IMC_02 - Diccionario de Indicadores para Mejora de la Ciberresiliencia (IMC)

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
incibe cert_

Mayo 2020

imc_02_diccionario-indicadores.pdf versión 1.2

Índice

Índice de tablas

1. Objeto del documento

Este diccionario describe los indicadores para la mejora de la ciberresiliencia (IMC) en organizaciones y empresas de sectores industriales e infraestructuras críticas industriales con respecto a ámbitos de IT *(Information Technology)* y OT *(Operation Technology)*.

Estos indicadores se pueden usar para definir consultas de madurez —para cada empresa, sector o grupo de empresas— con las que determinar los niveles de resiliencia (para los objetivos: Anticipar, Resistir, Recuperar y Evolucionar) correspondientes a la provisión de sus servicios esenciales.

Los distintos indicadores se valoran siguiendo los criterios indicados en la metodología de evaluación descrita en el documento: IMC_01 - Metodología de evaluación de Indicadores para Mejora de la Ciberresiliencia.

2. Indicadores

En esta sección se describen, en tablas independientes, cada uno de los Indicadores para Mejora de la Ciberresiliencia.

Los indicadores se identifican con un código (X-XX-OEN-NN) formado por:

- X: una letra que se corresponde con la inicial de la meta según la metodología.
- XX: dos letras que indican el dominio funcional según la metodología.
- OEN: el literal OE seguido de un número que identifica cada uno de los objetivos específicos.
- NN: un número que identifica cada métrica.

Para la definición de «servicio esencial[1]», se toma como referente la **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Cada tabla incluye los siguientes campos: identificación, caracterización, obtención y análisis.

El campo de **identificación** contiene los siguientes subcampos:

- el código del indicador, según lo descrito anteriormente;
- la meta a la que pertenece;
- el dominio funcional en el que se evalúa;
- el objetivo del indicador;
- la descripción del indicador;
- la pregunta planteada y
- el subcampo de correlación que incluye las guías, estándares y normas en las que se basa cada indicador.

El campo de **caracterización** establece y describe la **escala** de niveles con los que la organización identifica su estado para cada indicador: L0, L1, L2, L3, L4 o L5.

En el campo de **obtención** se detalla el **método de recogida** de la información para el indicador y el **responsable** encargado de realizarla.

Finalmente, la tabla incluye el campo de **análisis**, con dos subcampos:

- medida objetivo: donde se establece el nivel óptimo que la organización debe alcanzar.
- indicador con dos elementos: valores positivos y acciones correctivas. En el primero, se indica la justificación con la que la organización podrá considerarse en un nivel alto. En el segundo, se recogen las medidas a tomar por la organización para aumentar el nivel dentro de la escala con respecto al indicador.

[1] Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

2.1. Anticipar

A continuación, se detallan las fichas para las métricas correspondientes a la meta de Anticipar.

2.1.1. Política de ciberseguridad (PC)

El objetivo general de este dominio funcional es disponer de una política de Ciberseguridad que establezca los requisitos de Ciberresiliencia, contemple los riesgos de Ciberseguridad, asigne responsabilidades y sea comunicada a toda la organización. Sus objetivos específicos son:

- Establecer y comunicar a toda la organización su misión, objetivos y actividades prioritarias.
- Establecer responsabilidades en materia de Ciberseguridad.
- Identificar las funciones críticas de la organización y establecer los requisitos de Ciberresiliencia.
- Disponer de una estrategia de continuidad y recuperación.
- Colaborar con otros organismos en materia de Ciberseguridad.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-PC-OG1-01**
Meta	ANTICIPAR
Dominio Funcional	POLÍTICA DE CIBERSEGURIDAD
Objetivo del indicador	Establecer, actualizar y mantener una política de Ciberseguridad.
Descripción	Establecer las reglas formales a las que los activos de la organización (empleados, procesos y tecnología) deben someterse, en materia de seguridad de la información. Dicha política debe estar aprobada por la Dirección.
Pregunta planteada	¿Se ha establecido alguna política de ciberseguridad dentro de la organización?
Correlación	ISO/IEC 27001:2017 [A.5.1], [A.6.1.3] NIST SP 800-53 R4 [PL-1] ENS [Artículo 12] y Anexo II sección 3.1 Guía contenidos mínimos PSO (2.1, 4.2.1) NIS (Art.15)
CARACTERIZACIÓN	
Escala	**L0 -** No se ha establecido ninguna política de ciberseguridad.

	L1 - Se ha iniciado el establecimiento de una política de ciberseguridad. **L2 -** Se ha establecido una política, pero no es formal (no se ha documentado ni ha sido aprobada por la Dirección). **L3 -** Se ha documentado una política de Ciberseguridad que ha sido aprobada por la Dirección y se mantiene actualizada. **L4 -** Se gestiona, actualiza y mantiene la política de Ciberseguridad regularmente. **L5 -** Se aplican acciones que permiten medir el nivel de cumplimiento de la política de Ciberseguridad.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha establecido una política de ciberseguridad que permite proteger los activos de información de manera correcta.
	Acciones correctivas	Establecer, formalizar y revisar la política de Ciberseguridad, para garantizar la correcta adaptación al contexto de la organización, mientras se arbitran elementos para medir su nivel de cumplimiento (por ejemplo, a través de auditorías de seguridad).

