NORMA SOBRE RESPONSABILIDAD DE LA INFORMACIÓN Y CRITERIOS PARA SU CALIFICACIÓN

MUFACE

Documentación: MUFACE -Seguridad

Oficina de Seguridad de la Información

Referencia: Seguridad de la Información

Versión del documento 1.0

INDICE

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. Objeto

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.

El objeto de este documento es la adecuada protección de la información según el principio de proporcionalidad, de manera que se realice la gestión de la seguridad en función de los riesgos. Por este motivo, deben establecerse diversos niveles de calificación de la información que permitan aplicar las medidas de protección adecuadas para cada categoría.

La Norma sobre responsabilidad de la información y criterios para su calificación establece las directrices a seguir para llevar a cabo esa calificación.

2. Ámbito de Aplicación

Esta norma aplica a todos los usuarios (tanto de internos como externos) que tengan acceso a los sistemas de información gestionados por MUFACE con responsabilidad en la gestión de la información.

El ámbito de aplicación estricto se refiere a la información manejada por 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.

Tal y como indica el Artículo 2 del ENS, *"sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales"*.

3. Contexto

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

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.
- **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 correspondiente 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 que cada servicio.
- **Activo:** 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.
- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

- **Integridad:** propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Disponibilidad:** Propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Trazabilidad:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- **Calificar:** acto formal mediante el cual se establecen diferentes niveles de información en función de sus exigencias de seguridad.
- **Información Calificada:** Aquella información (en cualquier tipo de soporte, físico o informático) que ha pasado por el procedimiento de calificación y han sido determinados sus requisitos de seguridad.
- **Medidas de seguridad:** Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- **Sistema de Información:** Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **RTO:** Recovery Time Objective. Tiempo máximo que un servicio puede estar interrumpido o una información indisponible.

6. Directrices

Según las funciones atribuidas por la PSI en su Artículo 7 y de conformidad con lo establecido por el Artículo 44 del ENS y por la Norma de Organización de Seguridad y Responsabilidades, corresponde a cada Responsable de la Información la calificación de aquella información sobre la que tenga potestad, estableciendo sus necesidades de seguridad. Podrá contar para ello con el asesoramiento del Responsable del Sistema del Responsable del Servicio y del Responsable de Seguridad.

Se basará para realizar la calificación en los resultados de un análisis de riesgos sobre los activos de información bajo su responsabilidad.

Realizará y mantendrá actualizado al menos anualmente un inventario de todos los activos de información de los que es responsable en el que se indique tanto el nivel de calificación otorgado a cada tipo de información como las medidas mínimas de seguridad requeridas para los mismos en función de su nivel. Seguirá para ello el procedimiento de inventariado de activos de información. El inventario estará a disposición de los usuarios del sistema que deberán observar las medidas indicadas en el manejo de la citada información.

El responsable de la Información deberá revisar periódicamente la calificación de la información y tendrá la potestad de modificar el nivel de seguridad requerido en el momento en que lo considere necesario. Se deberá conservar en el inventario mencionado un histórico de cambios en el nivel de seguridad de cada tipo de información, conteniendo al menos la fecha, la motivación y la persona responsable de la realización del cambio en la definición del nivel de seguridad.

Seguirá para las tareas mencionadas el procedimiento de calificación de la información, que desarrollará la manera de calificarla según los criterios determinados por la presente norma y definirá cómo debe realizarse la aprobación formal de la misma.

El Responsable de la información deberá además determinar la periodicidad de realización de copias de respaldo y el periodo de retención de las mismas, que se reflejarán en la Política de Backup de la organización. La realización de las citadas copias de respaldo se llevará a cabo de acuerdo con lo explicitado en la Norma de retención de la información y de la realización y almacenamiento de salvaguardas de información (backups) y en sus procedimientos derivados.

