades que desarrolla la persona que ostente alguno de los dos (2) roles relacionados con la administración:

1. El administrador de la seguridad del sistema o administrador de Seguridad (ASS) es aquella persona que:
   - Implementa, gestiona y supervisa las medidas de seguridad aplicables al Sistema de Información.
   - Gestiona, configura y actualiza el hardware y software en el que se basan

los mecanismos y servicios de seguridad del Sistema de Información.

- Gestiona las autorizaciones concedidas a los usuarios y monitoriza que la actividad realizada se ajusta a lo autorizado.
- Monitoriza el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema
- Aplica los Procedimientos Operativos de Seguridad y aprobar los cambios en la configuración vigente del Sistema de Seguridad

2. El administrador del sistema (AS) es la persona que tiene como misión, la implantación, configuración y mantenimiento de los servicios TIC.

Se destaca que es habitual que ambos roles recaigan sobre la misma persona o grupo de personas.

**22. Pregunta. ¿Cómo debo interpretar el dato de número de personas con responsabilidad en la STIC?**

Respuesta. Se debe interpretar como el número de personas con responsabilidad en la seguridad TIC que incluye el número de administradores de seguridad, y otras personas con otras actividades de seguridad TIC, como responsables, directivos, sin ser administradores de seguridad propiamente dicho. Es decir, será el sumatorio de los Administradores de Seguridad del Sistema (ASS), de los Responsables del Servicio (RSERV), del Responsable de la Información (RINFO), de los Responsables del Sistema (RSIS) y del Responsable de la Seguridad (RSEG). Su valor siempre será igual o superior al número de administradores de seguridad.

Ejemplos:

1. Una empresa tiene un Responsable de la Información, un Responsable del Servicio, un Responsable del sistema, tres Responsables del Sistema Delegados y un Responsable de la Seguridad Física. Además, tiene dos Administradores de la Seguridad del Sistema, uno de ellos encargado del aseguramiento de la prestación del servicio y el otro encargado de la protección de la información.
   - Número de administradores de seguridad: 2
   - Número de personas con responsabilidad sobre la seguridad TIC: 8
2. Una empresa tiene una persona que tiene el cargo de Responsable de la Información y Responsable del Servicio y otra persona tiene el cargo de Responsable del sistema. Además, tiene un Administradores de la Seguridad del Sistema y 3 Administradores de la Seguridad del Sistema Delegados, dos de ellos encargados de la configuración y actualización del hardware y software y otro encargado de la gestión de autorizaciones.
   - Número de administradores de seguridad: 4
   - Número de personas con responsabilidad sobre la seguridad TIC: 6
3. Una empresa tiene un Responsable de la Información, un Responsable del

sistema, tres Responsable de Seguridad, dos de ellos son Responsables de Seguridad Delegados y un Administrador de la Seguridad del Sistema.

- Número de administradores de seguridad: 1
- Número de personas con responsabilidad sobre la seguridad TIC: 6

4. Una empresa tiene un Comité de Seguridad de la Información formado por un Responsable de Seguridad de la Información y 3 representantes de las distintas áreas de la empresa, un Responsable del sistema, un Responsable de Seguridad y un Administrador de la Seguridad del Sistema.
   - Número de administradores de seguridad: 1
   - Número de personas con responsabilidad sobre la seguridad TIC:4

**23. Pregunta. ¿Cómo debo interpretar el concepto de administrar la seguridad de las plataformas y/o infraestructuras?**

Respuesta. Se debe interpretar considerando que administrar la seguridad de una plataforma y/o infraestructura supone administrar las cuentas y/o contraseñas de los usuarios, sus privilegios de acceso, el bastionado o los registros (logs) de actividad de dichas plataformas y/o infraestructuras.

**24. Pregunta. ¿Cómo debo interpretar el concepto de productos de seguridad?**

Respuesta. Se debe interpretar considerando productos de seguridad como todos aquellos productos tecnológicos cuya finalidad principal es la seguridad: Gestores de identidades y accesos, gestores de contraseñas, herramientas contra código dañino y correo basura, cifrado, firma electrónica, sellado de tiempo, cortafuegos (firewall), Sistemas de detección de intrusiones (*Intrusion Deteccion Systems IDS*), Sistemas de prevención de intrusiones (*Intrusion Prevention Systems IPS*), Sistemas de Información de Seguridad y Administración de eventos (*Security Information and Event Management SIEM*),filtros de contenidos, equipos y sistemas trampa (*Honeypot*), limpieza de metadatos, herramientas de auditoría, etc.

