ANEXO III.

PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN

PR30

INDICE

1. OBJETO

1. El objeto del presente documento es la definición del Procedimiento aplicable a la Generación de Copias de Respaldo y Recuperación de la Información manejada por el <<ORGANISMO>>.

Se implantará el presente Procedimiento atendiendo al **nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas del <<ORGANISMO>>,** que resulten de la aplicación de las previsiones contempladas en los Anexos I y 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 (ENS).

2. ÁMBITO DE APLICACIÓN

2. Este Procedimiento es de aplicación a todo el ámbito de actuación del <<ORGANISMO>>, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad del <<ORGANISMO>>.
3. El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el <<ORGANISMO>>, especialmente, los responsables de los Servicios de Explotación de los Sistemas de Información del <<ORGANISMO>> y los propios usuarios, como actores ambos, en sus respectivas competencias, de la generación de copias de respaldo y su ulterior recuperación, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información del <<ORGANISMO>>.
4. En el ámbito del presente Procedimiento, se entiende por usuario cualquier empleado público perteneciente o ajeno al <<ORGANISMO>>, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el <<ORGANISMO>> y que utilice o posea acceso a los Sistemas de Información del <<ORGANISMO>>.

3. VIGENCIA

5. El presente Procedimiento ha sido aprobado por la <<U/OC>> del <<ORGANISMO>>, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que el <<ORGANISMO>> pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, cuando proceda, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.
6. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del <<ORGANISMO>>.
7. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este Procedimiento.

4. REVISIÓN Y EVALUACIÓN

8. La gestión de este Procedimiento corresponde a la <<U/OC>>, que es competente para:

   - Interpretar las dudas que puedan surgir en su aplicación.
   - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
   - Verificar su efectividad y grado de cumplimiento.

9. Anualmente (o siempre que existen circunstancias que así lo aconsejen), la <<U/OC>> revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación de la <<U/OC>> del <<ORGANISMO>>.

10. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

11. Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS

12. Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:

   - 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.
   - Ley 15/1999, de Protección de Datos de Carácter Personal.
   - Real Decreto 1720/2007, por el que se aprueba el reglamento de Desarrollo de la LOPD.
   - Documentos y Guías CCN-STIC.

6. ROLES Y RESPONSABILIDADES

13. Las responsabilidades personales derivadas de las actividades descritas en el presente Procedimiento son las siguientes[1].

Roles	Responsabilidades
Personal del área de Explotación del Departamento de Sistemas del <<ORGANISMO>>	Gestionar las copias de respaldo de los activos recogidos en el alcance del Procedimiento, siguiendo las directrices señaladas.
Responsable del área de Explotación del Departamento de Sistemas del	• Custodiar los soportes de almacenamiento extraíbles donde se almacenan las copias de respaldo del <<ORGANISMO>>. • Garantizar la correcta ejecución de las operaciones periódicas de copia de respaldo.

[1] Se ha optado por una asignación de responsabilidades habitual en los organismos de las AA.PP. españolas.

<<ORGANISMO>>	• Ejecutar las comprobaciones periódicas de los procedimientos de restauración del <<ORGANISMO>>.
Responsables de los Activos[2]	• Tramitar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo. • Tramitar las solicitudes de recuperación de activos alterados, dañados o destruidos desde la realización de la(s) copia(s) de respaldo. • Validar las operaciones de restauración de activos gestionadas por el personal del área de Explotación del Departamento de Sistemas del <<ORGANISMO>>.
<<U/OC>> competente[3]	• Aprobar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo solicitadas por los Responsables de los Activos. • Aprobar las solicitudes de recuperación de activos a partir de copias de respaldo, solicitadas por los Responsables de los Activos.

7. CUESTIONES GENERALES

Las Copias de Respaldo

14. Toda la información del <<ORGANISMO>> del ámbito de aplicación del ENS será periódicamente respaldada en soportes de backup.
15. Los Responsables de la Información y de los Servicios4 establecerán los ciclos de copia más adecuados para cada tipo de información.
16. Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción o pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración e, incluso, la imagen del sistema operativo.
17. Para todos los sistemas relevantes se definirán los estándares de respaldo, que incluirán, al menos, la siguiente información:
    - Periodicidad de las copias de respaldo.
    - Periodos de retención de las copias.
    - Ubicación de los soportes de respaldo.
    - Procedimientos de recuperación de la información.