Tabla 1 - Métrica A-PC-OG1-01: Establecer, actualizar y mantener una política de Ciberseguridad.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-PC-OE3-02**
Meta	ANTICIPAR
Dominio Funcional	POLÍTICA DE CIBERSEGURIDAD
Objetivo del indicador	Establecer los requisitos de Ciberresiliencia para soportar los servicios esenciales.
Descripción	Se establecen los requisitos de ciberresiliencia para el servicio esencial identificado como de más alto impacto. Se trata de conocer en qué medida se concibe la ciberresiliencia como algo diferente y específico dentro de la ciberseguridad. Para medir la ciberresiliencia se ha de identificar al menos un servicio esencial crítico. Este indicador mide el grado de compromiso de la organización con la definición de los objetivos específicos de ciberresiliencia (para el servicio esencial identificado como de mayor impacto) y los requisitos para cumplirlos. En el caso de que haya varios servicios esenciales identificados se podrá hacer una encuesta por cada uno de ellos. También se podrán hacer encuestas diferentes para los ámbitos de OT e IT. Si el servicio esencial pertenece al ámbito OT, los requisitos de ciberresiliencia deben incluir por ejemplo, proteger los accesos remotos desde Internet a elementos como PLC, HMI, RTU, etc. que soportan el servicio esencial.
Pregunta planteada	¿Se han establecido los requisitos de ciberresiliencia para un servicio esencial (eligiendo aquel cuya interrupción o alteración ocasione mayor impacto)?
Correlación	ISO/IEC 27001: 2013 [A.5.1.1], [A.14.1.1] NIST SP 800-53 R4 [PM-7], [SA-2], [SA-13] ENS [org.1] [Artículo 11] Guía contenidos mínimos PSO (3.1,3.3) NIS (Directivas 2, 24)
CARACTERIZACIÓN	

Escala	**L0 -** No se han establecido requisitos de ciberresiliencia. **L1 -** Se ha iniciado la identificación de requisitos de ciberresiliencia. **L2 -** Se han establecido requisitos de ciberresiliencia, pero no se han documentado. **L3 -** Se han documentado los requisitos de ciberresiliencia y se mantienen actualizados. **L4 -** Se gestionan, actualizan y verifican los requisitos de ciberresiliencia. **L5 -** Se aplican acciones de mejora en la definición de requisitos de ciberresiliencia.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha identificado y documentado los requisitos de ciberresiliencia para el servicio esencial identificado, que dichos requisitos son exactos y que están actualizados. Estos requisitos deben permitir gestionar los riesgos, gestionar las vulnerabilidades, gestionar los incidentes, gestionar la continuidad del servicio y gestionar las configuraciones y los cambios, reduciendo el impacto o alteración de los servicios esenciales identificados.
	Acciones correctivas	• Identificar, documentar y revisar los requisitos de ciberresiliencia del servicio esencial identificado. • Actualizar la documentación asociada a la política de ciberseguridad.

Tabla 2 - Métrica A-PC-OE3-02: Establecer los requisitos de Ciberresiliencia para soportar los servicios esenciales.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-PC-OE5-01**
Meta	ANTICIPAR
Dominio Funcional	POLÍTICA DE CIBERSEGURIDAD
Objetivo del indicador	Colaborar con entidades públicas o privadas en materia de ciberresiliencia.
Descripción	Establecer acuerdos formales de ayuda mutua, cooperación o intercambio de información con entidades públicas o privadas en materia de ciberresiliencia como, por ejemplo, centros de respuesta a incidentes o CERT, Incibe-CERT, compañías de consultoría en ciberseguridad, proveedores y otras empresas del sector. Por formal se entiende plasmado en un documento aprobado por la Dirección.
Pregunta planteada	¿Se ha establecido algún acuerdo formal de ayuda mutua, cooperación o intercambio de información con otras entidades públicas o privadas en materia de ciberresiliencia?
Correlación	ISO/IEC 27001:2017 [A.5.1.1], [A.6.1.3 y A 6.1.4] NIST SP 800-53 R4 [PM-7], [AT-5], [PM-15] ENS [org.1] NIS (Directiva 24, 35, 47,59, 62, 67, Artículo 8, punto 7, Artículo 13) Guía contenidos mínimos PSO (2.2.4)
CARACTERIZACIÓN	
Escala	**L0 -** No se ha establecido ningún acuerdo de ayuda mutua, cooperación o intercambio de información con entidades públicas o privadas. **L1 -** Se ha iniciado el establecimiento de acuerdos de ayuda mutua, cooperación o intercambio de información mutua con entidades públicas o privadas. **L2 -** Se han establecido acuerdos con entidades públicas o privadas, pero no son formales (no se han documentado ni han sido aprobados por la Dirección). **L3 -** Se han documentado los acuerdos establecidos con entidades públicas o privadas, han sido aprobados por la Dirección y se mantienen actualizado. **L4 -** Se gestionan, actualizan y verifican los acuerdos formalmente establecidos. **L5 -** Se aplican acciones de mejora en los acuerdos formalmente establecidos con entidades públicas o privadas.
OBTENCIÓN	
Método de recogida	Manual

Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha establecido y actualiza con regularidad acuerdos de ayuda mutua, colaboración o intercambio de información de ciberresiliencia con entidades privadas o públicas, para garantizar la colaboración o el soporte de entidades externas, si fuera necesario, en caso de un ciberataque que pueda producir indisponibilidad de los servicios esenciales. Este intercambio de información mejora la anticipación en la gestión de incidentes, la gestión de vulnerabilidades y la continuidad del servicio esencial.
	Acciones correctivas	Establecer, formalizar y revisar acuerdos de ayuda mutua, cooperación o intercambio de información con entidades privadas o públicas, para garantizar la colaboración mutua en caso de un ciberataque.

Tabla 3 - Métrica A-PC-OE5-01: Colaborar con entidades públicas o privadas en materia de ciberresiliencia.

2.1.2. Gestión de riesgos (GR)

El objetivo general de este dominio funcional es identificar, documentar y gestionar los riesgos de los activos durante su ciclo de vida, para garantizar la productividad mantenida de los servicios esenciales.

Sus objetivos específicos son:

- Identificar, documentar y gestionar los activos durante su ciclo de vida, para garantizar la productividad mantenida de los servicios esenciales.
- Establecer, implementar y mantener un proceso formal y documentado de análisis de impacto (BIA).
- Desarrollar una estrategia para identificar, analizar y mitigar los riesgos.
- Identificar los riesgos y niveles de tolerancia al riesgo.
- Analizar los riesgos y asignarles un mecanismo de tratamiento.
- Controlar los riesgos sobre activos y servicios.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OE1-03**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Establecer, implementar y mantener un proceso formal y documentado de análisis de impacto (*BIA*) sobre los procesos y actividades que soportan el servicio esencial.
Descripción	Identificar el impacto en la provisión del servicio esencial de la interrupción o alteración de sus procesos y actividades valorando cuáles de ellos son más críticos. Se trata de conocer si se lleva a cabo un análisis de impacto (*BIA*) sobre el servicio esencial, que analice las consecuencias de una interrupción en la provisión o alteración del mismo, con el fin de identificar cuáles son los procesos y actividades críticos que soportan este servicio para priorizar su recuperación. Se debe asegurar que se prioriza el tratamiento de los riesgos de acuerdo con su criticidad para la organización o para la sociedad (personas afectadas e impacto económico, medioambiental, público y social).
Pregunta planteada	¿Se ha identificado el impacto sobre el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan? y, ¿se han valorado cuáles de dichos procesos y actividades resultan más críticos en función de este impacto?
Correlación	ISO/IEC 31000: 2018 NIST SP 800-53 R4 [RA-2], [RA-3], [PM-9], [PM-11], [SA-14]

	ENS [op.pl.1] Guía contenidos mínimos PSO (4.1, 4.4) Guía contenidos mínimos PPE (4.2, 4.3) NIS (Artículo 15-2,3)	
CARACTERIZACIÓN		
Escala	**L0** - No se ha iniciado el análisis de impacto sobre el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan. **L1** - Se ha iniciado el análisis de impacto en el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan. **L2** - Se ha establecido el análisis del impacto en la provisión del servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan valorando cuáles de ellos son más críticos, pero no se ha documentado. **L3** - Se han documentado el análisis de impacto en el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el análisis de impacto en el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan. **L5** - Se aplican acciones de mejora en el análisis de impacto en el servicio esencial de la interrupción o alteración de los procesos y actividades que lo soportan.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha identificado y priorizado los posibles impactos de la interrupción o alteración de los procesos y actividades que soportan el servicio esencial, es decir, ha implementado un análisis de impacto (*BIA*) para este servicio.
	Acciones correctivas	• Identificar el posible impacto que causaría una interrupción de los distintos procesos y actividades que soportan los servicios esenciales. • Categorizar dichos impactos para priorizar su tratamiento.

