GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo E.4: Sistemas de prevención de fuga de datos

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Sistemas de prevención de fuga de datos** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.

2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.

3. Además, la aplicación de estos criterios permitirá:

   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.

4. Por lo tanto, los productos catalogados dentro de la familia **Sistemas de prevención de fuga de datos** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.

5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los sistemas para la prevención de fugas de datos o sistemas DLP (*Data Loss Prevention*), son soluciones que protegen las redes de transferencias de datos no autorizadas dentro o fuera de una organización. La pérdida de datos es el proceso por el cual información confidencial abandona el sistema como resultado del establecimiento de una comunicación no autorizada a través de distintos medios: aplicaciones, dispositivos físicos o comunicaciones de red.

7. La prevención de fuga de datos es un término de seguridad computacional que se refiere a sistemas diseñados para detectar y prevenir el uso no autorizado de información confidencial que identifican, monitorizan y protegen datos "en uso" (*endpoints*), "en movimiento" (acciones de red) o datos "en reposo" (almacenamiento de datos) por medio de inspecciones profundas de contenido, análisis de la seguridad contextual de una transacción (atributos del originador, objetos de datos, medio, tiempos, destinos), etc.

2.2 CASODE USO

8. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan tres casos de uso para esta familia de productos tal como se definen a continuación.

2.2.1. CASO DE USO 1 – DLP EN RED

9. Un **DLP de red** es una solución software o hardware que se instala cerca del perímetro de la red. Su función es analizar el tráfico de red para detectar envíos de datos sensibles que violen las políticas de seguridad de la información. Cada vez que es detectada una fuga de datos a través de la red, el dispositivo genera un evento de seguridad. Los datos referidos son definidos como "datos en movimiento".

10. El DLP de red puede monitorizar o bloquear automáticamente las transmisiones identificadas, o poner en cuarentena mensajes que pueden necesitar aprobación previa antes de dejar la red. Además, puede desarrollarse cifrado de correos que contienen contenido sensible cuando se configura la herramienta para hacerlo.