Por otra parte, el Responsable de la Información se asegurará de que los soportes conteniendo la información estén correctamente etiquetados según su calificación. En el caso de contener información con distintos niveles de calificación se etiquetará según el más alto. Se seguirá el procedimiento de etiquetado de soportes de información que detalle la forma en que debe llevarse a cabo en función de su nivel de seguridad.

El responsable del Sistema implementará al menos las medidas de seguridad definidas por el Responsable de la Información. Contará para ello con un Procedimiento de protección y tratamiento de la información, que precisará cómo se han de realizar aspectos como control de acceso, almacenamiento y custodia, realización de copias de seguridad,

transmisión de información, etc., de acuerdo con lo explicitado en las normas correspondientes y sus procedimientos de desarrollo.

7. Criterios de calificación de la información

Se deben considerar para calificar la información los distintos criterios detallados en el presente capítulo.

7.1 Calificación frente al ENS

El ENS establece que la determinación de la categoría de cada activo ha de realizarse sobre la base del impacto que tendría un incidente que afectara a la seguridad en las siguientes dimensiones, enunciadas en el anexo I del ENS: autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad.

Según establece el anexo I del ENS, una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada y no se ocasiona por tanto perjuicio alguno, no se adscribirá a ningún nivel.

Se valorarán los activos de tipo información, en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad. En el Anexo I del ENS y en la guía CCN-STIC-803 del Centro Criptológico Nacional se detallan los criterios de apoyo que se recogen en el ANEXO II: de este documento para proceder a la valoración en las dimensiones de cada activo de información detectado. Se aplicarán dichos criterios para calificar la información contemplada en el ámbito de aplicación de la presente Norma.

Se adjunta a continuación una tabla resumen de los mismos:

DIMENSIÓN			VALORES

	El nivel de seguridad se establecerá en función de las consecuencias que tendría ...	Impacto, ¿qué pasa si...?	SIN VALORAR	BAJO	MEDIO	ALTO
CONFIDENCIALIDAD	... su revelación a personas no autorizadas o que no necesitan conocer la información.	¿Qué sucede si la información cae en manos de personas no autorizadas?	Información de carácter público o cuya revelación no causa perjuicio alguno.	No debe ser conocida fuera de la organización.	Solo debe ser conocida por las personas que la necesiten para su trabajo. Su revelación causaría perjuicios graves de imagen, legales, etc.	Debe ser conocida solo por un número limitado de personas. Su revelación causaría perjuicios muy graves de imagen, legales, etc.
INTEGRIDAD	... su modificación por alguien que no está autorizado a modificar la información.	¿Qué impacto tendría que la Información sea modificad a por alguien no autorizado?	Errores en la información carecen de consecuencias.	Causarían algún inconveniente (retrasos leves o modificación de los resultados con poca repercusión).	Causarían un perjuicio grave, aunque subsanable (acciones correctoras costosas).	Causarían un daño muy grave de imposible o muy difícil recuperación.
AUTENTICIDAD	... el hecho de que la información no fuera auténtica.	¿Qué pasa si no puedo garantizar la identidad del origen y/o destino de la información?	La falsedad en el origen y destino es irrelevante (anonimato).	La falsedad en el origen y destino causaría perjuicio limitado, pudiendo ser subsanable.	La falsedad en el origen y destino causaría daños significativos y de difícil recuperación.	La falsedad en el origen y destino causaría daños muy graves, irreparables.

TRAZABILIDAD	… el no poder rastrear a posteriori quién ha accedido a, o modificado una cierta información.	¿Qué conlleva que el tratamiento de la información (acceso, modificación, borrado) no pueda ser verificado (trazado)?	Es irrelevante conocer la autoría de las actuaciones sobre la información.	La pérdida de trazabilidad dificultaría la subsanación de problemas y dificultaría la persecución de delitos, causando un perjuicio limitado.	La pérdida de trazabilidad dificultaría notablemente la subsanación de problemas o la persecución de delitos, provocando un perjuicio grave.	La pérdida de trazabilidad facilitaría enormemente la comisión de delitos graves, ocasionando un perjuicio muy grave, de difícil o imposible reparación.
DISPONIBILIDAD	… el hecho de que no se pudiera acceder a la información.	¿Qué sucede si no se puede acceder a la información?	Se puede prescindir de esta información durante más de una semana.	Causaría el incumplimiento leve de alguna norma o protestas individuales.	Supondría el incumplimiento material o formal de una norma y podría provocar alteración del orden público.	Causaría un grave daño de difícil o imposible reparación, un incumplimiento grave de una norma o un enorme daño reputacional.