[2] Generalmente: Responsable de la Información y/o Responsable del Servicio.
[3] Generalmente: Responsable de la Gestión y Custodia de los Soportes. El Responsable de la Gestión y Custodia de los soportes de almacenamiento suele ser el responsable del área de explotación del Departamento de Sistemas del <<ORGANISMO>> de que se trate.

[4] Asesorados habitualmente por el Responsable del Sistema y el Responsable de Seguridad.

- Procedimientos de restauración y verificación de la integridad de la información respaldada.
- Procedimientos de inventario y gestión de soportes.

Tipos de Copias de Respaldo

Completa	Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda.
Incremental	Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.
Diferencial	Se copian los datos modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

Ordenadores Portátiles

18. Todos los usuarios de ordenadores portátiles deberán realizar copias de respaldo de sus datos con la regularidad que se especifique.
19. Para la realización de estas copias de respaldo deberá utilizarse la herramienta que, a tal propósito, se defina a nivel corporativo.

Cifrado de soportes almacenados externamente

20. Toda la información de copias de respaldo que el <<ORGANISMO>> almacene fuera de sus locales[5] debe estar cifrada, según los procedimientos definidos a tal efecto.
21. El procedimiento de envío y recepción de soportes permitirá asegurar que éstos no son extraviados ni han sido manipulados durante su transporte.

[5] Perímetro de seguridad

Copia de respaldo de información de usuarios

22. Los usuarios son responsables de la realización de copias de respaldo con la frecuencia definida y siempre que haya cambios significativos en la información que manejan, para lo que utilizarán las carpetas de red que a tal efecto les sean habilitadas.
23. En ningún caso se deberán almacenar copias de respaldo en el domicilio del usuario o en dependencias de terceros ajenas al <<ORGANISMO>> si no existe un acuerdo previamente suscrito con el tercero en el que se prevea tal posibilidad y se expliciten las cautelas debidas respecto de la custodia de la información almacenada.
24. Los responsables de las unidades administrativas del <<ORGANISMO>> deberán asegurarse de que la información de los empleados a su cargo se salvaguarda de forma satisfactoria.

Retención de información

25. Los documentos originales y los ficheros en formato electrónico deben ser retenidos durante el tiempo que en cada caso el ordenamiento jurídico prescriba.
26. Además de lo anterior, hay que tener en cuenta que puede haber requerimientos para retener datos, tales como "logs para auditorías", de cara a la realización de acciones administrativas, disciplinarias, civiles o penales, por lo que habrán de definirse los procedimientos pertinentes para custodiar este tipo de información. Además, se implantarán los medios necesarios para poder revisar las actividades de los usuarios que manejan este tipo de información.
27. El Departamento de Asesoría Jurídica del <<ORGANISMO>>, con la colaboración del resto de Departamentos involucrados del <<ORGANISMO>>, especialmente los Responsables de la Información, los Servicios y de Seguridad, se encargará de definir los periodos de retención de la información en función de la naturaleza de la misma y del ordenamiento jurídico vigente en cada momento.
28. Cuando la información del <<ORGANISMO>> deje de ser necesaria, deberá ser destruida o eliminada de manera segura. Para dar soporte a este requisito, los responsables de las unidades administrativas del <<ORGANISMO>> deberán revisar, de forma periódica, el valor y la utilidad de la información almacenada.
29. Todos los datos almacenados en soportes de información que se desechen serán eliminados según un procedimiento definido a tal efecto, que asegure los objetivos de seguridad para la información de los citados soportes. En este sentido, se deberá tener especial cuidado con respecto a la información almacenada en servidores o estaciones de trabajo, el software licenciado o desarrollado a medida y los elementos que recibirán mantenimiento dentro del <<ORGANISMO>> por usuarios que no tengan permiso permanente de acceso a los mismos.

Identificación de información crítica

30. Los responsables de las unidades administrativas del <<ORGANISMO>> serán los encargados de identificar y mantener una relación actualizada de aquella información que sus departamentos necesitan para recuperar la operativa de sus procesos, durante eventuales operaciones de restauración. Se deberá adoptar especial cuidado con

aquella información que proporcione evidencia de la existencia de un hecho, responsabilidad u obligación contractual.