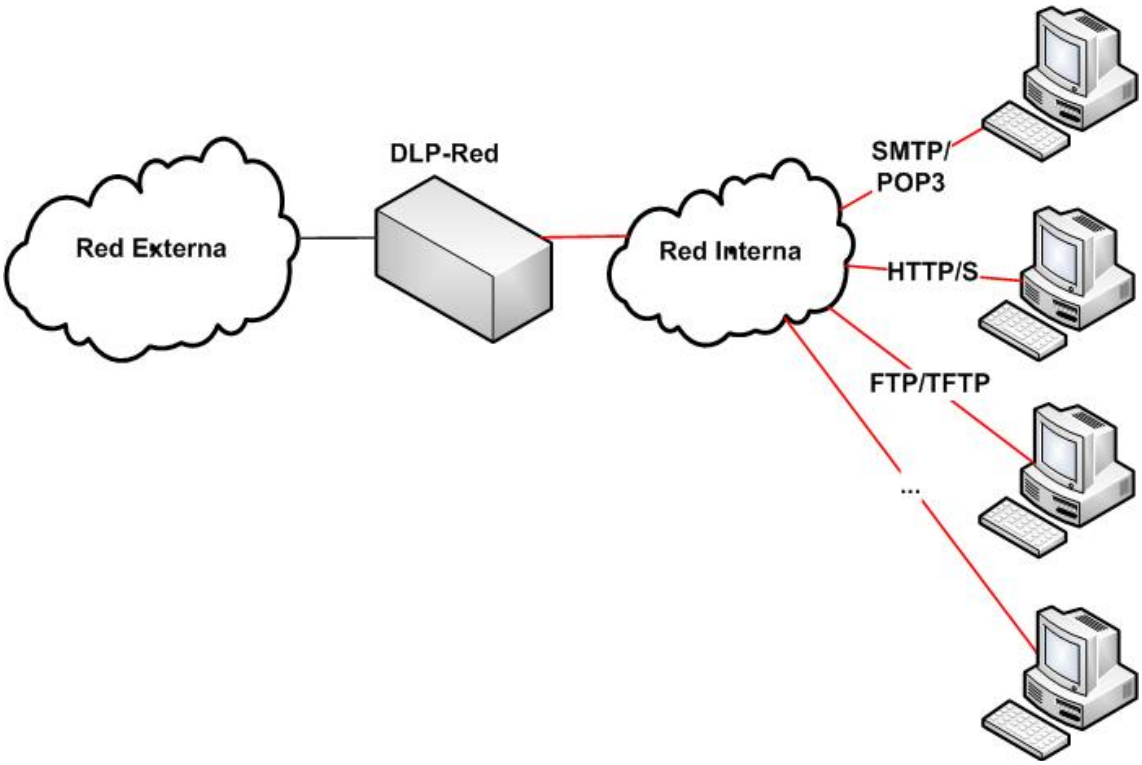

Figura 1 - Caso de uso 1: DLP Red

2.2.2. CASO DE USO 2 DLP END POINT

11. Los **DLP tipo *endpoint*** corren en las estaciones de usuario o en servidores de la organización. Al igual que los sistemas basados en red, pueden estar dirigidos a comunicaciones internas o externas y por lo tanto ser usados para controlar el flujo de información entre grupos o tipos de usuarios. Pueden también controlar comunicaciones vía email o mensajería instantánea antes de que sean almacenados.
12. Tienen la ventaja de que pueden monitorizar y controlar el acceso a dispositivos físicos (como teléfonos móviles con capacidad de almacenamiento de datos) y en algunos casos acceder a información antes de que sea cifrada. Algunos sistemas basados en *endpoint* pueden también bloquear intentos de transmisión de información confidencial y notificarlo de inmediato al usuario. Tiene la desventaja de que necesitan ser instalados en cada estación de trabajo de la red.