7.2. Calificación frente a la normativa específica según la naturaleza de la información

El Responsable de la Información deberá identificar la naturaleza de la información que maneja y deberá considerar para su calificación la Normativa específica que le es de aplicación. Se recogerá en el inventario información sobre la Normativa de aplicación.

Determinará en función de esto los requisitos de seguridad que sea necesario aplicar de manera adicional a los incluidos en los apartados anteriores.

De igual manera, definirá cualesquiera otras necesidades de seguridad específicas que puedan requerirse por motivos de servicio u operacionales.

8. Responsabilidades

El contenido de esta norma es de obligado conocimiento y cumplimiento por parte de las personas con responsabilidad en la gestión de la información en MUFACE, 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.

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.

9. 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.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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-803: Esquema Nacional de Seguridad. Valoración de los Sistemas.
- 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.
- Centro Criptológico Nacional. Guía de Seguridad CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC.

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

9.1 Medida mp.info.1 – Datos de carácter personal

Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del

mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

9.2 Medida mp.info.2 – Calificación de la información

- Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
- El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

9.4 Artículo 40 del ENS (RD 311/202). Categorías de seguridad

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.
2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I

9.5 Artículo 41 del ENS (RD 311/2022). Facultades

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

9.6 Los Responsables de la Información.

Conforme a los artículos 10 y 44 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS), el Responsable de la Información es 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 su seguridad. Tiene, además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (anexo II.5.7.2 del ENS).

Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione el procedimiento o trámite.

Son funciones de cada Responsable de Información, dentro de su ámbito de actuación, las siguientes:

a. Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 44 del ENS).
b. Son los encargados, junto a los Responsables del Servicio y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.
c. Son los responsables, junto a los Responsables del Servicio, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

10 ANEXO II: Criterios para la valoración en las dimensiones de cada activo de información

10.1 Criterios del apartado 3 del anexo I (Categorías de los sistemas) del ENS: Determinación del nivel requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.

2º Causar un daño menor en los activos de la organización.

3º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.

5º Otros de naturaleza análoga.

Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.

2º Causar un daño significativo en los activos de la organización.

3º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5º Otros de naturaleza análoga.

Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3º El incumplimiento grave de alguna ley o regulación.
4º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

10.2 Criterios de la Guía CCN-STIC-403

A continuación, se detallan los criterios de valoración especificados por la guía CCN-STIC-803 del CCN, que deberán utilizarse como referencia.

10.2.1 Criterios generales para valorar la Confidencialidad necesaria

[C=A] Nivel ALTO

- porque la información debe conocerla un número muy reducido de personas.
- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque su revelación causaría un grave daño, de difícil o imposible reparación.
- porque su revelación supondría el incumplimiento grave de una norma.
- porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas.
- porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones.

- porque su revelación podría desembocar en protestas masivas (alteración sería del orden público).

[C=M] Nivel MEDIO

- porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita
- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque su revelación causaría un daño importante, aunque subsanable.
- porque su revelación supondría el incumplimiento material o formal de una norma.
- porque su revelación causaría pérdidas económicas importantes.
- porque su revelación causaría un daño reputacional importante con los ciudadanos con otras organizaciones.
- porque su revelación podría desembocar en protestas públicas (alteración del orden público).

