CCN-CERT
centro criptológico nacional

CCN-TEC 010

La disponibilidad de los sistemas TIC

CCN
centro criptológico nacional

Enero 2023

Edita:

CCN-PYTEC

Fecha de Edición: enero de 2023

ÍNDICE

1. INTRODUCCIÓN

1. En el ámbito de tecnologías de la información y las comunicaciones, el concepto de disponibilidad se puede definir como la capacidad de un servicio, conjunto de datos o sistema de ser operable y accesible en el periodo de tiempo determinado en el que son requeridos. Dicha operación debe estar garantizada y para ello, son necesarias medidas y mecanismos que permitan a un sistema o servicio mantener su estado de operatividad y accesibilidad en caso de que un evento amenazara con inhabilitarlo.

2. La disponibilidad conforma una de las tres (3) dimensiones principales de la seguridad de un sistema de información, junto con la **confidencialidad**, que garantiza que la información solo esté a disposición de sistemas o usuarios autorizados **y la integridad**, que garantiza que su estado original no ha sido manipulado durante un proceso o comunicación. Hay que tener en cuenta que las amenazas a la disponibilidad y los mecanismos para contrarrestarlas también suelen afectar a estos otros dos aspectos.

3. Se considera alta disponibilidad a la capacidad de un servicio, sistema o conjunto de datos de encontrarse operativos para los usuarios en todo momento y sin interrupciones. El objetivo de la alta disponibilidad es mantener los sistemas funcionando 24 horas al día, 7 días a la semana. Generalmente este tipo de disponibilidad se establece para sistemas de carácter crítico.

4. Existen distintos niveles de disponibilidad en un sistema, generalmente estimado por su tiempo de inactividad en el periodo de un año, según el cual se estima el porcentaje de disponibilidad. Por ejemplo, un alto nivel de exigencia de alta disponibilidad podría ser de, aproximadamente, 5 minutos de inactividad al año, lo que supone una disponibilidad de un 99,999% (cinco nueves). Comúnmente la disponibilidad se mide en “nueves”, indicando el porcentaje.

Porcentaje de disponibilidad	Minutos de sistema inactivo	Horas de sistema inactivo
99,9999%	0,53	0,009
99,999%	5	0,08
99,99%	53	0,88
99,9%	526	8,77
99,5	2628	43,8
99%	5256	87,6

Tabla 1. Tiempo aproximado acorde a los porcentajes de disponibilidad

5. Normalmente, el coste por cada hora de parada se utiliza como factor determinante para establecer el umbral de exigencia al sistema de alta disponibilidad, ya que deben equilibrarse las pérdidas asociadas al tiempo de inactividad con el coste de garantizar un mayor tiempo de disponibilidad.

2. MÉTRICAS

6. Para poder determinar con precisión los requisitos necesarios para el aseguramiento de la disponibilidad y seleccionar las salvaguardas necesarias, se dispone de distintas métricas que miden la disponibilidad y fiabilidad de los servicios.

7. Las principales métricas son:

- **MTTF (*Mean Time to Failure*).** Es la medida que estima el tiempo entre fallos en los sistemas, durante la operación normal. Se puede calcular como la media aritmética entre fallos de un sistema.
- **MTTR (*Mean Time to Recover*).** Es la medida que indica el tiempo medio que lleva a un sistema reestablecerse a una situación de normalidad tras haberse provocado un fallo.
- **Disponibilidad**. El cálculo del porcentaje de disponibilidad del sistema se calcula mediante la siguiente fórmula:

$$Disponibilidad = \frac{MTTF}{(\mathrm{MTTF} + \mathrm{MTTR})}$$

  Este porcentaje se suele representar también como tiempo/año:

  - 99,9% (tres nueves) -> 8,76 horas/año inactivo.
  - 99,99% (cuatro nueves) -> 52,6 minutos/año inactivo.
  - 99,999% (cinco nueves) -> 5,26 minutos/año inactivo.

- **RTO (*Recovery Time Objective*) o Tiempo de recuperación.** Es el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado. En función del nivel disponibilidad requerido por el sistema, se deberá establecer un RTO máximo para los distintos procesos de la organización.

  Recomendación 1:

  Según define la guía *CCN-STIC-803 Valoración de sistemas en el ENS*, se recomienda tratar de alcanzar un RTO máximo para los procesos de la organización de:

  - Cuatro (4) horas para sistemas críticos que requieren de una alta disponibilidad.
  - Un (1) día para sistemas que requieren de una disponibilidad media.
  - Cinco (5) días para sistemas que requieren de una disponibilidad baja.

- **Tiempo máximo tolerable de caída o MTD (*Maximum Tolerable Downtime*).** Es el tiempo que un proceso puede permanecer caído antes de que se produzcan consecuencias críticas para la organización.
- **Nivel mínimo de recuperación de servicio o ROL (*Revised Operating Level*).** Es el nivel mínimo de operación que debe tener una actividad para ser considerada como recuperada, aunque el nivel de servicio no sea óptimo.
- **Objetivo de Punto de Recuperación (*Recovery Point Objective*).** Este valor determina el impacto que tiene sobre la actividad la perdida de datos. Es crítico a la hora de determinar las políticas de copias de seguridad.

3. PLAN DE CONTINUIDAD DE NEGOCIO

8. Existen también algunos procedimientos que servirán para mejorar la seguridad de la organización, prevenir ataques a la disponibilidad de los sistemas y, en caso de desastre, retomar la actividad en el menor tiempo posible para reducir al mínimo el impacto en el negocio.

9. **El Plan de Continuidad de Negocio establece la continuidad de una organización desde múltiples perspectivas**: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc.

10. Cada uno de estos ámbitos deberá tener, a su vez, un plan de continuidad más específico. Por ejemplo, se deberá crear un Plan de Continuidad TIC (PCTIC), centrado en el ámbito de las tecnologías de la información o un Plan de Recuperación ante Desastres (PRD), centrado un ámbito más general de la organización

11. Un PCN sirve para:

    - Mantener el nivel de servicio en los límites definidos.
    - Establecer un periodo de recuperación mínimo.
    - Recuperar la situación inicial antes de que se produzca un incidente de seguridad.
    - Analizar los resultados y motivos de un incidente.
    - Evitar que las actividades de la organización se vean interrumpidas.