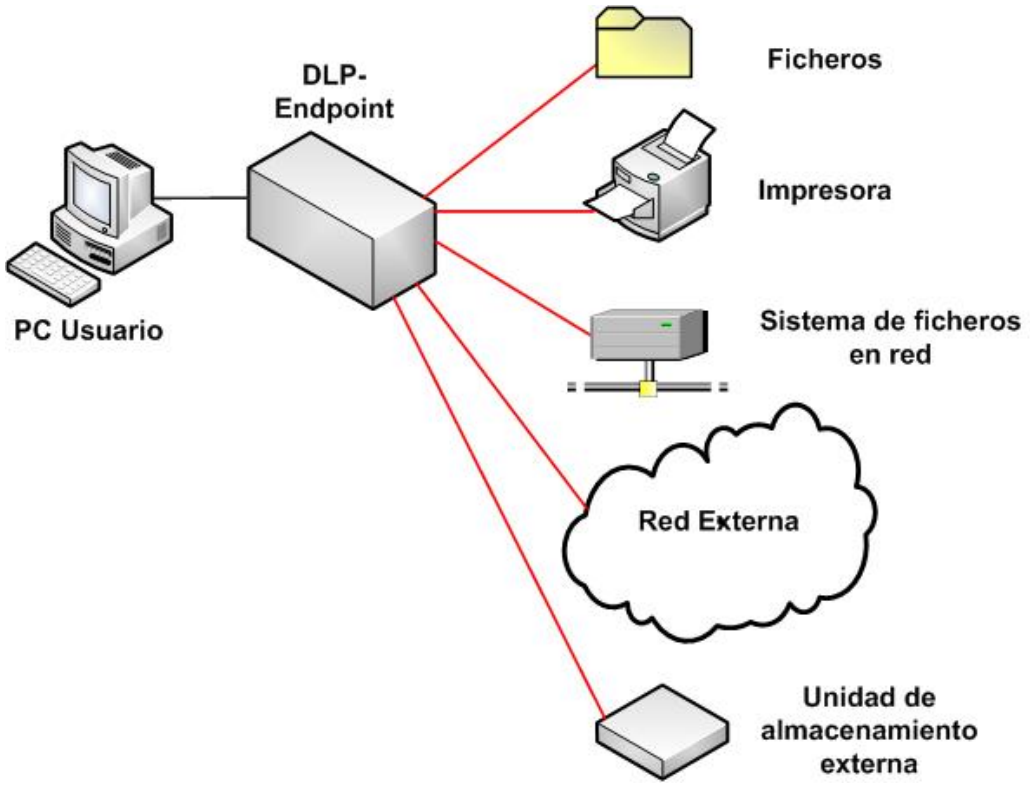

Figura 2 - Caso de uso 2: DLP *End point*

2.2.3. CASO DE USO 3 - DLP CENTRO DE DATOS

13. El **DLP *datacenter*** es típicamente una solución software que se instala en centros de datos para descubrir datos confidenciales que se encuentran almacenados en una localización insegura o inapropiada: sistema de ficheros compartido, servidores, portátiles.
14. Un DLP *data center* puede escanear conjuntos de máquinas configuradas por el administrador como grupos de escaneo, entre los que pueden llegar a incluirse grandes repositorios de información en red NAS[1]/SAS[2].

[1] *Network Attached Storage.*Almacenamiento conectado en red
[2] *Serial Attached SCSI (Small Computer System Interface)*

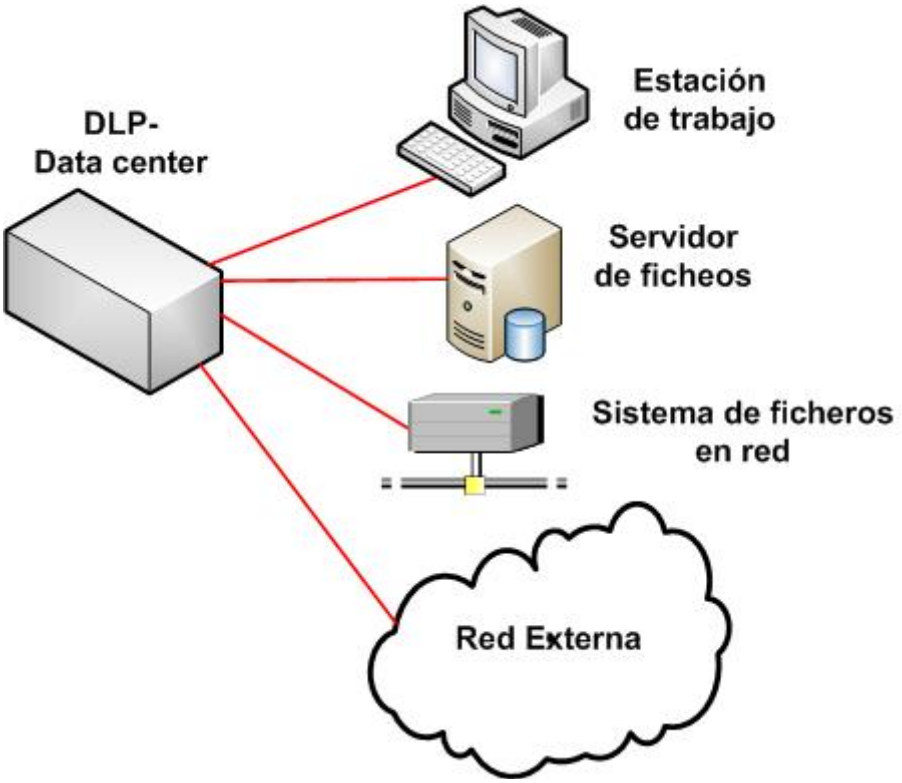

Figura 3– Caso de uso 3: DLP *Data center*

2.3 ENTORNO DE USO

15. Para la utilización en condiciones óptimas de seguridad de los sistemas para la prevención de fuga de datos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física:** El producto deberá instalarse en un área donde el acceso solo sea posible para el personal autorizado.
    - **Administración confiable:** El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la administración/empresa. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina.
    - **Política de seguridad de la información:** Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.
    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos suele presentarse en formato de software instalable que se ejecuta en uno o varios servidores/hosts.