Prueba de Soporte Informático

31. La información del ámbito de aplicación del ENS, almacenada en un medio informático durante un período prolongado de tiempo, deberá ser verificada al menos una vez al año, para asegurar que la información es recuperable.

Periodicidad de las copias de respaldo

32. La realización de copias de respaldo de forma periódica permitirá al <<ORGANISMO>> disponer de su información en caso de destrucción de los equipos o errores producidos en los datos y/o aplicaciones.
33. Las copias de respaldo de software, ficheros de datos y bases de datos se deberán realizar regularmente. La frecuencia con la que se deben realizar los back-ups se definirá en función de la sensibilidad de las aplicaciones o datos y de su impacto en el adecuado desarrollo de las competencias atribuías al <<ORGANISMO>>. Por ello, tal periodicidad deberá determinarse sobre la base de las consecuencias que la pérdida de la información tendría para el <<ORGANISMO>>.
34. Respecto de los ficheros que contengan datos de carácter personal, habrá de tenerse en cuenta lo siguiente:

- Se deben crear procedimientos para la realización de, al menos, una copia de respaldo semanal, si en tal periodo se hubiere producido alteración o modificación de los datos.
- Cuando las pruebas anteriores a la implantación o modificación de los sistemas de información, traten ficheros con datos reales de carácter personal, se deberá realizar previamente una copia de seguridad de los datos.

Almacenamiento de las Copias de Respaldo en dependencias externas

35. Suele ser frecuente el almacenamiento de la última copia de seguridad[6] en una ubicación externa, lo que minimiza el riesgo de pérdida de datos en caso de producirse una contingencia.
36. Deberán adoptarse las siguientes cautelas, especialmente cuando se traten ficheros que contengan datos de carácter personal o con información sensible.

- La última copia de seguridad, junto con los procedimientos de recuperación, deberá ubicarse en edificios distintos de las ubicaciones de los CPD´s. A ser posible, en un centro externo.
- Deberá existir un registro con el contenido de las copias de respaldo, lo que facilitará un control efectivo en su gestión.
- Deberá llevarse un registro de las copias de respaldo ubicadas, tanto en las dependencias del <<ORGANISMO>>, como en las sedes de almacenamiento alternativas.

[6] Mensual, por ejemplo.

Protección de las Copias de Respaldo

37. La adecuada protección de las copias de respaldo permitirá tanto su correcta conservación, como un control de acceso efectivo a los datos almacenados.

38. La protección de las copias de respaldo alcanzará tanto a archivos de información como a librerías de aplicaciones. El almacenamiento de los soportes se hará efectivo ubicando las copias en armarios ignífugos, bajo llave y restringiendo el acceso a personal previamente autorizado.

Automatización del sistema de Backup

39. La automatización de los procedimientos de backup reducirán la posibilidad de omitir ciclos de respaldo o que éstos sean erróneos.
40. La programación periódica de las copias de respaldo se debe efectuar a través de un sistema de administración de soportes.

Descripción del contenido de las Copias de Respaldo

41. La documentación del contenido de las copias de seguridad facilitará su identificación.
42. En las correspondientes etiquetas se deberá identificar la fecha a que corresponde. En el inventario de copias de respaldo se detallará los archivos de los cuales se hace backup.

Control de entrada y salida de las Copias de Respaldo

43. La existencia de un registro que controle las entradas y salidas de copias de respaldo proporciona fiabilidad al inventario de copias de seguridad.
44. Debe quedar registrado el flujo de entradas y salidas de los soportes fuera de las instalaciones del <<ORGANISMO>>, dejando constancia del solicitante de cada petición y de los motivos.
45. En cuanto a los ficheros que contengan datos de carácter personal (o especialmente sensibles), se deberá tener en cuenta que las copias de seguridad que contengan datos de carácter personal sólo deberán salir con autorización del Responsable del Fichero y llevándose a cabo bajo su última responsabilidad.

Transporte de las Copias de Respaldo

46. El transporte de las copias de respaldo deberá contar con las adecuadas medidas de seguridad que garanticen la no alteración, robo o destrucción de los datos durante su transporte.
47. El transporte de las copias de respaldo con información sensible se deberá realizar utilizando maletas provistas de mecanismos de apertura operados bajo llave y/o mecanismos de cifrado, y cuyas llaves o claves se encontrarán bajo custodia. La responsabilidad de la destrucción o pérdida de información durante el transporte o almacenamiento recaerá sobre el personal / unidad administrativa / personas jurídicas responsables de su gestión.