12. Para lograr esto, se utilizarán las siguientes fases:

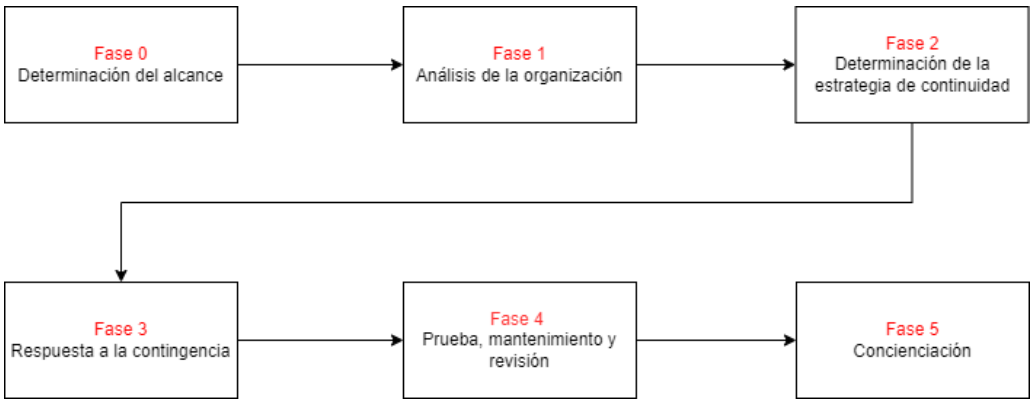


Ilustración 1. Fases de un PCN

Recomendación 2:

Se recomienda crear un Plan de Continuidad de Negocio siempre que sea posible, lo que permitirá:

- Conocer el estado actual de la organización, determinar las amenazas que afectan a los sistemas y servicios e identificar las salvaguardas necesarias para proteger la disponibilidad de los sistemas.
- Disponer de acciones específicas que llevar a cabo en caso de una degradación de la disponibilidad del sistema, permitiendo una recuperación eficiente en un tiempo predeterminado.

1.1. FASE 0: DETERMINACIÓN DEL ALCANCE

13. La principal función de esta fase es determinar la magnitud y coste del Plan de Continuidad, así como su viabilidad futura.

14. Se deberán determinar los elementos que serán objeto de la mejora de continuidad, quedando así implicados:

    - El personal. DD
    - Los activos de información.
    - Los sistemas informáticos.
    - Otros servicios y procesos de la organización.

15. Habitualmente el alcance se centrará en aquellos sistemas y procesos de mayor criticidad, en los cuales una pérdida de disponibilidad tendría un alto impacto sobre la organización.

1.2. FASE 1: ANÁLISIS DE LA ORGANIZACIÓN

16. Esta fase busca la obtención y comprensión de las tecnologías, procesos y recursos de la organización. Se analizarán también las posibles amenazas que afectan a la organización. De esta forma, se podrá determinar con exactitud qué se quiere proteger y cómo, para poder abordar las fases posteriores con precisión.

17. Las siguientes tareas se pueden utilizar para analizar la organización eficazmente:

    - Mantener reuniones con los responsables de los procesos críticos. De tal forma que se conozca el detalle de las dependencias del proceso que se desea proteger.

    - **Análisis del impacto sobre el negocio** (BIA – *Business Impact Analysis*). Este documento ayudará a clasificar los procesos que se desean proteger según su criticidad y a identificar los activos de los que dependen dichos procesos. Contendrá los requisitos temporales y de recursos de los procesos (el detalle de las métricas utilizadas se encuentra en el apartado 2. Métricas):

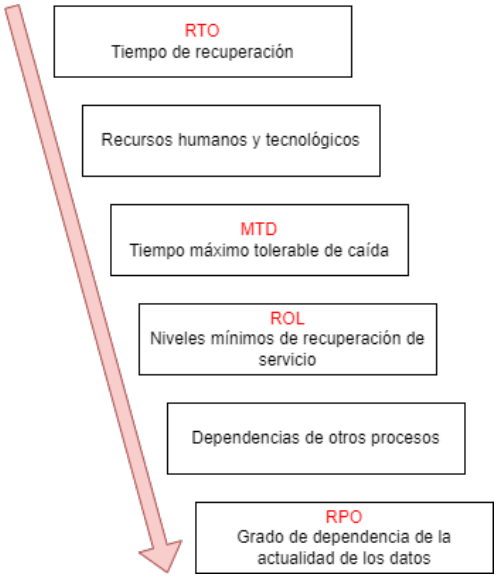


Ilustración 2. Métricas de un BIA

- **Análisis de riesgos**. Una vez identificados en las fases anteriores los distintos activos de la organización que se desea proteger, se estudiará qué amenazas pueden materializarse poniendo en riesgo los procesos dentro del alcance del Plan de Continuidad (ver apartado 5. Amenazas Contra la Disponibilidad). Se deberá determinar qué amenazas pueden implicar una indisponibilidad, su probabilidad de materialización y qué impacto tendrían sobre el proceso. Si se considera el producto de la probabilidad por el impacto, se podrá identificar aquellos riesgos que deben ser tratados con mayor prioridad y que, por tanto, deben ser protegidos mediante la implantación de salvaguardas (ver apartado 6. Protección contra las amenazas).
- **Plan de tratamiento de riesgos**. En base a los riesgos identificados, se definirá cómo se tratarán, siendo posible transferir el riesgo a un tercero, asumir el riesgo o implantar medidas para mitigarlo o eliminarlo. Habitualmente, se asumirán los riesgos que no alcancen un nivel de amenaza determinado; se mitigarán aquellos que sí sobrepasen dicho nivel y se transferirán los riesgos asociados a servicios o procesos prestados por terceros.

1.3. FASE 2: DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD

18. A partir de la información recopilada en las fases anteriores, se determinará cuál es la diferencia entre las necesidades de los procesos incluidos en el alcance y las capacidades de los recursos que utilizan actualmente.
19. De esta forma se identificará si los recursos y estrategias actuales permiten cubrir el MTD establecido para cada proceso. Se determinará qué estrategia seguir para cada elemento potencialmente afectado por una contingencia.
20. Se deberá contemplar la recuperación de los siguientes elementos:
    - Ausencias de personal.
    - Indisposición de la ubicación habitual de trabajo.
    - Fallos o ataques a las tecnologías.
    - Indisponibilidad de la información.
    - Indisponibilidad de los proveedores.

1.4. FASE 3: RESPUESTA A LA CONTINGENCIA

21. Una vez definidas las estrategias de recuperación, estas deben ser implementadas. Para ello, se comenzará desarrollando el Plan de Crisis o Incidentes, centrado en la gestión de una situación de crisis, evitando la toma de decisiones improvisadas.
22. El Plan de Crisis determinará:
    - El evento que determinará cuándo se da una situación de crisis.
    - Los flujos de toma de decisiones.
    - Los medios para la declaración de una situación de crisis.
    - El personal responsable de activar y gestionar el Plan.

- El contacto y los datos del personal implicado en la gestión de la crisis.
- Los niveles de priorización en la recuperación.
- Los requisitos temporales de puesta en marcha.
- Los planes operativos y el personal responsable de su activación.

23. Los planes operativos de recuperación contendrán información específica sobre el entorno al cual aplican, utilizando, como base para la recuperación de las infraestructuras, los procedimientos técnicos de trabajo. Estos últimos describirán cómo se deben llevar a cabo las tareas necesarias para la gestión y recuperación de una aplicación, sistema, infraestructura o entorno.