[C=B] Nivel BAJO

- porque la información no deben conocerla personas ajenas a la organización.
- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque su revelación causaría algún perjuicio.
- porque su revelación supondría el incumplimiento leve de una norma.
- porque su revelación supondría pérdidas económicas apreciables.
- porque su revelación causaría un daño reputacional apreciable con los ciudadanos con otras organizaciones.
- porque su revelación podría desembocar en múltiples protestas individuales.

Sin valorar

- información de carácter público, accesible por cualquier persona.

10.2.2 Criterios generales para valorar la Integridad necesaria

[I=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...

- porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación.
- porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas.
- porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones.
- porque su manipulación o alteración no autorizada podría desembocar en protestas masivas (alteración sería del orden público).

[I=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento…
- porque su manipulación o modificación no autorizada causaría un daño importante, aunque subsanable.
- porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma.
- porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes.
- porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones.
- porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público).

[I=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento…
- porque su manipulación o modificación no autorizada causaría algún perjuicio.
- porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma.
- porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables.
- porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones.
- porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales.

Sin valorar

- cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables.

10.2.3 Criterios generales para valorar la Autenticidad necesaria

[A=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento…
- porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación.
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
- porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones.
- porque la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración sería del orden público)

[A=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento…
- porque la falsedad en su origen o en su destinatario causaría un daño importante, aunque subsanable
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes.
- porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones
- porque la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público).

[A=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento…
- porque la falsedad en su origen o en su destinatario causaría algún perjuicio.
- porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables.

- porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones.
- porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales.

Sin valorar

- cuando el origen es irrelevante o ampliamente conocido por otros medios.
- cuando el destinatario es irrelevante, por ejemplo, por tratarse de información de difusión anónima.

10.2.4 Criterios generales para valorar la Trazabilidad necesaria

[T=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave.
- porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos.
- porque la incapacidad para rastrear un acceso a la información facilitaría enormemente la comisión de delitos graves.

[T=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante.
- porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos.
- porque la incapacidad para rastrear un acceso a la información facilitaría la comisión de delitos.

[T=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...

- porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores.
- porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos.

Sin valorar

- cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios.
- cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios.

10.2.5 Criterios generales para valorar la Disponibilidad necesaria

Los requisitos de disponibilidad de la información derivan de su uso o necesidad de ser utilizada.

Uno de los criterios que son útiles para determinar los requisitos de disponibilidad de un servicio es el establecimiento de un tiempo de interrupción de referencia, que a menudo se conoce como RTO, y mide el tiempo máximo que el servicio puede permanecer interrumpido. La valoración de la disponibilidad mide las consecuencias en caso de que ese tiempo se supere; es decir, que quedemos fuera de servicio por un periodo superior al RTO establecido.

[D=A] Nivel ALTO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible reparación.
- porque la indisponibilidad de la información supondría el incumplimiento grave de una norma.
- porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones.
- porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración sería del orden público).
- cuando el RTO es inferior a 4 horas.

[D=M] Nivel MEDIO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque la indisponibilidad de la información causaría un daño importante, aunque Subsanable.
- porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma.
- porque la indisponibilidad de la información causaría un daño reputacional importante con los ciudadanos o con otras organizaciones.
- porque la indisponibilidad de la información podría desembocar en protestas públicas (alteración del orden público).
- cuando el RTO se sitúa entre 4 y 24 horas (un día).

[D=B] Nivel BAJO

- por disposición legal o administrativa: ley, decreto, orden, reglamento...
- porque la indisponibilidad de la información causaría algún perjuicio.
- porque la indisponibilidad de la información supondría el incumplimiento leve de una norma.
- porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones.
- porque la indisponibilidad de la información podría desembocar en múltiples protestas individuales.
- cuando el RTO se sitúa entre 1 y 5 días (una semana).

Sin valorar

- cuando la información es prescindible por tiempo indefinido.
- cuando el RTO es superior a 5 días laborables (una semana).