NORMA ESPECÍFICA DE CONTINUIDAD DE ACTIVIDADES

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

1 INTRODUCCIÓN 4

2 ÁMBITO DE APLICACIÓN 6

3 CONTEXTO DE LA PRESENTE NORMA 6

4 VIGENCIA 7

5 TERMINOLOGÍA RELEVANTE 7

6 CONTINUIDAD DE LAS ACTIVIDADES 8

6.1 Referentes y Definiciones. 8

6.2 Proceso Integral. 9

6.3 Gestión. 9

6.4 Análisis de Impacto [op.cont1] 10

6.5 Planes de Continuidad o Planes de Contingencia [op.cont.2] 12

7 RESPONSABILIDADES 15

8 REVISIÓN DE LA NORMA 15

ANEXO I: REFERENCIAS 16

Medida op.cont.1 16

Medida op.cont.2 17

Medida op.cont.3 17

Medida op.cont.4 17

Medida mp.info.6 18

Cuadro Resumen del Documento

Tipo de Documento	Norma sobre responsabilidad de la información y criterios para su calificación
Autor	Oficina de Seguridad de la Información MUFACE
Fecha de elaboración	03/10/2025
Revisado por	Leonardo González García
Aprobado por	Silvia Lacleta (Responsable de Seguridad)

Control de Cambios

Versión	Fecha	Descripción de la modificación
1.0	03/10/2025	Versión inicial

1 Introducción

El Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad (ENS) en el ámbito de aplicación al sector público, según el artículo 2 de la Ley 40/2015 del 1 de octubre, y según el artículo 156.2, establece los principios básicos y requisitos mínimos requeridos para proteger la información. Las Administraciones Públicas deberán aplicarlo para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

Uno de los requisitos mínimos establecidos en el Esquema Nacional de Seguridad (ENS) es el de la continuidad de la actividad. Dicho requisito, desarrollado en el artículo 26 del ENS dispone que:

"Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales"

En el desarrollo normativo de la Política de Seguridad de MUFACE se ha preferido desglosar el cumplimiento de este requisito en dos normas diferentes, debido a la amplitud de las mismas y con objeto de disponer de un cuerpo normativo más claro y sencillo.

La norma de "Retención de la información y de la realización y almacenamiento de salvaguardad de información (backup)", que también forma parte del cuerpo normativo de la Política de Seguridad de la Información de MUFACE, responderá a la disposición de copias de seguridad y tenderá a asegurar principalmente la Información.

Esta norma específica de Continuidad de Actividades establece los mecanismos necesarios para garantizar la continuidad de las operaciones, y por tanto principalmente asegurar la continuidad de los Servicios en tres de los cinco ámbitos de seguridad definidos en la PSI de MUFACE:

- El ámbito de seguridad gestionado por la División de Sistemas de Información y Comunicaciones (DSIC).
- El ámbito de Seguridad gestionado por el INAP
- El ámbito de Seguridad gestionado por Muface.

La norma específica de continuidad de actividades trata también de reflejar dos de los principios básicos del Esquema Nacional de Seguridad. Por un lado, el principio básico de la Gestión de la Seguridad basada en los Riesgos (art. 6 del ENS), parte fundamental, como se verá más adelante, de cualquier plan de continuidad de actividades. Y por otro, el principio básico del Prevención, reacción y recuperación (art.7 del ENS) que alienta una serie de medidas y planes que permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

La serie de medidas descritas en el Anexo II del ENS [op.cont] de continuidad del servicio, guían también la redacción de esta norma. Medidas encaminadas a frenar incidentes desastrosos y permitir que los servicios se sigan prestando en unas condiciones mínimas tras la ocurrencia de un desastre. Entendiendo por desastre cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa. Estas medidas se entienden como complemento holístico de las medidas requeridas en otros puntos o normas relativas a medios alternativos y copias de seguridad de la información.

A primera vista la Seguridad de la Información y la Continuidad de la Actividad no tienen mucho en común, aparte de que ambas están actualmente fuertemente relacionadas con la Tecnologías de la Información. Sin embargo, el nexo de unión entre ambos conceptos tiene que ver con una de las dimensiones de seguridad que establece en ENS, **la disponibilidad**. Entendiendo como disponibilidad la propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieran.