17. Es típica la configuración en la que se instala un gestor en un servidor dedicado y aplicaciones agente en cada una de las máquinas que van a ser auditadas.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

18. No se utilizará ningún perfil de protección *Common Criteria* como referencia para esta familia de productos.
19. El nivel de confianza EAL (*Evaluation Assurance Level*) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser **EAL2 o superior**.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

20. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

- Toda la información que debe monitorizar el sistema, ya sea en tránsito como en almacenamiento.
- Datos de configuración del producto y de auditoría generados por éste.
- Actualizaciones de la herramienta.

3.2 AMENAZAS

21. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

- Un atacante podría acceder a información confidencial que forme parte de los datos de usuario que debe proteger el producto violando las políticas de seguridad.
- Un atacante podría acceder a datos de seguridad alojados en el producto, a pesar de que no estar autorizado a ello de acuerdo a las políticas de seguridad.
- Un atacante podría comprometer la integridad de:
    - Los datos de usuario mientras están siendo transferidos.
    - Los datos de usuario mientras están almacenados.
    - Los datos de configuración del dispositivo.
- Un atacante podría intentar borrar o destruir datos recogidos o producidos por el producto.
- Un atacante podría intentar comprometer el producto ejecutando acciones no autorizadas.
- Un atacante podría intentar capturar el tráfico que atraviesa los canales de comunicaciones establecidos por el producto, con objeto de capturarlo y modificarlo.
- Un atacante podría suplantar al producto y capturar datos de identificación y autenticación de un administrador legítimo y conseguir así acceso al producto.
- Un atacante podría realizar operaciones de seguridad relevantes en el producto sin que estas fuesen registradas.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

22. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 REQUISITOS CRIPTOGRÁFICOS

23. **REQ. 1** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

4.2 AUDITORÍA Y REGISTROS DE SEGURIDAD

24. **REQ. 2** Por cada evento auditable, el producto generará un registro de auditoría que contenga, como mínimo, la siguiente información:
    a) Tipo de evento.
    b) Resultado del evento.
    c) Hora y fecha.
    d) Identidad del usuario (si aplica).
25. **REQ. 3** Se generará un registro de auditoría, al menos en los siguientes casos:
    a) Inicio y finalización de las funciones de auditoría.
    b) Eventos de gestión de usuarios (creación, modificación, eliminación, cambio de privilegios/roles).
    c) Cambios de configuración del sistema.
    d) Registro de entrada y salida (*Login/logout*) de usuarios.
    e) Cambios en las políticas. (Creación, modificación, eliminación…)
    f) Borrado de eventos.
    g) Acciones de reparación (establecimiento de ACLs[3], puesta en cuarentena, borrado, etc).
26. **REQ. 4** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor/administrador del sistema).
27. **REQ. 5** El producto suministrará los datos de auditoría en un formato legible.

[3] *Access Control List*. Lista de control de accesos

28. **REQ. 6** En el caso de que permita almacenamiento remoto de los registros de auditoría, el producto deberá utilizar los protocolos IPsec[4], TLS o TLS/HTTPS para establecer un canal de comunicaciones seguro con la entidad remota.