1.5. FASE 4: PRUEBA, MANTENIMIENTO Y REVISIÓN

24. El Plan de Continuidad de Negocio tiene como objeto la recuperación de manera óptima, reduciendo los tiempos de indisponibilidad. Por lo tanto, **se deberá mantener actualizado y se revisará periódicamente**.
25. Para ello, se llevarán a cabo pruebas sobre los entornos del alcance, al menos una vez al año, para probar su eficiencia y funcionamiento. Cualquier incidencia que se detecte se deberá analizar para mejorar o corregir, según se considere.

1.6. FASE 5: CONCIENCIACIÓN

26. La última fase de la implantación del Plan de Continuidad de Negocio es la concienciación al personal en relación al mismo. Las tareas de concienciación se centrarán en el personal implicado en los procesos críticos de negocio y el personal TIC.

4. AMENAZAS CONTRA LA DISPONIBILIDAD

27. A continuación, se definen las **principales amenazas contra la disponibilidad** que podrían materializarse en la organización. En función de las características de la organización, podrán aparecer otras amenazas más específicas, que será necesario identificar durante el Análisis de Riesgos del sistema.
28. Dichas amenazas, en muchas ocasiones, afectarán a varias dimensiones de la seguridad del sistema (disponibilidad [D], confidencialidad [C], integridad [I], autenticidad [A] y trazabilidad [T]).
29. **La identificación de las distintas amenazas que puedan afectar al sistema será determinante a la hora de establecer los requisitos de seguridad mínimos**. Para la protección contra estas amenazas, se deberán desarrollar los distintos procedimientos y desplegar las protecciones físicas y lógicas, detalladas en el Apartado 6. Protección contra las amenazas.

4.1 INTERRUPCIONES

30. La disponibilidad de un sistema puede verse alterada por dos (2) tipos de interrupciones:
    - **Interrupciones previstas**. Se realizan cuando el sistema se paraliza voluntariamente para realizar modificaciones o actualizaciones *software* y/o *hardware*.

- **Interrupciones imprevistas.** Suceden por incidencias imprevistas de naturaleza ambiental e involuntaria (apagones, errores del *hardware*/*software*, desastres naturales, etc.) o por influencia humana (*malware*, negligencia operativa, mantenimiento incorrecto, intrusiones, etc.).

4.1.1 FALLOS DE HARDWARE

31. Una interrupción imprevista puede suceder en caso de fallo en el *hardware* del sistema. La probabilidad de que sucedan estos fallos es baja durante la vida útil del *hardware*, pero se eleva rápidamente una vez finaliza esta.

Ilustración 3. Gráfico probabilidad de fallo del hardware

32. Tal como se puede ver en el gráfico, la mayor probabilidad de fallo se da al principio de la vida del producto, en las pruebas previas a salir de fábrica, y cuando finaliza su vida útil.

Recomendación 9:

Se recomienda mantener un inventario actualizado de los activos *hardware* del sistema, sustituyendo aquellos que sea necesario una vez alcancen el fin de su vida útil.

4.1.2 FALLOS DE *SOFTWARE*

33. Las interrupciones imprevistas también pueden venir dadas por fallos de *software*. Estos fallos se pueden dividir en fallos del *software* propio o de terceros.

34. En el caso de los fallos en el *software* de terceros, el comportamiento será similar a los fallos *hardware*.

35. Los fallos en el *software* propio se pueden identificar a través de un registro de la densidad de defectos de *software* en el sistema. Este número puede obtenerse haciendo un seguimiento del historial de defectos del *software*. La densidad de defectos dependerá de los siguientes factores:

- Proceso utilizado para desarrollar y diseñar el código.

- Complejidad del *software*.
- Tamaño del *software*.
- Experiencia del equipo que desarrolla el *software*.
- Porcentaje de código reutilizado de un proyecto estable anterior.
- Rigor y profundidad de las pruebas antes de enviar el producto.
- La densidad de defectos se suele medir en número de defectos por cada mil líneas de código (defectos/KLOC).

4.2 AMENAZAS FÍSICAS

36. Estas se pueden dividir principalmente en:

- **Sabotajes.** Ataques físicos llevados a cabo intencionadamente. Por ejemplo, cortes de cableados de equipos o red o incendios provocados.
- **Desastres naturales o causas externas**. Problemas con los sistemas o la ubicación de los sistemas por causas externas a la organización. Por ejemplo, terremotos, incendios o inundaciones no provocadas.
- Cortes, subidas o bajadas repentinas de **suministro eléctrico**.

4.3 AMENAZAS LÓGICAS

37. Estas se pueden dividir en distintos ataques o situaciones:

- ***Malware***. Virus informáticos que puedan afectar a la disponibilidad de los datos o el servicio. Por ejemplo, *ransomware*.
- **Malas configuraciones**. Configuraciones incorrectas de los sistemas que pueden provocar problemas de disponibilidad. Por ejemplo, servidores DNS con el KSK de la zona raíz de DNSSEC obsoleto.
- **Denegación de servicio (DoS)**. Ataques que afecten a la capacidad de suministro del servicio. Por ejemplo, el envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
- **Denegación de servicio distribuida (DDoS).** Ataques distribuidos que afecten a la capacidad de suministro del servicio. Por ejemplo, inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

5. PROTECCIÓN CONTRA LAS AMENAZAS

38. Una vez identificadas las distintas amenazas presentes en la organización, la necesidad de protegerse contra ellas y la prioridad con la que debe hacerse, se deberán implantar las distintas salvaguardas que permitan impedir la materialización de dichas amenazas o mitigar su impacto, para lograr eliminar o reducir a valores aceptables el riesgo de la organización.

39. Estas salvaguardas pueden organizarse en tres (3) categorías:

- **Disponibilidad por diseño**. Son decisiones a nivel de diseño que permiten lograr un mayor grado de disponibilidad.
- **Protección física**. Se trata de aquellas medidas tomadas para proteger las instalaciones y sistemas contra amenazas físicas.
- **Protección lógica**. Se trata de aquellas medidas tomadas para proteger las instalaciones y sistemas contra amenazas lógicas.