Pruebas de realización y restauración de las Copias de Respaldo

48. La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos, y garantizará la integridad de los datos que contienen.
49. Se establecerán pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad previamente establecida.
50. Las pruebas y los resultados deberán estar convenientemente documentados y, como consecuencia de las mismas, se subsanarán las incidencias que se hayan puesto de manifiesto durante su desarrollo.
51. Además, cuando se traten ficheros que contengan datos de carácter personal, el Responsable del Fichero deberá verificar semestralmente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación.

Periodo de existencia de las Copias de Respaldo y su eventual destrucción

52. El establecimiento de un período de existencia de las copias de respaldo, de acuerdo con el ordenamiento jurídico vigente en cada momento y lo dispuesto en la Política de Seguridad del <<ORGANISMO>>, facilitará la salvaguarda de las mismas, el cumplimiento legal y el uso eficiente del espacio físico disponible para el almacenamiento.
53. Se deberá establecer el período de existencia para las copias de seguridad y los procedimientos a seguir para proceder a su destrucción definitiva una vez concluido tal periodo.

8. HERRAMIENTAS PARA LA GENERACIÓN DE COPIAS DE RESPALDO

54. El Departamento de Sistemas del <<ORGANISMO>>[7] contará con un conjunto de herramientas para la generación de copias de respaldo, que le permitirá realizar copias de seguridad de los activos y sistemas de información del <<ORANISMO>> sujetos al ámbito de aplicación del ENS.
55. Estas herramientas de copia se detallan en el registro de herramientas para la generación de copias de respaldo del que se presenta un modelo en el epígrafe 12 del presente Procedimiento.

9. GENERACIÓN DE COPIAS DE RESPALDO

9.1 INCLUSIÓN DE ACTIVOS EN LA COPIA DE RESPALDO

56. La operación de inclusión de activos en la copia de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por la <<U/OC>> competente.

[7] Dirigido por el Responsable del Sistema, en terminología del ENS.

57. Para solicitar la inclusión, el Responsable del Activo abrirá una incidencia en el <<gestor de incidencias>> del <<ORGANISMO>>, a la que adjuntará la Solicitud de Inclusión de activos en la Copia de Respaldo. Un modelo de este documento se muestra en el epígrafe 13 del presente Procedimiento.

58. La <<U/OC>> competente:

- Aprobará la petición, y asignará la incidencia al responsable del área de explotación del Departamento de Sistemas del <<ORGANISMO>>, o
- Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

9.2 PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO

59. La generación de copias de respaldo de los activos del <<ORGANISMO>> del ámbito de aplicación del ENS se soporta en los procedimientos y herramientas de copia del Departamento de Sistemas del <<ORGANISMO>>.

60. Las operaciones de copia de respaldo de los activos del <<ORGANISMO>> recogidos dentro del alcance del ENS se gestionarán de forma programada en fechas y horas concretas, a través de las herramientas de copia del Departamento de Sistemas del <<ORGANISMO>>.

61. El Departamento de Sistemas del <<ORGANISMO>> mantendrá un inventario de los activos sobre los que se realiza copia de seguridad en el **Registro de Activos sujetos a Copia de Respaldo**. Un modelo de este registro se presenta en el epígrafe 12 del presente Procedimiento.

9.3 PROCEDIMIENTO DE VERIFICACIÓN DE COPIAS DE RESPALDO

62. La herramienta de generación de copias de respaldo del <<ORGANISMO>> contará con un sistema automático de verificación de copias. Este sistema, que se mantendrá permanentemente activado, verificará las copias de respaldo una vez generadas y almacenará el resultado de la operación en el registro del sistema.

63. El Departamento de Sistemas del <<ORGANISMO>> comprobará diariamente el registro del sistema, al objeto de garantizar la correcta ejecución de las operaciones de copia de respaldo.

64. En caso de detectar un fallo en el proceso de generación, el Departamento de Sistemas del <<ORGANISMO>> investigará y resolverá la incidencia y relanzará la tarea de copia.

9.4 GESTIÓN DE SOPORTES

65. Las herramientas de gestión de copias de respaldo del <<ORGANISMO>> contarán con una librería de soportes que permita la inserción de múltiples volúmenes para facilitar la gestión automatizada de las operaciones[8].