**25. Pregunta. ¿Cómo debo interpretar el concepto de fracción de horas dedicadas a la Seguridad de las TIC?**

Respuesta. Se refiere a la fracción de horas STIC sobre el total de horas dedicadas a las TIC. No se hará distinciones en función de la categoría de la persona. Suma lo mismo personal fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios, se imputará en este apartado de horas dedicadas la carga de trabajo indicada en el contrato de prestación de servicios.

Dedicación STIC incluye todas las tareas relacionadas con la Seguridad de las TIC. Pueden usarse las tareas a las que hace mención el ENS como inventario:

1. Tareas técnicas: preventivas y de resolución de incidentes.
2. Tareas administrativas, incluyendo contratación de personas, bienes y servicios.
3. Tareas de concienciación y formación.
4. Tareas de comunicación con las autoridades.

**26. Pregunta. ¿Cómo debo interpretar el concepto de fracción del presupuesto dedicado a seguridad TIC respecto al presupuesto dedicado a las TIC?**

Respuesta. Se debe interpretar como la fracción obtenida al sumar todos los recursos económicos dedicados a la subcontratación de administradores de seguridad, a la contratación de cursos de formación y concienciación, a la contratación de servicios de seguridad, a la compra de productos de seguridad y al mantenimiento y/o soporte de los productos de seguridad y dividirla por el presupuesto dedicado a las TIC, expresando el resultado en %.

**27. Pregunta. ¿Cómo debo interpretar el concepto de servicios de seguridad?**

Respuesta. Se debe interpretar como todos aquellos servicios de asesoría, consultoría o auditoría sobre aspectos específicos de seguridad, así como todos aquellos servicios de externalización de procesos de seguridad (Centro Operativo de ciberseguridad (*SOC*), etc.).

## 7. INTERCONEXIÓN CON OTROS SISTEMAS

**28. Pregunta. ¿Cuáles son los Niveles de Madurez?**

Respuesta. Los Niveles de Madurez son los siguientes:

- **L0 - Inexistente (0%)**

  Esta medida no existe o no se está siendo aplicada en este momento.

- **L1 - Inicial/ad hoc (10%)**

  En el nivel L1 de madurez, el proceso existe, pero no se gestiona. Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.

- **L2 - Reproducible, pero intuitivo (50%)**

  En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y riesgo.

- **L3 - Proceso definido (80%)**

  Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso

general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel L2 y el nivel L3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel L2, y que se gestiona en el nivel L3.

- **L4 - Gestionado y medible (90%)**

  Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, mientras que en el nivel L3, la confianza era solamente cualitativa.

- **L5 - Optimizado (100%)**

  El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

**29. Pregunta. ¿Qué es APP-1: cortafuegos?**

Respuesta. Quiere decir que su acceso a Internet se realiza a través de un dispositivo con funciones de cortafuegos o firewall que se despliega entre la red interna y el exterior.

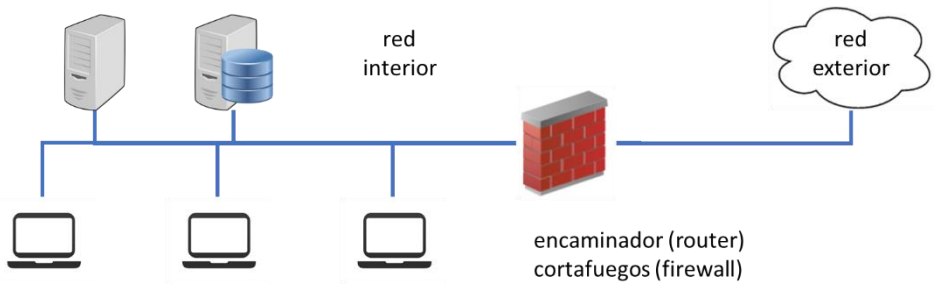


**Figura 2. Arquitectura de protección de perímetro tipo -1 (APP-1)**

El nivel de control de contenidos que permite esta arquitectura es muy limitado. El elemento que hace de cortafuegos está expuesto directamente a ataques desde el exterior y desde el interior. Ver guía CCN-STIC- 811. *Interconexión en el ENS.*

**30. Pregunta. ¿Qué es APP-2: Intermediario o proxy?**

Respuesta: Quiere decir que su acceso a Internet se realiza a través de un intermediario o proxy. Simplemente se despliega un intermediario (*proxy*) entre la red interna y el exterior. El mismo intermediario aúna las funciones de encaminador *(router*).