Tabla 4 - Métrica A-GR-OE1-03: Establecer, implementar y mantener un proceso formal y documentado de análisis de impacto (BIA) para el servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OE1-04**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Estimar el Tiempo Máximo Tolerable de caída (MTD) o tiempo que puede estar caído un servicio esencial antes de que se produzcan efectos no aceptables.
Descripción	Este es un parámetro de negocio que indica el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable. Este dato es generalmente subjetivo pero puede apoyarse en indicadores cuantitativos de impacto en el negocio (clientes no atendidos, disminución de las ventas,…) de la interrupción. Como criterio de estimación de estos valores pueden utilizarse procedimientos internos, guías y estándares de referencia o factores cualitativos basados en la intuición.
Pregunta planteada	¿Se ha estimado el tiempo máximo aceptable de duración de una interrupción o alteración del servicio esencial?
Correlación	ISO/IEC 31000:2018 NIST SP 800-53 R4 [RA-2], [RA-3], [PM-9], [PM-11], [SA-14] ENS [op.pl.1] Guía contenidos mínimos PPE (4.2) NIS (Directivas 27, 33)
CARACTERIZACIÓN	
Escala	**L0 -** No se ha estimado el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable. **L1 -** Se ha iniciado la estimación del máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable. **L2 -** Se ha determinado cómo estimar el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable, pero no se ha documentado. **L3 -** Se ha documentado el procedimiento para estimar el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable y se mantiene actualizado. **L4 -** Se gestiona, actualiza y verifica el procedimiento para estimar el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable.

	L5 - Se aplican acciones de mejora en el procedimiento para estimar el máximo tiempo de duración de una interrupción o alteración de la provisión del servicio esencial que se considera tolerable.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha estimado el máximo periodo tolerable de una interrupción para el servicio esencial. Esta estimación está basada en un criterio objetivo y se revisa periódicamente.
	Acciones correctivas	• Establecer criterios y procedimientos para estimar los periodos máximos tolerables de interrupción para cada proceso y actividad que soporte el servicio esencial para el cual estamos haciendo la encuesta. • Documentar, revisar y gestionar el procedimiento para estimar tiempo máximo tolerable de interrupción para el servicio esencial.

Tabla 5 - Métrica A-GR-OE1-04: Estimar el Tiempo Máximo Tolerable de caída (MTD) o tiempo que puede estar caído un servicio esencial antes de que se produzcan efectos no aceptables.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OG1-03**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Existe un procedimiento específico para implementar las actividades de gestión de riesgos.
Descripción	La gestión de los riesgos se constituye como uno de los pilares para conocer de manera detallada el servicio esencial y su funcionamiento interno, así como las consecuencias para la organización de una eventual interrupción del mismo. El procedimiento de gestión de riesgos debería girar en torno a los siguientes elementos: • Inventario de activos. • Conjunto de amenazas a las que está expuesto cada activo. • Conjunto de vulnerabilidades asociadas a cada activo. • Conjunto de medidas de seguridad implantadas. Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos y permite priorizar sobre qué riesgos se aplicarán los controles correspondientes.
Pregunta planteada	¿Se han establecido procedimientos para gestionar el riesgo asociado al servicio esencial?
Correlación	ISO/IEC 27005:2018 ISO/IEC 31000:2018 NIST SP 800-53 R4 [RA-2], [RA-3], [PM-9], [PM-11], [SA-14] ENS [op.pl.1] Guía contenidos mínimos PPE (4.2) NIS (Directiva 69)
CARACTERIZACIÓN	

Escala	**L0 -** No se realiza la gestión del riesgo relativa a la provisión del servicio esencial. **L1 -** Se ha iniciado la gestión del riesgo relativa a la provisión del servicio esencial. **L2 -** Se ha establecido la gestión del riesgo relativa a la provisión del servicio esencial pero no se han documentado. **L3 -** Se ha documentado la gestión del riesgo relativa a la provisión del servicio esencial y se mantiene actualizada. **L4 -** Se gestiona, actualiza y verifica la gestión del riesgo relativa a la provisión del servicio esencial. **L5 -** Se aplican acciones de mejora en la gestión del riesgo relativa a la provisión del servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización gestiona el riesgo relativo a la provisión del servicio esencial como un proceso de mejora continua.
	Acciones correctivas	Establecer un procedimiento de gestión del riesgos relativos a la provisión del servicio esencial basado en referencias como CCN-STIC 882 de Análisis de Riesgos para Entidades Locales, o el Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB) de INCIBE-CERT

Tabla 6 - Métrica A-GR-OG1-03: Establecer, implementar y mantener un procedimiento específico para implementar las actividades de gestión de riesgos.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OE5-03**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Establecer e implementar un plan de mitigación de riesgos del servicio esencial.
Descripción	Es importante entender que el objetivo de mitigación de riesgos es reducir la exposición al riesgo del servicio esencial con la intención de llevarlo a los límites de los umbrales aceptables definidos en cada organización. Se trata de documentar los controles, acciones o iniciativas de seguridad de corto, medio y largo plazo que necesitan ser implantadas con el fin de mitigar los riesgos al cual se encuentra expuesto el servicio esencial. Si el servicio esencial pertenece al ámbito OT, se trata de tener en cuenta los umbrales para los riesgos sobre activos relacionados con las infraestructuras OT, por ejemplo los controles para hacer frente a la dificultad de modificar configuraciones por defecto o la falta de cifrado y otros riesgo inherentes residuales de los sistemas SCADA.
Pregunta planteada	¿Se ha establecido e implementado un plan de mitigación de riesgos del servicio esencial?
Correlación	ISO/IEC 31000:2018 NIST SP 800-53 R4 [RA-2], [RA-3], [PM-9], [PM-11], [SA-14] ENS [op.pl.1] Guía contenidos mínimos PSO (4.1, 4.4) NIS (Directivas 49, 57)
CARACTERIZACIÓN	