[8] El Responsable de la Gestión y Custodia de los soportes de almacenamiento suele ser el responsable del área de explotación del Departamento de Sistemas del <<ORGANISMO>>.

66. Estos soportes se insertarán antes de una operación de copia y se retirarán para su almacenamiento, tras la verificación de la misma.

67. Los soportes de copia se obtendrán en <<señalar ubicación informática de grabación>> [9] situado en <<señalar ubicación física>> de las instalaciones del <<ORGANISMO>>, y se almacenan en <<*señalar dispositivo de custodia segura*>>[10] ubicada en <<*señalar ubicación*>>[11].

68. El <<ORGANISMO>> mantendrá un inventario de los soportes empleados en las operaciones de generación de copias de respaldo en el Registro de Soportes Extraíbles. Se presenta un modelo de este Registro en el epígrafe 12 del presente Procedimiento.

10. RECUPERACIÓN DE ACTIVOS A PARTIR DE COPIAS DE RESPALDO

10.1 SOLICITUD DE RECUPERACIÓN DE ACTIVOS

69. La operación de recuperación de activos a partir de copias de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por la <<U/OC>> competente.

70. Para solicitar una recuperación, el Responsable del Activo abrirá una incidencia en el <<gestor de incidencias>> del <<ORGANISMO>>, a la que adjuntará la Solicitud de Recuperación de Activos. Un modelo de esta solicitud se presenta en el epígrafe 13 del presente Procedimiento.

71. La <<U/OC>> competente:

- Aprobará la petición y señalará la incidencia al Departamento de Sistemas del <<ORGANISMO>>, o
- Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

10.2 RECUPERACIÓN DE ACTIVOS

72. El Departamento de Sistemas del <<ORGANISMO>> accederá al soporte físico en el que reside la copia de respaldo del activo a recuperar y lo cargará en la unidad de lectura de la herramienta de generación de copias de respaldo.

73. El personal del área de Explotación del Departamento de Sistemas del <<ORGANISMO>> responsable de la recuperación del activo, accederá al soporte y, empleando las herramientas de copia, restaurará el activo en una ubicación temporal12 a la que sólo tendrá privilegios de acceso su responsable, y actualizará la incidencia informándole de la ubicación donde puede localizar el activo.

[9] Por ejemplo: en el CPD del <<ORGANISMO>> o de la unidad administrativa correspondiente.
[10] Por ejemplo: en una caja fuerte ignífuga.
[11] Por ejemplo: Zona de Seguridad del <<ORGANSMO>>.
[12] La copia de respaldo no se restaurará en su ubicación original hasta identificar una copia válida. De esta forma se evita sobrescribir los soportes originales e invalidar la posibilidad de una recuperación del activo por otro medio si se detectan fallos en la copia.

74. El Responsable del Activo accederá a la ubicación temporal y:

- Validará la recuperación del activo, expresando su conformidad en el registro de la incidencia, autorizando de esta forma su restauración a partir de la copia en su ubicación original, o
- La rechazará, solicitando en el campo comentarios de la incidencia una nueva recuperación a partir de una copia de respaldo alternativa.

75. Una vez validada la restauración, el Responsable del Activo:

- Recuperará el activo en su ubicación original.
- Eliminará de su ubicación temporal el activo recuperado desde la copia de respaldo.

76. Por su parte, el Departamento de Sistemas del <<ORGANISMO>>:

- Retirará el soporte físico de la unidad de lectura de la herramienta de generación de copias y lo devolverá al armario ignífugo donde se almacenan los soportes del <<ORGANISMO>>.
- Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de restauración del <<ORGANISMO>>.
- Cerrará la incidencia.

11. COMPROBACIÓN PERIÓDICA DE LOS PROCEDIMIENTOS DE RESTAURACIÓN

77. Para garantizar la eficacia de los procedimientos de restauración del <<ORGANISMO>> y la capacidad para recuperar activos desde las copias de respaldo, se establecerá el procedimiento de comprobación periódica que se detalla a continuación.

11.1 PROCEDIMIENTO DE COMPROBACIÓN

78. Periódicamente[13], el Departamento de Sistemas del <<ORGANISMO>>[14]:

- Seleccionará al azar un activo de información[15] almacenado en la copia de respaldo.
- Ejecutará una restauración del activo sobre una ubicación temporal, comprobará la restauración del activo y lo eliminará posteriormente.
- Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobación periódicas del <<ORGANISMO>>.