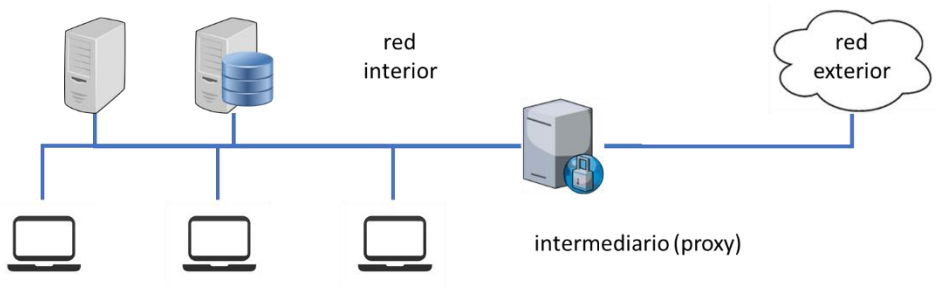


**Figura 3. Arquitectura de protección de perímetro tipo -2 (APP-2)**

Esta arquitectura permite monitorizar y controlar los intercambios de datos y los contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad. El elemento que hace de cortafuegos está expuesto directamente a ataques desde el exterior y desde el interior.

**31. Pregunta. ¿Qué es APP-3: cortafuegos + proxy?**

Respuesta. Quiere decir que su acceso a Internet se realiza a través de un dispositivo con funciones de cortafuegos o firewall, y que la navegación a Internet se realiza a través de un intermediario o proxy de salida instalado en la red interna, de modo que ningún equipo de la red interna accede directamente a Internet, y el cortafuegos evita el acceso directo desde Internet hacia la red interna.

El enrutador controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido a:

1. entre la red interior y en intermediario (proxy).
2. entre el intermediario (proxy) y la red exterior.
3. no pueden pasar paquetes directamente de la red exterior a la interior.

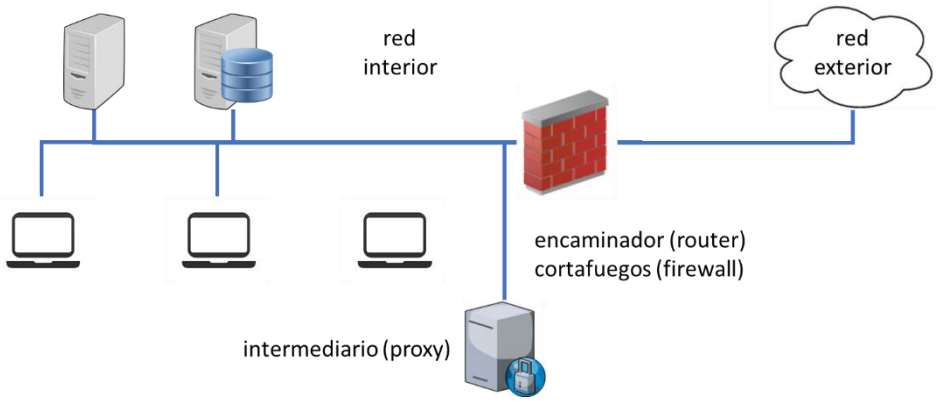


**Figura 4. Arquitectura de protección de perímetro tipo -3 (APP-3)**

Esta arquitectura permite monitorizar y controlar los intercambios de datos y los

contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad.

**32. Pregunta. ¿Qué es APP-4: DMZ con 1 cortafuegos + proxy?**

Respuesta. Quiere decir que su acceso a Internet se realiza a través de un dispositivo con funciones de cortafuegos o firewall con al menos 3 interfaces de red, una que conecta con la red interna, otra que conecta con el acceso a Internet y una tercera que conecta con una red aislada denominada DMZ, en la que se ubica el proxy, de modo que la navegación a Internet se realiza a través de dicha red aislada. Similar al tipo 3; pero el elemento que hace las funciones de cortafuegos y encaminador tiene 3 puertos, uno para la red interior, otro para la exterior y un tercero para el elemento que hace de intermediario. Se dice que el intermediador no está ni en la red interior ni en la interior, sino en una zona intermedia que se suele denominar zona desmilitarizada (DMZ).