Escala	**L0 -** No se ha establecido ni implementado un plan de mitigación de riesgos del servicio esencial. **L1 -** Se ha iniciado el establecimiento e implementación de un plan de mitigación de riesgos del servicio esencial. **L2 -** Se ha establecido e implementado un plan de mitigación de riesgos del servicio esencial, pero no se ha documentado. **L3 -** Se ha documentado el establecimiento e implementación de un plan de mitigación de riesgos del servicio esencial. Esta información se mantiene actualizada. **L4 -** Se gestiona, actualiza y verifica el establecimiento e implementación de un plan de mitigación de riesgos del servicio esencial. **L5 -** Se aplican acciones de mejora en el establecimiento e implementación de un plan de mitigación de riesgos del servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha definido e implementado el plan de mitigación de riesgos del servicio esencial para evitar que el riesgo exceda su umbral de tolerancia.
	Acciones correctivas	• Establecer e implementar un plan de mitigación de riesgos del servicio esencial. • Documentar, gestionar y actualizar los umbrales de tolerancia al riesgo para el servicio esencial para el cual estamos haciendo la encuesta.

Tabla 7 - Métrica A-GR-OE5-03: Establecer e implementar un plan de mitigación de riesgos del servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OE6-01**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Elaborar, documentar y mantener un inventario de los activos que soportan el servicio esencial.
Descripción	El inventario de activos conforma el primer elemento de la cadena en un sistema de gestión de la seguridad. Un inventario de activos incluye: • las personas que operan y monitorizan los servicios; • la información que alimenta y es producida por los servicios; • la tecnología que soporta los servicios; • las instalaciones en las que se llevan a cabo los servicios. En definitiva, todos aquellos elementos que tengan valor para la organización y la provisión de su servicio esencial, y por consiguiente necesiten ser protegidos de potenciales riesgos. Para cada activo se registrará ubicación, proceso o procesos en los que interviene, coste de su reposición y responsable. El objetivo de realizar este inventario es identificar las amenazas sobre estos activos y sus vulnerabilidades, para así poder analizar y gestionar los riesgos que podrían derivarse para el servicio esencial que soportan.
Pregunta planteada	¿Se elabora, documenta y mantiene un inventario de los activos que soportan directamente el servicio esencial?
Correlación	UNE-ISO/IEC 27001:2017 [A.8.1.1] NIST SP 800-53 R4 [CM-8] ENS [op.exp.1] Guía contenidos mínimos PSO (3.2 y 4.2) Guía contenidos mínimos PPO (3.2) NIS (Directivas 44, 46)
CARACTERIZACIÓN	

Escala	**L0** - No se realiza el inventario de los activos que soportan el servicio esencial. **L1** - Se ha iniciado la elaboración del inventario de los activos que soportan el servicio esencial, pero es incompleto. **L2** - Se ha elaborado el inventario de los activos que soportan el servicio esencial, pero no se documenta el proceso. **L3** - Se ha elaborado y documentado el proceso para realizar el inventario de los activos que soportan el servicio esencial. **L4** - Se revisa periódicamente el inventariado de los activos que soportan el servicio esencial. **L5** - Se aplican acciones de mejora sobre el proceso para realizar el inventario de los activos que soportan el servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha elaborado, documentado y mantiene un inventariado de los activos críticos para la provisión del servicio esencial.
	Acciones correctivas	Elaborar, documentar y revisar periódicamente un proceso de inventariado de activos que permita mantener actualizada la información de los activos que soportan el servicio esencial entre otra: nombre, descripción, identificador, código, tipo, propietario, responsable, ubicación y valoración del activo.

Tabla 8 - Métrica A-GR-OE6-01: Elaborar, documentar y mantener un inventario de los activos que soportan el servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-GR-OE6-02**
Meta	ANTICIPAR
Dominio Funcional	GESTIÓN DE RIESGOS
Objetivo del indicador	Realizar copias de seguridad y conservar los activos de información de clasificación más sensible.
Descripción	Una copia de seguridad o *backup* es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe; restaurar datos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica, etc. Permitiendo el traslado a ubicaciones distintas de la de los datos originales.
Pregunta planteada	¿Se realizan copias de seguridad y se conservan los activos de información de clasificación más sensible?
Correlación	ISO/IEC 27001: 2013 [A.12.3.1] NIST SP 800-53 R4 [CP-9] ENS [mp.info.9] [mp.per.4], [mp.info.2] Artículo 25 Guía contenidos mínimos PPE (4.2.2)
CARACTERIZACIÓN	
Escala	**L0** - No se realizan copias de seguridad de la información de clasificación más sensible ni se aplican procedimientos para su conservación. **L1** - Se ha iniciado la implantación de un proceso de copia de seguridad de la información de clasificación más sensible y la aplicación de procedimientos para su conservación. **L2** - Se ha implementado un proceso de copia de seguridad de la información de clasificación más sensible y se aplican procedimientos para su conservación. **L3** - Se han implementado y documentado un proceso de copia de seguridad de la información de clasificación más sensible y los procedimientos para su conservación. **L4** - Se revisan periódicamente el proceso de copia de seguridad de la información de clasificación más sensible y los procedimientos para su conservación. **L5** - Se aplican acciones de mejora sobre el proceso de copia de seguridad de la información de clasificación más sensible y sobre los procedimientos para su conservación.
OBTENCIÓN	