[13] Suele ser frecuente el primer día del mes.
[14] Habitualmente, a través de su Responsable de Explotación.
[15] Que puede ser un activo de información propiamente dicho o un sistema completo.

12. REGISTROS E INDICADORES

12.1 TABLA DE REGISTROS

Identificador	Nombre	Frecuencia	Archivo	Genera	Custodia
<<**x-R01**>>	Herramientas de generación de copias de respaldo	Una vez al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<**x-R02**>>	Activos sujetos a copia de respaldo	Dos veces al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<**x-R03**>>	Soportes extraíbles	Una vez al año	Gestor Documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<**x-R04**>>	Solicitudes de inclusión de activos en la copia de respaldo	No aplicable	Gestor de incidencias	Responsable del activo	Responsable de Gestión de Soportes
<<**x-R05**>>	Solicitudes de restauración	No aplicable	Gestor de incidencias	Responsable del activo	Responsable de Gestión de Soportes
<<**x-R06**>>	Operaciones de restauración	Una vez al año	Gestor documental	Responsable del área de Explotación	Responsable de Gestión de Soportes
<<**x-R07**>>	Operaciones de comprobación periódicas	Una vez al año	Gestor documental	Responsable del área de Explotación	Responsable de Gestión de Soportes

12.2 TABLA DE INDICADORES

Identificador	Rango	Frecuencia	Métrica	Objetivo	Descripción
<<**x-I01**>>	%	Una vez al año	Operaciones fallidas de recuperación con respecto al total	0%	--

13. SOPORTE Y MODELOS

13.1 SOPORTE

79. A continuación se detallan los elementos de soporte necesarios para la implantación del presente Procedimiento.

- Herramientas de generación de copias de respaldo.
- Soportes de almacenamiento.
- Armario ignífugo.
- Gestor de incidencias.

13.2 MODELOS

80. A continuación se detallan los modelos a emplear para la implantación del presente Procedimiento.

Modelo de solicitud de inclusión de activos en la copia de respaldo

81. Modelo para la solicitud de inclusión de activos en la copia de respaldo.

Activo	Sistema	Periodo Retención	Tipo (A/C)	Contenidos	Comentarios
	(Sistema de información que alberga el activo a incluir en la copia de respaldo.)		(Tipo de activo a incluir en la copia de respaldo: A: Activo de información, C: Sistema de Información completo.)	Únicamente para activos de tipo *Activo de información*, listado completo con el detalle de contenidos, incluyendo directorios y archivos sobre los que generar copia de respaldo.)	

Modelo de registro de herramientas para la generación de copias de respaldo

82. Modelo para el registro de herramientas para la generación de copias de respaldo.

Nombre	Tipo (HW/SW)	Fabricante	Versión	Responsable
	Tipo de herramienta: HW: Hardware, SW: Software.			

Modelo de registro de soporte extraíbles

83. Modelo para el registro de soportes para la generación de copias de respaldo.

Etiqueta	Contenido	Formato	Capacidad	Responsable

Modelo de solicitud de recuperación de activos

84. Modelo para la solicitud de recuperación de activos desde la copia de respaldo.

Activo a recuperar	Sistema	Tipo (A/C)	Fecha recuperación	Tamaño estimado	Comentarios
	(Sistema de información que alberga el activo a recuperar.)	(Tipo de activo a recuperar desde la copia de respaldo: A: Activo de información, C: Sistema de información completo.)	(Fecha estimada en la que el activo se encontrará disponible.)		

Modelo de registro de activos sujetos a copia de respaldo

85. Modelo para el registro de activos de la <<unidad administrativa>> de los que se realiza copia.

Activo	Tipo copia (C/I/D)	Periodicidad (D/S/M/A/BD)	Periodo retención	Contenido	Responsable	Soporte (C/D)	Tipo Activo (A/C)	Comentarios
	(Tipo de copia de respaldo: C: Completa, I: Incremental, D: Diferencial.)	(Periodicidad de la copia: D: Diaria, S: Semanal, M: Mensual, A: Anual, BD: Bajo Demanda.)				(Tipo de soporte en el que se almacena la copia: C: Cinta, D: Disco.)	(Tipo de activo: A: Activo de información, C: Sistema de información completo.)	