5.1 ALTA DISPONIBILIDAD EN EL DISEÑO DEL SISTEMA

5.1.1 TOLERANCIA A FALLOS

40. Se puede lograr tolerancia ante fallos mediante la redundancia de dispositivos *hardware* y *software* en la organización. Se analizará la necesidad de dicha redundancia en función de la criticidad de los sistemas y servicios.
41. Para lograr alta disponibilidad mediante redundancia, se dispondrá de los dispositivos necesarios para dar servicio, en activo, y adicionalmente de uno o varios dispositivos adicionales en espera que, en caso de fallo, puedan retomar el servicio en un corto periodo de tiempo.
42. Se describen a continuación los distintos modelos existentes, así como el comportamiento de sus nodos en caso de fallo.
    - **Modelo de equilibrio de carga (activo-activo).** Tanto el nodo primario como el secundario son activos y procesan las solicitudes del sistema en paralelo. Los datos se replican de forma bidireccional en función de los servicios del sistema. El tiempo de recuperación en caso de fallo de un nodo en este modelo es cero.
    - **Modelo de espera caliente.** Ambos nodos disponen del *software* instalado y disponible. El nodo secundario se encuentra activo y en ejecución, pero no procesa de forma activa datos hasta que falla el nodo primario. En este caso, el tiempo de recuperación es de pocos segundos.
    - **Modelo de espera templada**. En este modelo, los nodos disponen del *software* instalado y disponible, pero el nodo secundario no está ejecutándolo. En caso de fallo en el nodo primario, mediante un gestor de clúster, el nodo secundario inicia los componentes de *software*. Los datos se replican regularmente en el nodo secundario o se almacenan en un disco compartido. El tiempo de recuperación en caso de fallo es de pocos minutos.
    - **Modelo de espera fría**. El nodo secundario dispone de la misma configuración que el primario, pero se encuentra apagado. Solo se enciende y entra en acción en caso de fallo en el nodo primario. Los datos pueden ser copiados en un sistema de almacenamiento y restaurados en el nodo secundario en caso necesario. Es el modelo más lento y puede tardar unas horas en recuperarse.

5.1.2 REDUNDANCIA EN LAS COMUNICACIONES

43. Es necesario, a su vez, asegurar la disponibilidad de las comunicaciones de la organización mediante su redundancia. Esta se debe proteger en dos ámbitos distintos:

- Redundancia de los dispositivos empleados para llevar a cabo las comunicaciones.
    - Lograda a través de los mecanismos descritos en el anterior apartado (5.1.1 TOLERANCIA A FALLOS).
    - Mediante el empleo del protocolo VRRP (*Virtual Router Redundancy Protocol*). Se trata de un protocolo no propietario que elimina el punto único de fallo en una red mediante la generación de un router virtual empleado como puerta de enlace, en lugar del router físico. Realiza la configuración en dos o más router físicos que representan el router virtual, realizando el enrutamiento solo uno de ellos. En caso de fallo en el router físico que realiza el enrutamiento, otro lo sustituye, impidiendo una degradación en el servicio.
- Redundancia de los canales de comunicación. En este caso, se logrará mediante la duplicación de los canales de comunicación. Es decir:
    - Una red de cableado interna alternativa, disponible en caso de fallo en la red principal.
    - Una red externa alternativa, contratada con un Operador distinto al que suministre red principal. De tal forma que, en caso de problema con el Operador principal, se disponga de una contingencia inmediata.

5.1.3 *CLUSTERING*

44. Un tipo de redundancia comúnmente extendido es el *clustering*. Se basa en la unión de varios servidores que trabajan en una red como si fuesen uno solo, compartiendo servicios y monitorizándose entre sí. En función de la tecnología se distinguen tres (3) tipos de clúster:
    - Clúster *hardware*: unión de varios servidores físicos.
    - Clúster *software*: unión de varios servidores virtuales.
    - Clúster de bases de datos: en este caso se puede tratar de bases de datos virtuales o físicas, pero se comparte únicamente los datos.
45. También se pueden distinguir en función de la topología utilizada:
    - Topología N+1: en estas topologías solo hay un nodo en espera para adoptar el rol activo en caso de fallo. En esta situación el nodo secundario debe ser capaz de proveer los mismos servicios que el nodo primario.
    - Topología N+M: en estas topologías se dispone de varios nodos en espera para adoptar el rol activo. En este caso, cada nodo en espera podría no disponer de todos los servicios del nodo primario, utilizando varios nodos en espera en caso de fallo.
    - Topología N-to-1: en este caso se dispone de un solo nodo secundario. En caso de fallo el nodo secundario pasa a ser un remplazo temporal activo hasta que se restaure el primero.

- Topología N-to-N: se dispone de varios nodos secundarios. En caso de fallo los servicios del nodo principal se distribuyen entre los nodos secundarios. No hay nodos en espera, pero todos deben ser capaces de adoptar cualquier servicio. Esta topología combina un clúster activo-activo con N+M.

5.1.4 VIRTUALIZACIÓN

46. La virtualización de máquinas y sistemas puede ayudar a lograr un alto grado de disponibilidad debido a que, en caso de fallo, se pueden sustituir en un corto periodo de tiempo, pudiendo incluso volver a un estado previo de la máquina.

47. Permiten también una mayor escalabilidad, ahorrando el proceso de adquisición de *hardware* y permiten lograr redundancia de forma más sencilla. De esta forma, por ejemplo, se podría disponer de una máquina activa dando servicio y una máquina en espera, con la misma configuración, que se activaría en caso de error.

5.1.5 SISTEMAS DE ALMACENAMIENTO

48. Existen también distintos sistemas de almacenamiento que proporcionan mejoras en la disponibilidad y seguridad de los datos.

- **RAID (*Redundant Array of Independent Disks*)**. Se trata de un conjunto redundante de discos independientes, entre los que se distribuyen y replican los datos. Es una medida que busca la aumentar el rendimiento, aumentar la capacidad de almacenamiento y mejorar la tolerancia a fallos del sistema del almacenamiento, según el tipo de Nivel RAID. A continuación, se describen los niveles más comunes:
  - RAID 0: también llamado *data striping*. Distribuye los datos equitativamente entre los discos, sin duplicidades, por lo que los datos no son redundantes. Aporta un alto rendimiento, pero no mejora el nivel de disponibilidad.
  - RAID 1: también llamado *data mirroring*. Crea una copia exacta de los datos en varios discos. De esta forma el volumen de datos almacenados en el conjunto RAID 1 será, como máximo, el del menor de sus discos. Aporta un alto grado de disponibilidad al duplicar todos los datos en discos duros independientes.
  - RAID 5: también llamado conjunto dividido con paridad distribuida. Requiere al menos tres (3) unidades de disco. Los datos se dividen en bloques, distribuyendo la información de paridad entre todos los discos, de esta forma si falla uno se puede recuperar la información a partir de los demás discos.
- **SAN (*Storage Area Network*).** Se trata de una solución de almacenamiento en red que proporciona acceso al almacenamiento a nivel de bloque. Presenta los dispositivos de almacenamiento a los usuarios de red como si fuesen locales. Las ventajas de SAN son:
  - Proporciona varias rutas para acceder a los datos.

- Mejora el rendimiento de las aplicaciones al acelerar la consulta de información.

- **NAS (*Network Attached Storage*)**. Se trata de una solución de almacenamiento en red que proporciona acceso al almacenamiento a nivel de archivos de datos. Se conecta un dispositivo a la red que proporciona los servicios de acceso a ficheros. Las ventajas de NAS son:
  - Simplifica las copias de seguridad y la recuperación de datos.
  - Permite el acceso a los datos desde todas las ubicaciones de red necesarias.