Por lo tanto, el objetivo de la presente norma es sentar las bases que permitan garantizar la disponibilidad tanto de la información y de los servicios para aquellos que lo necesiten. Una adecuada gestión de la continuidad de la actividad permite a las organizaciones:

- Gestionar la interrupción de sus actividades de manera eficaz sin merma de su imagen.
- Adquirir una mayor flexibilidad ante la interrupción de su actividad.
- Disponer de una metodología estructurada para reanudar sus actividades después de una interrupción.

2 Ámbito de aplicación

Esta norma aplica a todos los usuarios (tanto internos como externos) con responsabilidad en la gestión de la seguridad en MUFACE, así como a todos aquellos usuarios con responsabilidad o involucrados en el aseguramiento de la continuidad de las actividades en los citados ámbitos de seguridad.

El ámbito de aplicación estricto se refiere a aquellos productos y servicios relacionados con el ejercicio de derechos, con el cumplimiento de deberes por medios electrónicos o con el acceso por medios electrónicos de los ciudadanos a la información, los servicios y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y con lo establecido por el ENS.

No obstante, lo establecido en el presente documento podrá ser, asimismo, de aplicación a todos aquellos sistemas o servicios que no queden contenidos en el ámbito de aplicación del ENS, si así se determinara por los responsables competentes.

3 Contexto de la presente norma

12. Este documento forma parte del cuerpo normativo de la Política de Seguridad de la Información (PSI) de la MUFACE, desarrollado para garantizar la seguridad de la información en la misma.

Es una norma específica que nace al amparo de la Norma sobre la Documentación de la Seguridad que especifica que cada ámbito de seguridad dentro de MUFACE debe desarrollar una norma específica que defina la continuidad de actividades según lo establecido en el ENS.

El *Responsable de Seguridad* correspondiente aprobará los procedimientos específicos que sean necesarios para el desarrollo de esta norma.

4 Vigencia

El presente documento es efectivo desde la fecha de aprobación, indicada en la segunda página del presente documento, y hasta que sea reemplazado por una nueva versión.

Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento. En cualquier caso, toda la información referente a versiones, modificaciones, etc., aparece descrita en la ficha de versiones al inicio del documento.

5 Terminología relevante

A lo largo del texto de los documentos de desarrollo normativo de seguridad requeridos por la PSI de MUFACE se citan una serie de definiciones, entre ellas algunas figuras o roles, a los que se aludirá con letra cursiva siguiendo la siguiente nomenclatura:

- **Usuario:** la persona o sistema que utiliza los sistemas de información de MUFACE, y/o a la información contenida en ellos.
- **Unidad TIC**: unidad encargada del desarrollo, mantenimiento y explotación del sistema de información al que estemos haciendo referencia.
- **Responsable del Sistema**: según define la PSI, esta responsabilidad recaerá en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes. Por tanto, según esta definición, recae sobre el titular de la Unidad TIC.
- **Responsable de Seguridad**: según define la PSI, la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y servicios.
- **Responsables de la Información:** según define la PSI, la persona que establece las necesidades de seguridad de la información que se maneja y efectúa las valoraciones del impacto que tendría un incidente que afectara a la seguridad. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione el procedimiento o trámite.
- **Responsables del Servicio:** según define la PSI, la persona que determina los requisitos de seguridad de los servicios prestados. Esta responsabilidad recaerá en el titular del órgano o unidad administrativa de cada servicio.

- **Norma específica de cada ámbito:** Una norma específica desarrolla con mayor detalle la norma correspondiente de aplicación general dentro del ámbito de competencia de cada Responsable de Seguridad, si se considera necesario por parte de éste. En caso de existencia de norma específica y de discrepancia entre ésta y la norma general, prevalecerá lo indicado en la específica para la información y servicios afectados por los sistemas de información gestionados por el ámbito de competencia del Responsable de Seguridad correspondiente.

6 Continuidad de las actividades

6.1 Referentes y Definiciones.

El Anexo A de la Norma ISO 27001 de Gestión de la Seguridad de la Información ofrece algunos controles dedicados exclusivamente a la continuidad del negocio con el objetivo de reaccionar a la interrupción de actividades y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

La norma ISO 22301:2012 – Sistemas de Gestión de la Continuidad, que se considera una actualización de la norma BD 25999-2, define la Continuidad del Negocio como la capacidad estratégica y táctica que tiene una organización para planificar y responder a incidentes e interrupciones del negocio con el fin de continuar con las operaciones críticas del negocio dentro de un nivel de servicio aceptable y asumible por la Organización.