Método de recogida	Manual Se recomienda la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un proceso mejorado para realizar la copia de seguridad de la información de clasificación más sensible y de los procedimientos para su conservación.
	Acciones correctivas	• En el caso de delegar la copia de seguridad a sistemas *cloud* de terceros, asegurar que cumplan con las políticas de seguridad de la organización para información de clasificación sensible, por ejemplo cifrado de la información y control de acceso. • Documentar los procesos, incluyendo el lugar o ubicación de almacenamiento de las copias de seguridad. • Revisar los procedimientos de conservación para adecuarlos a los distintos soportes de las copias según sus características y las de las copias que albergan. • Comprobar periódicamente que el procedimiento para recuperar las copias de información es útil y efectivo.

Tabla 9 - Métrica A-GR-OE6-02: Realizar copias de seguridad y conservar los activos de información de clasificación más sensible.

2.1.3. Formación en ciberseguridad (FO)

El objetivo general de este dominio funcional es promover el conocimiento y el desarrollo de habilidades y conocimientos de las personas en apoyo de sus funciones en la consecución y el mantenimiento de la ciberresiliencia operacional y la protección. Sus objetivos específicos son:

- Establecer programas de formación en Ciberseguridad.
- Llevar a cabo actividades de formación.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-FO-OG1-03**
Meta	ANTICIPAR
Dominio Funcional	FORMACIÓN EN CIBERSEGURIDAD
Objetivo del indicador	Definir y poner en marcha un procedimiento específico para implementar las actividades de formación.
Descripción	Definir y poner en marcha un plan de formación en ciberresiliencia destinado al personal implicado en el servicio esencial. Se trata de conocer si se promueve el conocimiento y el desarrollo de habilidades entre los usuarios relacionados, directa o indirectamente, con la provisión del servicio esencial, en apoyo a sus funciones para la consecución y el mantenimiento de la ciberresiliencia. El plan de formación podrá contemplar cualquier iniciativa de capacitación o entrenamiento en materia de ciberresiliencia, dirigida a estos usuarios, incluida su participación en ciberejercicios.
Pregunta planteada	¿Se ha definido y puesto en marcha un plan de formación en ciberresiliencia destinado al personal implicado en el servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.7.2.2] NIST SP 800-53 R4 [AT-1], [AT-3], [PM-13], [PM-14] ENS [mp.per.4] Guía contenidos mínimos PSO (2.2.2) NIS (Directivas 36, 38)
CARACTERIZACIÓN	

Escala	**L0 -** No se ha establecido un plan de formación en ciberresiliencia. **L1 -** Se ha iniciado la definición de un plan de formación. **L2 -** Se ha establecido un plan de formación, pero no se han documentado. **L3 -** Se ha documentado un plan de formación y las actividades asociadas. Este plan se mantiene actualizado. **L4 -** Se gestiona y verifica el plan de formación y las actividades asociadas. **L5 -** Se aplican acciones de mejora en el plan de formación y en las actividades asociadas.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización realiza actividades de formación o ciberejercicios orientados a formar y entrenar al personal de la organización en materia de ciberresiliencia. El plan de formación debe dirigirse a los empleados de la organización y, donde sea relevante, a contratistas y usuarios de terceros.

	Acciones correctivas	• Planificar, dedicar recursos, informar al personal y llevar a cabo actividades de formación en ciberresiliencia o ciberejercicios orientados a formar al personal de la organización en esta materia. • Identificar las necesidades y carencias en las capacidades del personal responsable de la ciberseguridad • Evaluar el número de usuarios (internos y externos) que han completado satisfactoriamente las sesiones de formación periódicas de acuerdo a lo establecido en el plan. • Evaluar la efectividad de los planes de formación. • Se actualizan periódicamente estos planes para adecuarlos a los cambios de la plantilla o de los procesos, cuando se incorporan nuevos equipos y tecnologías, y para estar al día de la evolución de las amenazas.