5.1.6 CLOUD

49. El empleo de entornos *Cloud* también puede ayudar a mejorar la disponibilidad, tanto de los servicios como los datos.
50. El almacenamiento de datos y copias de seguridad en la nube proporciona un grado adicional de disponibilidad, pero deberá ir acompañado de Acuerdos a Nivel de Servicio (SLA) adecuados y se deberá prestar especial atención a la confidencialidad de los datos. Se podría requerir, por tanto, que los datos se almacenen cifrados, en caso de que sean confidenciales, sensibles o de carácter personal.
51. El uso de servicios *Cloud* también permite mayor disponibilidad debido a la facilidad de despliegue, ampliación de recursos y tolerancia a fallos de los entornos. De igual manera, se deberá prestar especial atención durante la definición de los SLA, para determinar de forma clara y precisa los niveles de disponibilidad y seguridad necesarios.

5.2 SEGURIDAD FÍSICA Y AMBIENTAL

5.2.1 CENTROS DE RESPALDO

52. Como protección contra posibles desastres naturales, incendios, inundaciones, o cualquier problema en las instalaciones, se debe valorar disponer de instalaciones de respaldo, capaces de garantizar la disponibilidad de los datos y servicios de la organización.
53. Este tipo de respaldos requieren tener en cuenta varios aspectos:
    - La localización de respaldo debe situarse a una distancia mínima de la principal, para asegurar que, en caso de desastre natural, este no afecte a ambas.
    - Los datos de la instalación de respaldo deben estar actualizados para permitir dar continuidad al servicio. Por lo tanto, será necesario realizar copias de seguridad periódicas y copiarlas de forma segura en dicha instalación. En función de la criticidad del servicio, se deberá valorar mantener una copia síncrona de los datos.
54. Los centros de respaldo pueden mantenerse disponibles de distintas maneras, en función de las necesidades de la organización y el tiempo de recuperación:
    - **Sitio frío**. Dispone de los suministros y mobiliario necesarios para la operación. Se deberán llevar todos los equipos, el *software*, el personal y los datos necesarios.
    - **Sitio templado**. Dispone de los suministros, el mobiliario y gran parte del *hardware* y *software*. Se deberán llevar los equipos y programas específicos, el personal y los datos necesarios.

- **Sitio caliente**. Dispone de toda la infraestructura salvo equipos o *software* muy específico. Solo es necesario aportar los datos y el personal. Generalmente permiten realizar anualmente un simulacro.
- **Sitio espejo**. Aporta una redundancia completa respecto a la ubicación habitual. Solo es necesario mover al personal para retomar la operación normal de la organización.

5.2.2 CENTRO DE PROCESAMIENTO DE DATOS (CPD)

55. Los CPDs son salas o instalaciones debidamente acondicionadas que contienen servidores y redes de comunicación necesarias para la operación de la organización. Mantienen una gran cantidad de dispositivos informáticos y electrónicos.
56. Estos centros ayudan a lograr un alto grado de protección física gracias a la implementación de las siguientes medidas:
    - Monitorización de la ubicación mediante video vigilancia.
    - Control de acceso estricto.
    - Control ambiental (humedad y temperatura) y prevención contra incendios e inundaciones.

5.2.3 PROTECCIÓN DEL ENTORNO FÍSICO

57. Las medidas más importantes de protección del entorno físico son:
    - **Control de acceso físico**. El control de acceso físico ayuda a prevenir sabotajes y robos en las instalaciones de la organización dado que se permite el acceso a los recursos únicamente a aquellas personas que esté autorizadas.
    - **Sistemas de alimentación ininterrumpida (SAI).** Dispositivo formado por baterías que proporciona suministro eléctrico a los dispositivos conectados durante un tiempo limitado, en caso de corte en el suministro habitual. Previene los cortes de energía, las subidas y las bajadas de tensión.
    - **Fuentes de alimentación redundantes**. Suministro de energía proporcionado por dos (2) proveedores distintos, con distintas redes. De tal forma, un fallo de un proveedor o red, no supondrá una pérdida total de la energía.

Recomendación 10:

En caso de fallo del suministro principal de energía, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

5.3 SEGURIDAD LÓGICA

5.3.1 AUDITORÍA DE SEGURIDAD DE LOS SISTEMAS

58. De forma general, las auditorías de seguridad de los sistemas abarcan el análisis y la gestión de los sistemas para identificar y corregir posibles vulnerabilidades. El objetivo de la auditoría de seguridad es:

    - Verificar la seguridad de entornos y sistemas.
    - Verificar el cumplimiento con legislaciones y normativas.
    - Realizar un informe que permita la posterior mejora.

Recomendación 11:

Se recomienda realizar este proceso secuencial de auditoría de forma periódica, permitiendo así la mejora de la seguridad del sistema de forma progresiva en caso necesario. El proceso de auditoría puede llevarse a cabo de forma interna o puede contratarse a una empresa externa para realizarlo.

5.3.2 PROTECCIÓN CONTRA ATAQUES

59. En la actualidad, existen muchos ataques a los equipos, sistemas y redes que pueden desembocar en una degradación del servicio. Para proteger la organización contra estos ataques, se pueden utilizar distintas herramientas y salvaguardas:

    - Dispositivos de protección de perímetro: Cortafuegos, Servidores proxy, Pasarelas de intercambio seguro, diodos de datos.
    - Balanceadores de carga.
    - Sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).
    - Protección de las comunicaciones mediante redes privadas virtuales (VPN).
    - Uso de software antimalware: Endpoint Protection Platform (EPP) y Endpoint Detection and Response (EDR).
    - Políticas de contraseñas.
    - Control de acceso a los equipos y cuentas de usuario.
    - Planificación y dotación del sistema de capacidad suficiente para atender la carga prevista, con holgura para posibles picos de servicio.

5.3.3 ACUERDOS A NIVEL DE SERVICIO (SLA)

60. En los casos donde se requiera la contratación de recursos externos para el desarrollo de las actividades de la organización, será necesario establecer contractualmente un Acuerdo de Nivel de Servicio.

61. Este acuerdo incluirá las características del servicio prestado, lo que debe entenderse como "servicio mínimo admisible", así como, la responsabilidad del prestador y las consecuencias en caso de incumplimiento.