La norma ISO/IEC 24762:2008 - Tecnología de la información - Técnicas de seguridad - Directrices para servicios de recuperación de desastres TIC, proporciona guía para la provisión de los servicios de recuperación de desastres en las tecnologías de la información y las comunicaciones como parte de la gestión de la continuidad del negocio, aplicable tanto a proveedores internos como externos de este tipo de servicios.

La norma ISO/IEC 27031:2011 - Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la información y tecnología de las comunicaciones para la continuidad del negocio, describe los conceptos y principio de las TIC en la continuidad del negocio, y proporciona un conjunto de métodos y procesos para identificar y especificar todos los aspectos para la mejora de la preparación de las TIC en la organización para asegurar la continuidad del negocio.

Todas estas referencias y definiciones pueden extrapolarse a la continuidad de las actividades, y han sido inspiradoras de la presente norma. En definitiva, se trata de planificar y anticipar, evitando tener que improvisar ante una contingencia, de manera que el modelo de gestión sirva para situaciones previstas e imprevistas.

6.2 Proceso Integral.

Como bien dice el ENS en su artículo 6, la seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

El caso de la gestión de continuidad de actividades se debe considerar como un proceso con entradas procedentes de diversas funciones (alta dirección, TI, operaciones, RRHH, etc.) y actividades (evaluación de riesgos, etc.).

Y, aunque en esta norma nos centramos en la continuidad de actividades que viene relacionadas con la seguridad, debemos asegurarnos la coherencia con otros planes o normas de continuidad no relacionados con los servicios de información que pudieran existir.

6.3 Gestión.

Se deberá implantar un proceso de gestión de continuidad de la actividad para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.

Este proceso deberá identificar los procesos críticos e integrar los requisitos de gestión de la seguridad de información para la continuidad de la actividad con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.

Se deberán analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los servicios esenciales se pueden restaurar en los plazos requeridos.

La gestión de la continuidad de la actividad debería incluir adicionalmente al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.

Por lo tanto, para desarrollar esta gestión de la continuidad de la actividad se deberán desarrollar en cada ámbito los Análisis de impacto dentro del Análisis y gestión de Riesgos, los Planes de Contingencias necesarios y la Prueba Periódica de todos ellos.

Las medidas del ENS, anexo II, del plan de continuidad y pruebas periódicas son aplicables para todos los sistemas cuya disponibilidad haya sido categorizada como nivel alto.

La organización debe evaluar la conveniencia de su aplicación también a los sistemas categorizados como nivel medio, teniendo en cuenta que los requisitos mínimos que exige el ENS podrán ser ampliados por causa del prudente arbitrio del responsable de seguridad del sistema, habida cuenta de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.
Así mismo en los sistemas o servicios cuya dimensión de Disponibilidad sea de nivel ALTO habrá de preverse medidas alternativas.

6.4 Análisis de Impacto [op.cont1]

Un análisis de impacto es aquella actividad que permite que una organización identifique los procesos críticos que apoyan a sus productos y servicios claves, las interdependencias entre procesos y recursos requeridos para operar los procesos en un nivel mínimamente aceptable.

Dicho análisis está íntimamente ligado al Análisis y Gestión de Riesgos y debe realizarse al mismo tiempo. La continuidad de la actividad y su gestión es un concepto ligado a la **gestión de riesgos** cuya finalidad es analizar los riesgos a que están expuestos los servicios y las operaciones, así como las consecuencias que provocarían dichos riesgos centrándose en el impacto de la interrupción de la actividad, identificando cuales son los productos y servicios de los que la organización depende para su supervivencia.