El enrutador controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido a:

1. entre la red interior y en intermediario (proxy).
2. entre el intermediario (proxy) y la red exterior.
3. no pueden pasar paquetes directamente de la red exterior a la interior.

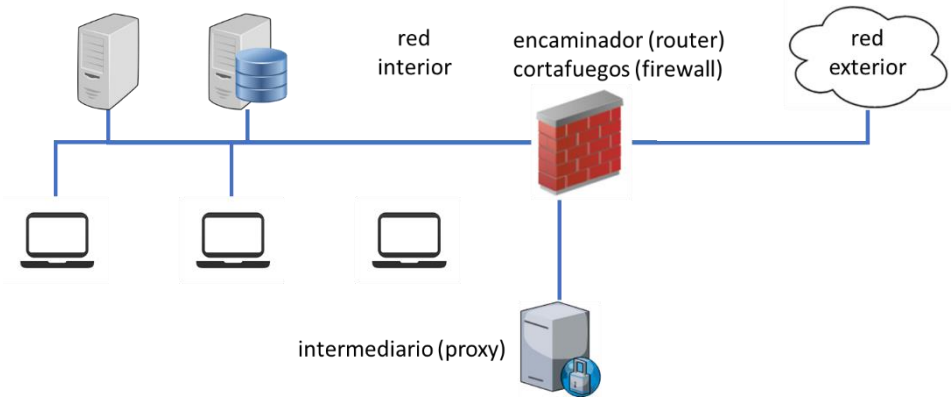


**Figura 5. Arquitectura de protección de perímetro tipo -4 (APP-4)**

Comparado con APP-3, esta arquitectura controla qué flujos de información se permiten entre el interior y el intermediario. Esto reduce la exposición a ataques o errores internos que puedan llevar flujos no autorizados al intermediario.

**33. Pregunta. ¿Qué es APP-5: DMZ con 2 cortafuegos + proxy?**

Respuesta. Quiere decir que su acceso a Internet se realiza a través de una doble capa de firewalls o cortafuegos de diferente fabricante, de modo que uno de ellos protege la red interna, otro protege el acceso a Internet y el proxy se ubica en una red intermedia, aislada de las anteriores, a través del que se lleva a cabo la navegación. Se disponen dos elementos de cortafuegos y un intermediario, pero dejando un tramo de red intermedio. Esta red intermedia se denomina zona desmilitarizada (DMZ), está compuesta por el tramo de red y el intermediario y no

está previsto que circulen paquetes por ella directamente entre los cortafuegos.

El enrutador controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido a:

1. entre la red interior y en intermediario (proxy).
2. entre el intermediario (proxy) y la red exterior.
3. no pueden pasar paquetes directamente de la red exterior a la interior; es decir, un paquete IP no puede pasar directamente de un enrutador al otro, en ningún sentido.