62. Entre las distintas cláusulas que deberán componer el documento, se destacan las siguientes relativas a la disponibilidad del servicio:

    - **Gestión de copias de seguridad y restauración de datos.** La entidad adjudicataria deberá disponer de mecanismos para implementar una política de respaldo y de pruebas de recuperación que contemplen como mínimo:
        - Identificación del alcance de los respaldos.
        - Política de copias de seguridad.
        - Medidas de cifrado de información en respaldo.
        - Procedimiento de solicitud de restauraciones de respaldo.
        - Realización de pruebas de restauración.
        - Traslado de copias de seguridad (si aplica).
    - **Plan de continuidad.** Para garantizar la continuidad del servicio prestado objeto del contrato, la entidad adjudicataria, deberá disponer y presentar un plan de recuperación ante cualquier contingencia. Este plan se activará ante la indisponibilidad total o parcial de los recursos principales, que por cualquier motivo provoque la indisponibilidad de los servicios prestados. Este plan incluirá:
        - La identificación y descripción de los medios alternativos planificados para la provisión de los servicios, personal alternativo, existencia o planificación de instalaciones y medios de comunicación alternativos, etc.
        - Realización de al menos una prueba de recuperación anual. El informe final de la prueba deberá ser remitido al responsable que determine la organización, así como un plan de trabajo con acciones correctivas si se detectaran eventos o acciones a corregir.
        - Actualización de la documentación del plan de recuperación ante desastres tanto como sea necesario.

63. Deberá quedar acordado, mediante métricas:

    - La disponibilidad de los servicios contratados:
        - Se determinará, en porcentaje, el tiempo que los servicios contratados deben permanecer activos y dar servicio (por ejemplo: 99,99%).
    - La disponibilidad del almacenamiento:
        - Se determinará, en porcentaje, el tiempo que el almacenamiento deberá estar activo y dando servicio. Por ejemplo: 99,99%.
    - La disponibilidad de las copias de seguridad:

- Se determinará, en porcentaje, el número de copias de seguridad planificadas que deberán ejecutarse con éxito. Por ejemplo: 99,9%.

- Fiabilidad de la recuperación de datos:
  - Se determinará, en porcentaje, el número de recuperaciones desde copias de seguridad ejecutadas correctamente (por ejemplo: 99%).
- Activación del servicio de respaldo:
  - Se determinará, en horas, el tiempo consumido en poner en marcha el servicio de respaldo. Por ejemplo, 24h.
- Disponibilidad de la capacidad contratada:
  - Se determinará, en días, un umbral de uso de recursos en el cual la entidad adjudicataria deberá avisar a la organización, con objeto de autorizar el aumento de recursos.

5.4 COPIAS DE SEGURIDAD

64. Las Copias de Seguridad o Respaldo son una herramienta de gran importancia para preservar la disponibilidad de los datos y servicios de la organización.
65. **Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio** en caso de pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración, e incluso la imagen del sistema operativo. Para determinar qué información se incluirá en las copias de seguridad, se clasificará en base a la criticidad para el servicio y el impacto en caso de pérdida.
66. Para definir y estructurar la forma de realizar dichas copias de seguridad, se puede desarrollar una **Política de Copias de Seguridad** en la organización. Esta deberá incluir, para todos los sistemas críticos, la siguiente información:
    - Periodicidad de las copias de respaldo.
    - Periodos de retención de las copias.
    - Ubicación de los soportes de respaldo, tanto en la ubicación propia como en posibles ubicaciones remotas.
    - Controles para el acceso autorizado a las copias de respaldo.
    - Procedimientos de recuperación de la información.
    - Procedimientos de restauración y verificación de la integridad de la información respaldada.
    - Procedimientos de inventario y gestión de soportes.

Recomendación 3:

Se recomienda crear una Política de Copias de Seguridad, lo que permitirá determinar con exactitud qué información debe respaldarse y, en función de su criticidad, con qué periodicidad. Además, permitirá definir procedimientos para realizar las tareas de copia y restauración con unas garantías mínimas de seguridad.

Recomendación 4:

Se recomienda llevar a cabo la automatización de los procedimientos de copias de seguridad, de tal forma que se reduzca la probabilidad de no realizar ciclos de respaldo. Esto se podrá llevar a cabo haciendo uso de sistemas de administración de soportes.

5.4.1 TIPOS DE *BACKUP*

67. Las copias de seguridad se pueden categorizar en tres (3) tipos:

- **Copia de seguridad 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. Debido a la carga que conlleva sobre el sistema, se recomienda realizar este tipo de copias fuera del horario laboral.
- **Copia de seguridad 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, ya que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.
- **Copia de seguridad 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.

68. La selección del tipo de copia de seguridad a realizar se deberá hacer teniendo en cuenta los siguientes parámetros:

- Tipo de datos a copiar y su criticidad, determinada en el Análisis de Riesgos de la organización. Se debe tener en cuenta el volumen de datos total y el volumen de datos modificados/generados por la organización.
- RTO o Tiempo de Recuperación. Como se ha visto anteriormente, este valor determina el tiempo tras el cual un proceso debe estar en funcionamiento tras un fallo. Por lo tanto, se deberá seleccionar un tipo de copia de seguridad cuyo tiempo de recuperación permita cumplir con el tiempo impuesto.
- Los soportes empleados para realizar las copias, ya que de estos dependerá, en gran parte, la velocidad de las copias.

5.4.2 FRECUENCIA DE LAS COPIAS

69. Con carácter general, la frecuencia de realización de las copias de seguridad será determinada por las organizaciones en función de la sensibilidad y el impacto de la indisponibilidad de la información almacenada.

Recomendación 5:

De forma específica, para aquellos ficheros que contengan datos de carácter personal, se deberá tener en cuenta:

- Se deben crear procedimientos para la realización de, al menos, una copia de respaldo semanal, si en tal periodo se hubiese producido alteración o modificación de los datos.
- Cuando las pruebas anteriores a la implantación o modificación de los sistemas de información, se deberá realizar previamente una copia de seguridad de los datos.
- Cuando finalice el periodo de tratamiento de los datos personales, estos deberán eliminarse también de todas las copias en las que pudieran estar.

5.4.3 ALMACENAMIENTO DE LAS COPIAS

70. Se deberá definir el periodo de retención de las copias de seguridad en función de la información que contengan. Por ejemplo, es posible que los datos de tipo “logs de auditoría” requieran un periodo de retención superior a otros datos, para la realización de actividades administrativas o legales. Una vez se alcance el periodo de retención de la información, esta deberá ser eliminada de forma segura.

71. El almacenamiento de los soportes de copias de respaldo se realizará en armarios ignífugos, bajo llave y restringiendo el acceso a personal previamente autorizado.

Recomendación 6:

Se recomienda almacenar la última copia de seguridad realizada, junto con los procedimientos de recuperación, en una ubicación externa al sistema para minimizar el riesgo a una pérdida de datos en caso de una contingencia en la ubicación usual de trabajo. Se deberán tomar las siguientes cautelas:

- 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 instalaciones de la organización, como en las sedes de almacenamiento alternativas.

La información almacenada fuera de las ubicaciones de la organización deberá ser cifrada, cumpliendo con los estándares definidos en la guía CCN-STIC 807. Se definirá un procedimiento de envío y recepción de soportes que permita asegurar que estos no son extraviados ni manipulados en su transporte.