Esta gestión se debe realizar, tal como indica la metodología de análisis y gestión de riesgos de los sistemas de información Magerit v3.0, sobre todos los activos de los Sistemas de información de la organización. Entendiendo como activos a cualquier componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

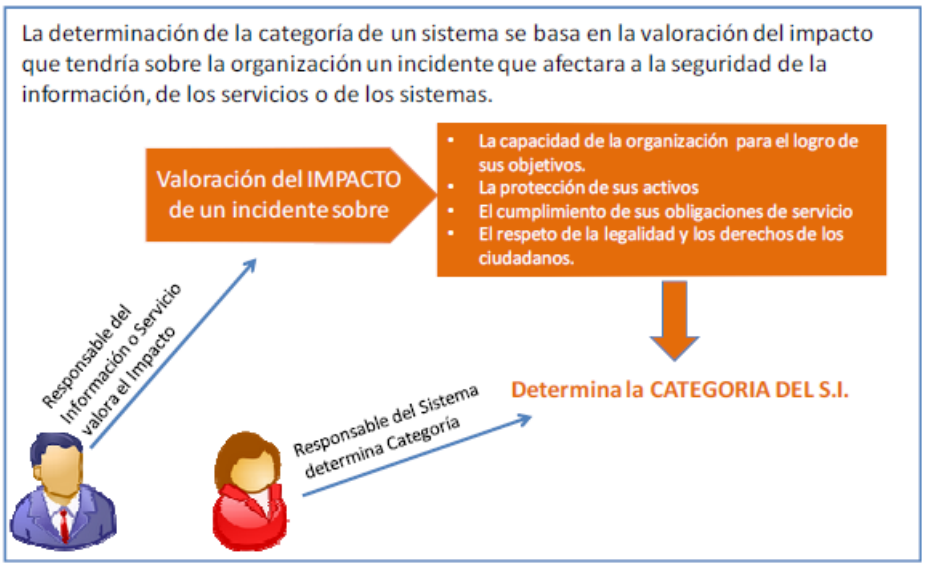
En un sistema de información hay 2 activos esenciales:

- La **información** que maneja.
- Los **servicios** que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** *(software)* que permiten manejar los datos.
- **Los equipos informáticos** *(hardware)* que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

Esta valoración o análisis del impacto resulta fundamental para la determinación de la categoría de los sistemas de información.



Para todos aquellos Sistemas de Información donde la dimensión de disponibilidad presente un nivel Medio o Alto se deberá realizar un análisis de impacto que permita determinar:

- Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
- Los elementos que son críticos para la presentación de cada servicio, bien sean propios o proporcionado por externos.

Dicho análisis de impacto deberá concluir en un informe formal, aprobado por la Dirección y sometido a un proceso de revisión periódica.

Una vez que los requisitos se han establecido a través del análisis de impacto en la actividad y la evaluación de riesgos, las estrategias pueden ser desarrolladas para identificar disposiciones que permitan que la organización proteja y recupere actividades críticas, basadas en la tolerancia de riesgo organizacional y dentro de objetivos de tiempo de recuperación definidos. Estas estrategias vendrán marcadas por los Planes de Continuidad definidos.

6.5 Planes de Continuidad o Planes de Contingencia [op.cont.2]

Un plan de Contingencia es un caso particular del Plan de Continuidad del negocio aplicado a los departamentos de Tecnologías de la Información. Otros departamentos pueden tener sus planes de continuidad que persiguen el mismo objetivo desde otro punto

de vista. Pero dada la importancia que las tecnologías de la información adquieren en una organización madura, el plan de contingencia es el más relevante.

Como esta norma está encuadrada dentro de la Política de Seguridad de la información, en este caso el Plan de Continuidad (de actividades) es lo que denominaremos Plan de Contingencia.

Este plan de continuidad o plan de contingencia contendrá las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las actividades de la organización.

El Plan de contingencia sigue el conocido ciclo de vida PDCA (Plan-do-check-act). Nace de un análisis de riesgos (identificar amenazas que afectan a la continuidad del negocio) para seleccionar contramedidas que se plasman en el plan de contingencia y que debe sufrir un proceso de mejora continua revisando los planes con cada nuevo análisis de riesgo efectuado.

Este plan de contingencia podría a su vez subdividirse en otros subplanes:

- **Plan de Respaldo:** Contramedidas preventivas antes de que se materialice una amenaza
- **Plan de Emergencia:** Contramedidas necesarias durante la materialización de las amenazas o justamente después con el objetivo de paliar sus efectos
- **Plan de Recuperación:** Medidas necesarias después de materializada la amenaza. La finalidad es restaurar los servicios a su estado original.