Tabla 10 - Métrica A-FO-OG1-03: Definir y poner en marcha un procedimiento específico para implementar las actividades de formación.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-FO-OE1-02**
Meta	ANTICIPAR
Dominio Funcional	FORMACIÓN EN CIBERSEGURIDAD
Objetivo del indicador	Identificar las necesidades de formación en Ciberseguridad para los servicios esenciales.
Descripción	Para la determinación de las necesidades de formación en Ciberseguridad de la organización, un análisis debe valorar las actividades de los empleados (riesgos a los que están expuestos, competencias que requieren desarrollar en su día a día, certificaciones o normativas que deben alcanzarse o mantenerse para asegurar el correcto funcionamiento del servicio esencial) e integrarlas en los planes formativos corporativos.
Pregunta planteada	¿Se han identificado las necesidades de formación en Ciberseguridad para los servicios esenciales?
Correlación	ISO/IEC 27001:2017 [A.7.2.2] NIST SP 800-53 R4 [AT-1], [AT-3], [PM-13], [PM-14] ENS [mp.per.4] Guía contenidos mínimos PSO (2.2.2) NIS (Directivas 36, 38)
CARACTERIZACIÓN	
Escala	**L0** - No se han identificado las necesidades de formación en Ciberseguridad para los servicios esenciales. **L1** - Se han identificado las necesidades de formación en Ciberseguridad para los servicios esenciales. **L2** - Se han identificado las necesidades de formación en Ciberseguridad para los servicios esenciales, pero no se han documentado. **L3** - Se han documentado las necesidades de formación en Ciberseguridad para los servicios esenciales. Y se mantienen actualizadas. **L4** - Se gestionan y verifican las necesidades de formación en Ciberseguridad para los servicios esenciales. **L5** - Se aplican acciones de mejora en la identificación de las necesidades de formación en Ciberseguridad para los servicios esenciales.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO

ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha identificado las necesidades de formación en Ciberseguridad para los servicios esenciales, y las mantiene en un ciclo de mejora constante.
	Acciones correctivas	• Destinar tiempo y dedicar recursos para identificar las necesidades de formación en Ciberseguridad de la organización. • Actualizar periódicamente las necesidades de formación en Ciberseguridad para adecuarlas al nivel de seguridad necesario, a las nuevas amenazas y a los distintos perfiles profesionales de la empresa.

Tabla 11 - Métrica A-FO-OE1-02: Identificar las necesidades de formación en Ciberseguridad para los servicios esenciales.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**A-FO-OE3-01**
Meta	ANTICIPAR
Dominio Funcional	FORMACIÓN EN CIBERSEGURIDAD
Objetivo del indicador	Llevar a cabo actividades de concienciación en ciberresiliencia.
Descripción	Definir y poner en marcha un plan de concienciación en ciberresiliencia. Se trata de conocer si se promueve una cultura de ciberresiliencia dentro de la organización que alcance a todo el personal. Este plan incorpora cualquier iniciativa de sensibilización en materia de ciberresiliencia.
Pregunta planteada	¿Se ha definido y puesto en marcha un plan de concienciación en ciberresiliencia destinado a todo el personal implicado en el servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.7.2.2] NIST SP 800-53 R4 [AT-1], [PM-16], [AT-2], [PM-15], [PM-16] ENS [mp.per.3] Guía contenidos mínimos PSO (2.2.2) NIS (Directivas 36, 38)
CARACTERIZACIÓN	
Escala	**L0** - No se ha establecido un plan de concienciación en ciberresiliencia. **L1** - Se ha iniciado la definición de un plan de concienciación **L2** - Se ha establecido un plan de concienciación, pero no se ha documentado. **L3** - Se ha documentado un plan de concienciación y las actividades asociadas. Este plan se mantiene actualizado. **L4** - Se gestiona y verifica el plan de concienciación y las actividades de concienciación asociadas. **L5** - Se aplican acciones de mejora en el plan de concienciación y actividades de concienciación asociadas.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO
ANÁLISIS	
Medida Objetivo	L5

Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización realiza actividades de concienciación orientados a sensibilizar al personal de la organización en materia de ciberresiliencia.
	Acciones correctivas	• Incorporar el plan de concienciación como parte de la estrategia de seguridad de la empresa. • Destinar tiempo y dedicar recursos para informar a todo el personal de los riesgos de seguridad que pueden evitar y de los procesos que han de activarse en caso de incidente. Llevar a cabo actividades de concienciación en ciberresiliencia orientados a sensibilizar al personal de la organización en esta materia. • Actualizar periódicamente estos planes para adecuarlos al nivel de seguridad necesario, a las nuevas amenazas y a los distintos perfiles profesionales de la empresa.

Tabla 12 - Métrica A-FO-OE3-01: Llevar a cabo actividades de concienciación en ciberresiliencia.

2.2. Resistir

A continuación, se detallan las fichas para las métricas correspondientes a la meta de Resistir.