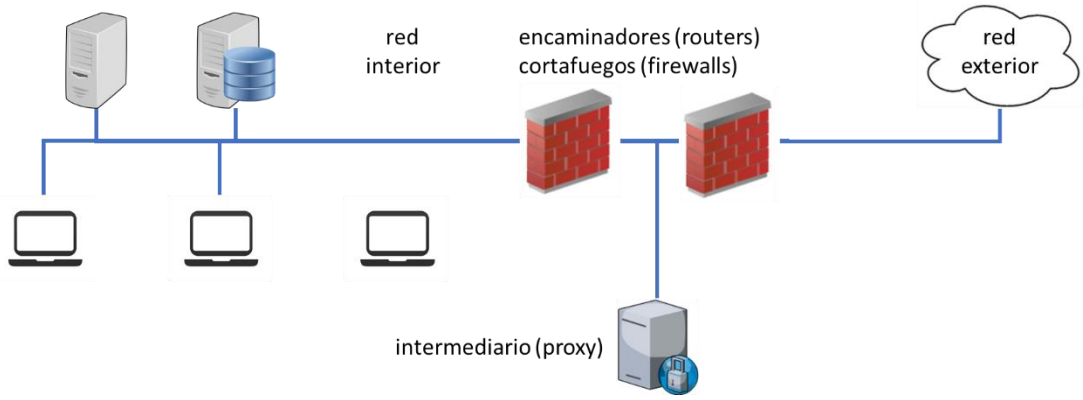


**Figura 6. Arquitectura de protección de perímetro tipo -5 (APP-5)**

Comparado con APP-4 se ha eliminado el riesgo de que una vulnerabilidad en el cortafuegos exterior se traduzca en un acceso directo al interior. En previsión de defectos del software del cortafuegos, se requiere que los cortafuegos sean de fabricantes diferentes.

**34. Pregunta. ¿Cómo debo interpretar la madurez de los diferentes productos tecnológicos y/o herramientas de seguridad?**

Respuesta. Se debe indicar la madurez utilizando los niveles (L0 a L5) que en este caso concreto se pueden interpretar siguiendo las pautas indicadas a continuación:

1. L0: No dispongo de dicha tecnología. La herramienta no está implantada.
2. L1: La herramienta se instaló en su momento, pero nadie se ocupa de ella.
3. L2: La herramienta está instalada y sabemos gestionarla; pero no existe ningún procedimiento para atenderla regularmente y solamente se atiende cuando se ve en dificultades.
4. L3: Está integrada en la infraestructura tecnológica del organismo y es administrada u operada de manera habitual, según el procedimiento establecido, por un técnico con el suficiente conocimiento.
5. L4: No sólo está integrada en la infraestructura tecnológica del organismo, sino que sus resultados se evalúan.
6. L5: El organismo dedica recursos a la mejora continua del desempeño de la herramienta.

## 8. APLICACIÓN DE LA SEGURIDAD

**35. Pregunta. ¿Cómo debo interpretar el concepto de sistemas que emplean contraseñas?**

Respuesta. Se debe interpretar considerando el total de sistemas de información para las que sus usuarios se autentican mediante una contraseña que el propio usuario puede modificar a su voluntad.

**36. Pregunta. ¿Cómo debo interpretar el concepto de sistemas que emplean claves concertadas?**

Respuesta. Se debe interpretar considerando el total de sistemas de información para las que cada usuario se autentica mediante una clave fija acordada y predefinida, que el usuario no puede modificar.

**37. Pregunta. ¿Cómo debo interpretar el concepto de sistemas que emplean *tokens*?**

Respuesta. Se debe interpretar considerando el total de sistemas de información para las que cada usuario se autentica haciendo uso de algo (físico o lógico) que sólo el usuario posee: tarjetas electrónicas, de coordenadas, certificados electrónicos, *token* de autenticación o generador de claves dinámicas como los llaveros OTP (*One Time Password* – contraseña de un solo uso).

**38. Pregunta. ¿Cómo debo interpretar el concepto de usuarios externos?**

Respuesta. Se debe interpretar como los destinatarios o receptores de los servicios electrónicos, que acceden a los mismos desde el exterior del organismo (ciudadanos, personas jurídicas, alumnos, etc.), excluye al personal interno de dicho organismo.

**39. Pregunta. ¿Cómo debo interpretar el concepto de sistemas que emplean doble canal?**

Respuesta. Se debe interpretar considerando el total de sistemas de información para las que a cada usuario se le envía una clave de autenticación de un solo uso a través de un canal de comunicación diferente al utilizado para acceder al servicio (generalmente web + Mensajes cortos (SMS) o mensajería instantánea (tipo *WhatsApp*).

**40. Pregunta. ¿Cómo debo interpretar el concepto de servicios externalizados o subcontratados?**

Respuesta. Se debe interpretar como aquellos servicios TIC recibidos por el organismo que son provistos por entidades con una personalidad jurídica diferente a la del organismo, que puede ser privada o pública, y por lo tanto subcontratados bajo diversas formas jurídicas como convenios, contratos, encomiendas, etc. Además, sólo se deben considerar los servicios TIC sobre los que funcionen los servicios del organismo, sin considerar los que se estén probando o experimentando.