Tenido en cuenta lo anterior para aquellos Sistemas de Información que en lo relativo a la dimensión de Disponibilidad presente un nivel ALTO se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:

a) Se identificarán funciones, responsabilidades y actividades a realizar.
b) Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.

d) Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
e) El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Se debe identificar funciones, responsabilidades y actividades a realizar en caso de desastre que impida prestar el servicio en las condiciones habituales y con los medios habituales y en particular:

- Quiénes componen el comité de crisis que toma la decisión de aplicar los planes de continuidad tras analizar el desastre y avaluar las consecuencias.
- Quiénes se encargarán de la comunicación con las partes afectadas en caso de crisis.
- Quiénes se encargan de reconstruir el sistema de información (recuperación de desastre).

Debe existir una previsión de los medios alternativos que se van a conjugar para poder seguir prestando los servicios en caso de no poder hacerse con los medios habituales:

- instalaciones alternativas (ver [op.cont.4])
- comunicaciones alternativas (ver [op.cont.4])
- equipamiento alternativo (ver [op.cont.4])
- personal alternativo (ver [op.cont.4])
- recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto (ver [mp.info.6 REF 1]).

El plan debe determinar la coordinación de todos los elementos para alcanzar la restauración de los servicios en los plazos estipulados.

6.6 Pruebas Periódicas [op.cont.3]

Deberían llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre.

Se deberían probar regularmente los planes de continuidad para garantizar su actualización y eficacia.

En los Sistemas de Información cuya dimensión de Disponibilidad presente un nivel ALTO se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.

Para ello deberá existir un plan de pruebas regular e informes de análisis de las pruebas realizadas, destacando las incidencias propias o en subcontratistas y derivando un plan de mejoras tanto en los medios como en los procedimientos y en la concienciación y formación de las personas implicadas.

7 Responsabilidades

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte de las personas con responsabilidad en la gestión de la seguridad en MUFACE, así como a todos aquellos usuarios con responsabilidad o involucrados en el aseguramiento de la continuidad de las actividades, pudiéndose derivar de su incumplimiento la pertinente responsabilidad en el ámbito disciplinario, si a ello hubiera lugar en aplicación de las disposiciones reguladoras del estatuto jurídico del usuario.

Las responsabilidades asociadas a cada componente de la estructura organizativa para la gestión de la seguridad en MUFACE es la definida en la Norma de Organización de Seguridad y Responsabilidades.

La detección de actuaciones irregulares, ilícitas o ilegales podrá acarrear la iniciación de las medidas disciplinarias oportunas y, en su caso, de las acciones legales correspondientes.

8 Revisión de la norma

La presente norma y cualquier modificación a la misma, entrará en vigor en el momento en que sea aprobada por el *Comité de Seguridad de la Información* de MUFACE, lo que se notificará oportunamente mediante su publicación en la Intranet de MUFACE.

Las modificaciones totales o parciales de la presente normativa, así como la referencia de los documentos o versiones que sustituyen a este documento serán registradas mediante control de cambios y versión del documento.

Anexo I: Referencias

Se deberán tomar en consideración los siguientes textos y normativas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- PSI Política de Seguridad de la Información de MUFACE.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-800: Esquema Nacional de Seguridad - Glosario de Términos y Abreviaturas
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-804: Esquema Nacional de Seguridad. Guía de implantación.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-808: Verificación del Cumplimiento de las Medidas en el ENS.
- UNE-ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la intimidad - Sistemas de gestión de la seguridad de la información. Requisitos.
- ISO 22301:2012: Seguridad de la información – Sistemas de gestión de la continuidad del negocio – Requisitos.
- ISO 24762:2008: Tecnología de la información - Técnicas de seguridad - Directrices para servicios de recuperación de desastres TIC.
- ISO 27031:2011: Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la información y tecnología de las comunicaciones para la continuidad del negocio.
- Magerit versión 3.0: Metodología de Análisis de Gestión de Riesgos de los Sistemas de información.

Las directrices estipuladas en esta norma se fundamentan en los requisitos establecidos en el ENS que se mencionan a continuación.

Medida op.cont.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.

Medida op.cont.2

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:

- Se identificarán funciones, responsabilidades y actividades a realizar.
- 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.
- Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

- Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

- Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Medida op.cont.3

Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Medida op.cont.4

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.

Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.

Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

- El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Medida mp.info.6

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.

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.

Refuerzo R1-Pruebas de recuperación.

- Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

- 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.