4.3 CONTROL DE ACCESOS, AUTENTICACIÓN Y PRIVILEGIOS

29. **REQ. 7** La gestión de usuarios, incluyendo su creación y asignación de privilegios, así como la baja o supresión de aquellos, sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador).
30. **REQ. 8** El producto presentará al menos dos tipos de perfiles: administradores del Sistema y usuarios, a los que se asociarán diferentes permisos.
31. **REQ. 9** El producto implementará políticas de control de acceso basadas en roles de usuario, grupos, identificadores de usuario y permisos de usuario, de forma que solo se permita el acceso a un objeto controlado si el usuario es administrador o tiene permisos de acceso.
32. **REQ. 10** El producto requerirá un proceso de autenticación positivo previo a la realización de cualquier tarea.

4.4 ADMINISTRACIÓN DEL PRODUCTO

33. **REQ. 11** La administración del producto sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador de seguridad).
34. **REQ. 12** El producto será capaz de desarrollar funciones de administración relativas al comportamiento de las funciones de seguridad y administración de los atributos de seguridad.
35. **REQ. 13** El producto restringirá las actividades de administración: cambio de la configuración, consulta, modificación y borrado de los atributos de seguridad (roles de usuario, identificadores de usuario, grupos de usuario, permisos de usuario, permisos asignados a objetos, credenciales de administrador), a un usuario privilegiado del sistema (p.ej.: rol de administrador).
36. **REQ. 14** En el caso de que permita administración remota, el producto deberá utilizar los protocolos IPsec, TLS[5] o TLS/HTTPS[6] para establecer un canal de comunicaciones seguro.

4.5 PROTECCIÓN DE DATOS DE USUARIO

37. **REQ. 15** El sistema permitirá a administradores autorizados a forzar políticas de seguridad de control de acceso. Los administradores con el rol de administrador tienen permiso para desarrollar cualquier función administrativa.

4Internet Protocol Security
5Transport Layer Security
6Hypertext Transfer Protocol Secure

4.5.1. DLP DE RED

38. **REQ. 16** Los DLP de red implementarán políticas de seguridad que regulen la capacidad de los usuarios finales a transmitir datos sensibles a través o fuera de la red. Estas políticas basan sus decisiones en:
    a) El contenido de los datos (palabras, frases, patrones de caracteres y huellas de documentos).
    b) Atributos de los datos como: tamaño del fichero, remitente, recipiente, IP origen, IP destino, host origen, host destino, URL[7] destino, etc.
39. **REQ. 17** Las posibles acciones resultantes incluirían: permitir la transmisión, grabar evento (auditoría), bloquear transmisión, cifrar la transmisión o poner los datos en cuarentena.
40. **REQ. 18** Podrán aplicarse a usuarios o grupos de usuarios.
41. **REQ. 19** La capacidad de cambiar la configuración por defecto, consultar, modificar y borrar los atributos de seguridad de las políticas implementadas por los DLP de red (id usuario, id grupo usuario, palabras, frases, patrones de caracteres, huellas de documentos, host, direcciones IP, email, URL, protocolo, servicios DLP) estará restringida a un usuario privilegiado (rol de administrador).
42. **REQ. 20** El sistema forzará la aplicación de políticas de seguridad de control de flujo de información de red cuando exista un flujo de información desde o hacia sujetos cubiertos por la política de seguridad.

4.5.2. DLP END POINT

43. **REQ. 21** Los DLP endpoint implementarán políticas de seguridad que regulen la capacidad de los usuarios finales a realizar acciones sobre datos (copiar, cortar, pegar, modificar, borrar, mover, imprimir, capturar, enviar) o máquinas específicas. Estas políticas basan sus decisiones en:
    a) El contenido de los datos (palabras, frases, patrones de caracteres y huellas de documentos).
    b) Atributos como: extensiones de ficheros, tamaño del fichero, remitente, fuente de ficheros, destino de ficheros, etc.
44. **REQ. 22** Las posibles acciones resultantes incluirían: permitir la acción, grabar evento (auditar), notificar al usuario final, solicitar justificación al usuario final, bloquear la acción, etc.
45. **REQ. 23** Estas políticas se aplicarán a usuarios o grupos de usuarios.
46. **REQ. 24** La capacidad de cambiar la configuración por defecto, consultar, modificar y borrar los atributos de seguridad de las políticas implementadas por los DLP endpoint(identificador de usuario, identificador de grupo de usuario,

[7] *Uniform Resource Locator*. Localizador uniforme de recursos

palabras, frases, patrones de caracteres, extensiones de ficheros, tamaños de fichero, ficheros destino) estará restringida a un usuario privilegiado (rol de administrador).