**41. Pregunta. ¿Cómo debo interpretar el concepto de servicios de comunicaciones?**

Respuesta. Se debe interpretar como cualquier servicio de comunicaciones de voz,

datos o comunicaciones unificadas.

42. **Pregunta. ¿Cómo debo interpretar el concepto de servicios de provisión de equipamiento hardware de respaldo?**

    Respuesta. Se debe interpretar como cualquier servicio de provisión de equipamiento hardware que el organismo tendrá que instalar para poder utilizarlo como equipamiento de respaldo, en caso de necesidad.

43. **Pregunta. ¿Cómo debo interpretar el concepto de servicio de instalaciones de respaldo?**

    Respuesta. Se debe interpretar como cualquier servicio que ofrezca al organismo un centro alternativo desde el que ofrecer sus servicios. Este centro de respaldo podrá tener diferentes variantes dependiendo de la inmediatez de uso que ofrezca, pudiendo ser *cold site* (Centro alternativo que sólo provee espacio físico y comunicaciones), *warm site* (Centro alternativo en el que existen sistemas de información sobre los que el organismo tendría que actuar para poder usarlos como sustitutos de los sistemas de información primarios) y *hot site* (Centro alternativo en el que los sistemas de información están completamente sincronizados y operativos respecto de los primarios). Cualquier de estas modalidades se considera servicio de instalaciones de respaldo.

44. **Pregunta. ¿Cómo debo interpretar el concepto de servicios de seguridad gestionada?**

    Respuesta. Se debe interpretar como cualquier servicio externalizado que lleve a cabo una gestión de la seguridad del organismo desde fuera del mismo, tanto de manera general (SOC[1], CERT[2], MSSP[3]) como de manera específica en relación a un servicio de operación de seguridad específico (monitorización, gestión de logs, etc.).

45. **Pregunta. ¿Si en un servidor expuesto en Internet he instalado parches tanto del sistema operativo como del servidor web, cómo debo contabilizarlos?**

    Respuesta. Se debe contabilizar ambos parches, tanto del sistema operativo como los propios del servidor web. Por ejemplo, si de una vez se instalaron 3 parches en el servidor web y 1 parche en el sistema operativo, y otra vez se instalaron 2 parches en el sistema operativo, el número de parches que debe ser contabilizado, para dicho servidor es 6.

46. **Pregunta. ¿Si mi parque de servidores tiene equipos Windows y Linux con diferente política de parcheo, de modo que en Windows he desplegado 30 actualizaciones de seguridad y en Linux he desplegado 7, cómo debo contabilizarlos?**

---

1 Security Operations Center, Centro de Operaciones de Seguridad.

2 Computer Emergency Response Team, Equipo de Respuesta ante Emergencias Informáticas.

3 Managed Security Service Provider, Proveedor de Servicios de Seguridad Gestionada

Respuesta. Se debe contabilizar como la suma de los parches de todos los equipos. Considerando que tengo 10 servidores Windows y uno Linux, el resultado sería: *10 X 30 + 7 X 1 = 307* actualizaciones de seguridad instaladas en mi parque de servidores.

47. **Pregunta. ¿Cómo debo interpretar el concepto de activos esenciales de nivel Alto?**

    Respuesta. Se debe interpretar considerando que los activos esenciales son todos aquellos que son de tipo servicio y/o de tipo información, que son aquellos activos cuyo nivel se valora como alto de acuerdo a lo establecido en el Anexo I del ENS.

48. **Pregunta. ¿Cómo debo interpretar el concepto de horas sin servicio de los servicios esenciales de nivel alto?**

    Respuesta. Se debe interpretar considerando el tiempo que todos los servicios esenciales de nivel alto han estado simultáneamente sin servicio (cortes de servicio globales) en el último año. Si no se ha producido ningún corte global de servicio este dato se debe definir como el mínimo de los tiempos que cada uno de los servicios esenciales ha estado sin servicio.

49. **Pregunta. ¿Cómo debo interpretar el dato de número de horas por persona dedicadas a cursos de formación en el último año?**

    Respuesta. Se debe interpretar como el esfuerzo realizado en cursos de formación STIC por el equipo de seguridad TIC, incluyendo formación a distancia y cursos online.