Recomendación 7:

Se recomienda seguir las siguientes pautas:

- Realizar dos (2) copias de la información que se ha determinado que debe salvarse.
- Almacenar dichas copias en dos (2) soportes distintos de almacenamiento, de tal forma que, en caso de problema con uno, se siga disponiendo de otra copia.
- Almacenar una copia fuera de la organización.
- Revisar periódicamente la vida útil de los soportes utilizados para realizar las copias.

5.5 PRUEBAS DE RESTAURACIÓN

72. Se deberán realizar pruebas periódicas de restauración para verificar el correcto funcionamiento de los procedimientos de recuperación de copias de seguridad. Tanto las pruebas como los resultados se documentarán, permitiendo así la subsanación de cualquier incidencia que pudiese suceder.

73. En los casos en los cuales los ficheros 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.

Recomendación 8:

Se recomienda realizar pruebas periódicas de restauración para verificar el correcto funcionamiento de los procedimientos de recuperación de copias de seguridad.

6. RESUMEN DE RECOMENDACIONES

Nº	Ámbito	Recomendación
1	**Métricas**	Se recomienda tratar de alcanzar un RTO máximo para los procesos de la organización de: • Cuatro (4) horas para sistemas críticos que requieren de una alta disponibilidad. • Un (1) día para sistemas que requieren de una disponibilidad moderada. • Cinco (5) días para sistemas que requieren de una disponibilidad baja.
2	**Plan de Continuidad de Negocio**	Se recomienda crear un Plan de Continuidad de Negocio siempre que sea posible, lo que permitirá: • Conocer el estado actual de la organización, determinar las amenazas que afectan a los sistemas y servicios e identificar las salvaguardas necesarias para proteger la disponibilidad de los sistemas. • Disponer de acciones específicas que llevar a cabo en caso de una degradación de la disponibilidad del sistema, permitiendo una recuperación eficiente en un tiempo predeterminado.
3	**Copias de seguridad**	Se recomienda crear una Política de Copias de Seguridad siempre que sea posible, lo que permitirá determinar con exactitud qué información debe respaldarse y, en función de su criticidad, con qué periodicidad. Además, permitirá definir procedimientos para realizar las tareas de copia y restauración con unas garantías mínimas de seguridad.
4	**Copias de seguridad**	En aquellos casos en los que sea posible, se recomienda llevar a cabo la automatización de los procedimientos de copias de seguridad, de tal forma que se reduzca la posibilidad de no realizar ciclos de respaldo. Esto se podrá llevar a cabo haciendo uso de sistemas de administración de soportes.
5	**Copias de seguridad**	De forma específica, para aquellos ficheros que contengan datos de carácter personal, se deberá tener en cuenta: • Se deben crear procedimientos para la realización de, al menos, una copia de respaldo semanal, si en tal periodo se produce alteración o modificación de los datos. • Cuando las pruebas anteriores a la implantación o modificación de los sistemas de información, se deberá realizar previamente una copia de seguridad de los datos. • Cuando finalice el periodo de tratamiento de los datos personales, estos deberán eliminarse también de todas las copias en las que pudieran estar.

Nº	Ámbito	Recomendación
6	**Copias de seguridad**	Se recomienda almacenar la última copia de seguridad realizada, junto con los procedimientos de recuperación, en una ubicación externa, para minimizar el riesgo a una pérdida de datos en caso de una contingencia en la ubicación usual de trabajo. Se deberán tomar las siguientes cautelas: • 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 ubicaciones de la organización, como en las sedes de almacenamiento alternativas. Adicionalmente, en todos los casos, la información almacenada fuera de las ubicaciones de la organización, deberá ser cifrada, cumpliendo con los estándares definidos en la guía CCN-STIC 807. Se definirá un procedimiento de envío y recepción de soportes que permita asegurar que estos no son extraviados ni manipulados en su transporte.
7	**Copias de Seguridad**	Se recomienda seguir las siguientes pautas: • Mantener tres copias de la información que se ha determinado debe salvarse: el original y dos copias. • Almacenar dichas copias en dos soportes distintos de almacenamiento, de tal forma que, en caso de problema con uno, se siga disponiendo de otra copia. • Almacenar una copia fuera de la organización. • Revisar periódicamente la vida útil de los soportes utilizados para realizar las copias.
8	**Copias de Seguridad**	Se recomienda realizar pruebas periódicas de restauración para verificar el correcto funcionamiento de los procedimientos de recuperación de copias de seguridad.
9	**Tolerancia a fallos**	Se recomienda mantener un inventario actualizado de los activos *hardware* del sistema, sustituyendo aquellos que sea necesario una vez alcancen el fin de su vida útil.
10	**Protección física**	En caso de fallo del suministro principal de energía, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información
11	**Auditoría de seguridad de los sistemas**	Se recomienda realizar este proceso secuencial de auditoría de forma periódica, permitiendo así la mejora de la seguridad del sistema de forma progresiva en caso necesario. El proceso de auditoría puede llevarse a cabo de forma interna o puede contratarse a una empresa externa para realizarlo.

7. ABREVIATURAS

BIA	*Business Impact Analysis*
CPD	Centro de Procesado de Datos
DDoS	*Distributed Denial of Service*
DoS	*Denial of Service*
DNS	*Domain Name System*
DNSSEC	*Domain Name System Security Extensions*
EDR	*Endpoint Detection and Response*
ENS	Esquema Nacional de Seguridad
EPP	*Endpoint Protection Platform*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
KLOC	*Thousands of Lines Of Code*
KSK	*Key Signing Key*
MTD	*Maximum Tolerable Downtime*
MTTF	*Mean Time To Failure*
MTTR	*Mean Time To Recover*
NAS	*Network Attached Storage*
PCN	Plan de Continuidad de Negocio
PCTIC	Plan de Continuidad de las Tecnologías de Información y Comunicación
PRD	Plan de Recuperación ante Desastres
RAID	*Redundant Array of Independent Disks*
ROL	*Revised Operating Level*
RPO	*Recovery Point Objective*
RTO	*Recovery Time Objective*
SAI	Sistema de Alimentación Ininterrumpida
SAN	*Storage Area Network*
SLA	*Service Level Agreement*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Network*

8. REFERENCIAS

REF1 CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes

REF2 CCN-STIC-220 Arquitecturas virtuales

REF3 CCN-STIC-823 Utilización de servicios en la nube

REF4 Anexo III Guía CCN-STIC-822 Procedimiento de generación de copias de respaldo y recuperación de la información

REF5 CCN-STIC-820 Protección contra denegación de servicio

REF6 CCN-STIC-803 Valoración de Sistemas en el ENS

REF7 CCN-STIC-805 Política de Seguridad de la Información

REF8 EventHelix - *Reliability and availability basics*
https://www.eventhelix.com/fault-handling/reliability-availability-basics/

REF9 Seguridad y Alta Disponibilidad. Libro de Jesús Costas Santos. Editorial RaMa.