4.5.3. DLP DATA CENTER

47. **REQ. 25** Los DLP *datacenter* implementarán políticas de seguridad que regulen la capacidad determinadas máquinas para almacenar datos sensibles. Estas políticas basan sus decisiones en:
    a) El contenido de los datos (palabras, frases, patrones de caracteres y huellas de documentos).
    b) Atributos como: fecha de modificación y creación del fichero, otras fechas de fichero.
48. **REQ. 26** Las posibles acciones resultantes incluirían: permitir conservar los datos, grabar evento (auditar), aplicar formulario RMS, conceder permiso a un usuario, mover a un emplazamiento seguro o ponerlo en cuarentena.
49. **REQ. 27** Estas políticas se aplicarán ficheros almacenados en escritorio, en dispositivos portátiles, servidores o repositorios de datos.
50. **REQ. 28** La capacidad de cambiar la configuración por defecto, consultar, modificar y borrar los atributos de seguridad de las políticas implementadas por los DLP *Datacenter*, para restringir la capacidad de cambiar la configuración por defecto, consultar, modificar, borrar los atributos de seguridad (fecha de modificación de fichero, de creación, otras fechas de fichero, palabras, frases, patrones de caracteres, huellas de documentos) estará restringida a un usuario privilegiado (rol de administrador).

4.6 GESTIÓN DE INCIDENTES

51. **REQ. 29** Para cada incidente detectado, el producto deberá notificar o escalar acciones dependiendo de la política configurada.
52. **REQ. 30** Podrá tomar las siguientes acciones:
    a) Notificar al remitente. (DLP de red)
    b) Al gestor del remitente. (DLP de red).
    c) Notificar al usuario final. (DLP *end point*).
    d) A un gestor de usuarios. (DLP *end point*).
    e) Notificar al propietario del fichero. (DLP *datacenter*).
    f) Notificar al gestor del propietario del fichero. (DLP *datacenter*).
    g) A un determinado usuario.
    h) A un determinado grupo.
    i) A un determinado grupo de usuarios.

j) Incrementar el nivel del incidente.

53. **REQ. 31** El producto deberá aplicar un conjunto de reglas en la monitorización de eventos generados basados en políticas y a partir de reglas generar un incidente.

54. **REQ. 32** Estas reglas podrán ser una o una combinación de las siguientes:

    a) Para cada evento generado por el DLP de red, crear un incidente.

    b) Para cada evento generado por el DLP *end point* si el número de eventos para un determinado usuario final dentro de una ventana de tiempo configurada coincide con un determinado nivel configurado en la política, generar un incidente.

    c) Para eventos generados por el DLP datacenter, crear un incidente de acuerdo a una política de seguridad que utilice una o varias de las siguientes reglas:

        i. Un número de eventos ocurre en un solo equipo dentro de una ventana de tiempo.

        ii. Un número de eventos son producidos por un mismo propietario de ficheros en una ventana de tiempo.

        iii. Un número de eventos son producidos sobre un mismo directorio compartido en una ventana de tiempo.

5. ABREVIATURAS

ACL	*Access Control List*
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
DLP	*Data Loss Prevention*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HTTPS	*Hypertext Transfer Protocol Secure*
IPSEC	*Internet Protocol Security*
NAS	*Network Attached Storage*
RFS	Requisitos Fundamentales de Seguridad
RMS	*Rights Management System*
SAS	*Serial Attached SCSI (Small Computer System Interface)*
TLS	*Transport Layer Security*