    El dato se calcula del sumatorio del número de horas de formación (incluidas las realizadas online) por cada curso multiplicado por el número de asistentes y dividido por el número total de personas del equipo de seguridad TIC. Para calcular el número de personas del equipo de seguridad no se hará distinciones en función de la categoría ni si el personal es fijo o temporal, propio, desplazado o subcontratado. Cuando se subcontraten servicios de seguridad, se contabilizarán también los recursos humanos indicados en el contrato de prestación de servicios.

50. **Pregunta. ¿Cómo debo interpretar el dato de número de horas por persona empleadas en cursos de formación o sesiones de concienciación en seguridad?**

    Respuesta. Se debe interpretar como el esfuerzo realizado en cursos de formación y sesiones de concienciación STIC por todo el personal de la organización (incluyendo el personal del equipo STIC), teniendo en cuenta la formación a distancia y cursos online.

    El dato se calcula como la división del sumatorio del número de horas dedicadas (incluidas las realizadas online) por cada curso de formación o sesión de concienciación, multiplicado por el número de asistentes o destinatarios del curso o sesión, entre el número de personas (trabajadores del organismo, propios o subcontratados).

## 9. GESTIÓN DE INCIDENTES

**51. Pregunta. ¿Cuáles son los niveles en los que se clasifican los incidentes de seguridad?**

Respuesta. Los incidentes de seguridad se clasifican en 5 niveles dependiendo de su gravedad, de acuerdo a lo establecido en la Guía CCN-STIC 817 ENS. Gestión de ciberincidentes. Estos niveles son, de mayor a menor, Crítico, Muy Alto, Alto, Medio o Bajo. Solo se solicita información de aquellos que tienen un impacto significativo que incluye las categorías (alto, muy alto y crítico). Ver sección 2.2 de la guía CCN-STIC 824 Informe nacional del estado de seguridad de los sistemas TIC.

**52. Pregunta. ¿Cómo se podrían eliminar los cálculos de los incidentes de seguridad cargados desde fichero?**

Respuesta. Los cálculos relativos a los incidentes de seguridad se pueden eliminar accediendo a la sección de importación de incidentes a través del botón "importación" situado en el menú superior derecho, y posteriormente, pulsando el botón de la papelera junto a la opción deseada, bien sea SAT-SARA, SAT-INET, SAT-ICS, LUCIA.

## 10. INDICADORES CLAVE DE RIESGO

**53. Pregunta. ¿Cómo debo interpretar el concepto de equipos de usuario en los que la configuración y su gestión están bajo el control exclusivo de los técnicos del organismo?**

Respuesta. Se debe interpretar como aquellos equipos en los que el usuario no tiene privilegios de administración sobre el equipo.

**54. Pregunta. ¿Cómo debo interpretar el concepto de equipos de los usuarios internos (BYOD) en los que la configuración y su gestión están bajo el control exclusivo de los técnicos del organismo?**

Respuesta. Se debe interpretar como aquellos equipos BYOD sobre los que se aplican tecnologías MDM/MAM (*Mobile Device Management / Mobile Application Management*). Es decir que el usuario no tiene privilegios de administrador sobre su equipo, aunque sea de su propiedad.

## 11. PRIVACIDAD

**55. Pregunta. ¿Cuáles son los principios relativos al tratamiento?**

Respuesta. El RGPD configura una serie de principios que deben ser respetados cuando se produzca el citado tratamiento. Estos principios son:

- Calidad
- Información
- Legitimación del tratamiento de datos

- Seguridad
- Cesiones a terceros
- Datos especialmente protegidos

**56. Pregunta. ¿Qué es el principio de licitud?**

Respuesta. Los datos de carácter personal deben ser tratados de manera lícita, leal y transparente.

De esta forma, el tratamiento de los datos personales debe estar amparado en alguna de las bases jurídicas que regula el RGPD. Además, este principio excluye que los datos personales sean tratados de forma desleal o sin proporcionar toda la información necesaria sobre el objeto y fines del tratamiento, sus consecuencias y posibles riesgos, obligando a los responsables que tratan los datos personales a ofrecer la mayor transparencia posible sobre el citado tratamiento

Por ejemplo: No se permite utilizar los datos personales para realizar una contratación fraudulenta, dando de alta a un determinado usuario en un servicio que no haya contratado.

**57. Pregunta. ¿Qué es una Evaluación de Impacto?**

Respuesta. Es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.