REF10 *NIST Special Publication 800-53 Revision 5 - Security and Privacy Controls for Information Systems and Organizations*

REF11 *NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers*

REF12 *BOE-A-2021-5032* - Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

REF13 *NIST Special Publication 800-34 rev1 - Contingency Planning Guide for Information Technology*

REF14 *RFC-3768 Virtual Router Redundancy Protocol.*
https://www.rfc-editor.org/rfc/rfc3768

ANEXO I. CATEGORIZACIÓN Y MEDIDAS PARA LA CONFORMIDAD CON EL ENS

74. Para las organizaciones que se encuentren dentro del ámbito del Esquema Nacional de Seguridad, será obligatorio establecer una serie de medidas y salvaguardas para el cumplimiento de los requisitos mínimos de disponibilidad. A fin de determinar el impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados, **se deberá establecer la categoría de seguridad de la dimensión de Disponibilidad [D]**.

75. Esa categorización servirá para conocer los activos y servicios de mayor importancia, permitiendo así seleccionar aquellas salvaguardas necesarias para la protección de los sistemas y priorizar estas mismas según su importancia.

76. Las categorías definidas dentro del marco del Esquema Nacional de Seguridad (ENS), son las siguientes:

- **Nivel BAJO**. Una interrupción en el acceso o uso de la información supone un perjuicio limitado sobre las funciones de la organización, sus activos o sobre los individuos afectados. Se entenderá por perjuicio limitado:
  - La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
  - Causar un daño menor en los activos de la organización.
  - El incumplimiento formal de alguna ley o regulación, que tenga carácter subsanable.
  - Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
  - Otros de naturaleza análoga.
- **Nivel MEDIO**. Una interrupción en el acceso o uso de la información supone un perjuicio grave sobre las funciones de la organización, sus activos o sobre los individuos afectados. Se entenderá por perjuicio grave:
  - La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
  - Causar un daño significativo en los activos de la organización.
  - El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
  - Causar un perjuicio significativo a algún individuo, de difícil reparación.
  - Otros de naturaleza análoga.
- **Nivel ALTO**. Una interrupción en el acceso o uso de la información supone un perjuicio muy grave sobre las funciones de la organización, sus activos o sobre los individuos afectados. Se entenderá por perjuicio muy grave:

- La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
- Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
- El incumplimiento grave de alguna ley o regulación.
- Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- Otros de naturaleza análoga.

77. Cuando el sistema trate distintas informaciones y preste diferentes servicios, el nivel de seguridad global del sistema será el mayor de los establecidos para cada información y servicio.
78. El detalle sobre cómo llevar a cabo la valoración de la categoría del sistema se puede consultar en la guía *CCN-STIC-803 Valoración de Sistemas en el ENS – REF6*.
79. A continuación, se indican las medidas a implementar que afectan exclusivamente a la disponibilidad:

Medida de seguridad	Nivel	Descripción	Refuerzos
[op] Marco Operacional			
[op.pl] Planificación			
[op.pl.4] Dimensionamiento / gestión de la capacidad	Alto: + R1 Medio: + R1 Bajo: Aplica	Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos: - [op.pl.4.1] Necesidades de procesamiento. - [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse. - [op.pl.4.3] Necesidades de comunicación. - [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional. - [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.	**Refuerzo R1** - Mejora continua de la gestión de la capacidad. - [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema. - [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.
[op.cont] Continuidad del Servicio			
[op.cont.1] Análisis de impacto	Alto: Aplica Medio: Aplica Bajo No Aplica	- [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.	**N/A**
[op.cont.2] Plan de continuidad	Alto: Aplica	Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos: - [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.	**Refuerzo R1** - Plan de emergencia y contingencia. - [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del

Medida de seguridad	Nivel	Descripción	Refuerzos
	Medio: No Aplica Bajo: No Aplica	- [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización. - [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes. - [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan. - [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.	análisis de Impacto, se determinarán los aspectos a cubrir. - Refuerzo R2 - Comprobación de integridad. - [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.
[op.cont.3] Pruebas periódicas	Alto: Aplica Medio: No Aplica Bajo: No Aplica	- [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.	**N/A**
[op.cont.4] Medios alternativos	Alto: Aplica Medio: No Aplica Bajo: No Aplica	- [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema: a) Servicios contratados a terceros. b) Instalaciones alternativas. c) Personal alternativo. d) Equipamiento informático alternativo. e) Medios de comunicación alternativos. - [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento. - [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.	**Refuerzo R1** - Automatización de la transición a medios alternativos. - [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Medida de seguridad	Nivel	Descripción	Refuerzos
[mp] Medidas de protección			
[mp.if] Protección de las instalaciones e infraestructuras			
[mp.if.4] Energía eléctrica	Alto: + R1 Medio: + R1 Bajo: Aplica	- [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.	**Refuerzo R1** - Suministro eléctrico de emergencia. - [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.
[mp.if.5] Protección frente a incendios	Alto: Aplica Medio: Aplica Bajo: Aplica	- [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.	**N/A**
[mp.if.6] Protección frente a inundaciones	Alto: Aplica Medio: Aplica Bajo: No Aplica	- [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.	**N/A**
[mp.info] Protección de la información			
[mp.info.6] Copias de seguridad	Alto: +R1 +R2	- [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.	**Refuerzo R1** - Pruebas de recuperación. - [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la

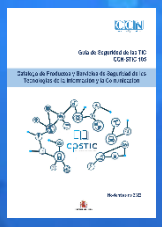
Medida de seguridad	Nivel	Descripción	Refuerzos
	Medio: +R1 Bajo: Aplica	- [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán: a) Frecuencia de las copias. b) Requisitos de almacenamiento en el propio lugar. c) Requisitos de almacenamiento en otros lugares. d) Controles para el acceso autorizado a las copias de respaldo.	criticidad de los datos y del impacto que cause la falta de disponibilidad. **Refuerzo R2** - Protección de las copias de seguridad. - [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
[mp.s] Protección de los servicios			
[mp.s.4] Protección frente a la denegación de servicio	Alto: +R1 Medio: Aplica Bajo: No Aplica	Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello: - [mp.s 4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista. - [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.	**Refuerzo R1** - Detección y reacción. - [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (*DoS y DDoS*). - [mp.s. 4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones. **Refuerzo R2** - Ataques propios. - [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

CCN-PYTEC
centro criptológico nacional

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

CPSTIC
CATÁLOGO DE PRODUCTOS Y SERVICIOS STIC

CATÁLOGO DE PRODUCTOS Y SERVICIOS DE SEGURIDAD TIC



PDF

ONLINE

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC

www.ccn.cni.es **https://oc.ccn.cni.es** **www.ccn-cert.cni.es**