2.2.1. Gestión de vulnerabilidades (GV)

El objetivo general de este dominio funcional es identificar, analizar y gestionar las vulnerabilidades en el entorno operativo de un servicio esencial. Sus objetivos específicos son:

- Preparar la realización de las actividades de análisis y resolución de vulnerabilidades.
- Establecer y mantener un proceso de identificación y análisis de vulnerabilidades.
- Gestionar la exposición a vulnerabilidades identificadas.
- Analizar las causas raíz de las vulnerabilidades.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OG1-03**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Elaborar, implementar y mantener un procedimiento específico para la gestión de vulnerabilidades.
Descripción	La gestión de vulnerabilidades es un proceso continuo de cualquier sistema de información que consiste en la identificación, evaluación y corrección de vulnerabilidades en cualquier sistema de la organización, ya sea software o hardware que dan soporte a la provisión del servicio esencial. Va más allá de la evaluación de las vulnerabilidades, ya que categoriza los activos y clasifica las vulnerabilidades según su nivel de riesgo. Si el servicio esencial pertenece a un entorno OT, se trata de gestionar aquellas vulnerabilidades que puedan afectar a los componentes que lo integran (PLC, RTU, HMI, SCADA, Controlador, etc.)
Pregunta planteada	¿Se ha elaborado, implementado y se mantiene un procedimiento específico para gestión de vulnerabilidades dentro de la organización?
Correlación	ISO/IEC 27001:2017 [A.12.6.1] NIST SP 800-53 R4 [CA-8], [RA-5], [SA-11], [SI-2], [SI-3] ENS [op.pl.1] [mp.sw.2] [op.exp.3] Artículo 20
CARACTERIZACIÓN	

Escala	**L0** - No se dispone de ningún procedimiento específico para la gestión de vulnerabilidades. **L1** - Se ha iniciado la definición de un procedimiento específico para la gestión de vulnerabilidades, pero es incompleto y no se ha formalizado. **L2** - Se ha establecido un procedimiento específico para la gestión de vulnerabilidades, está completo pero no se actualiza. **L3** - Se ha documentado un procedimiento específico para la gestión de vulnerabilidades. Este procedimiento se mantiene actualizado. **L4** - Se gestiona y verifica el procedimiento específico para la gestión de vulnerabilidades. **L5** - Se aplican acciones de mejora en el procedimiento específico para la gestión de vulnerabilidades.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores cercanos a L5 indican que la organización realiza una revisión activa del procedimiento específico para implementar la gestión de vulnerabilidades.
	Acciones correctivas	• Identificar y establecer una lista de fuentes de información sobre vulnerabilidades para los activos: fabricantes, CERT, listas de distribución, grupos de noticias, entre ellos. • Establecer en el procedimiento un apartado para el descubrimiento activo de vulnerabilidades, su priorización y evaluación del impacto sobre los activos. • Incorporar al procedimiento actividades de análisis y resolución de vulnerabilidades. • Establecer responsables del procedimiento para la gestión de vulnerabilidades.

Tabla 13 - Métrica T-GV-OG1-03: Elaborar, implementar y mantener un procedimiento específico para la gestión de vulnerabilidades.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE1-02**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Utilizar herramientas o mecanismos de identificación de vulnerabilidades en los activos.
Descripción	Las herramientas o mecanismos de identificación de vulnerabilidades son aplicaciones diseñadas para realizar análisis asistidos o automáticos de los activos tecnológicos de la organización. Aunque estas aplicaciones puedan no ser capaces de detectar la vulnerabilidad con total precisión, sí son capaces de detectar ciertos elementos que podrían desencadenar en una vulnerabilidad, facilitando el trabajo a los investigadores e ingenieros. Se trata de descubrir proactivamente, usando estas herramientas, las vulnerabilidades que afectan a la provisión del servicio esencial, y si se usan regularmente.
Pregunta planteada	¿Se utilizan herramientas o mecanismos de identificación de vulnerabilidades en los activos?
Correlación	ISO/IEC 27001:2017 [A.12.6.1] NIST SP 800-53 R4 [CA-8], [RA-5], [SA-11], [SI-2], [SI-3] ENS [op.pl.1] [mp.sw.2]
CARACTERIZACIÓN	
Escala	**L0** - No se utilizan herramientas o mecanismos de identificación de vulnerabilidades en los activos. **L1** - Se ha iniciado el uso de herramientas o mecanismos de identificación de vulnerabilidades en los activos. **L2** - Se ha establecido un procedimiento para el uso de herramientas o mecanismos de identificación de vulnerabilidades en los activos. **L3** - Se ha documentado el procedimiento y se utilizan herramientas o mecanismos de identificación de vulnerabilidades en los activos. **L4** - Se gestiona, actualiza y verifica el procedimiento de uso de herramientas o mecanismos de identificación de vulnerabilidades en los activos. **L5** - Se aplican acciones de mejora en el procedimiento de uso de herramientas o mecanismos de identificación de vulnerabilidades en los activos.
OBTENCIÓN	
Método de recogida	Manual

Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores cercanos a L5 indican que la organización realiza una revisión activa de las vulnerabilidades que afectan al servicio esencial, a través del uso de un conjunto conocido de herramientas o mecanismos de identificación de vulnerabilidades en los activos.
	Acciones correctivas	• Identificar y establecer una lista de herramientas de análisis de vulnerabilidades. • Documentar y revisar una lista de las herramientas de análisis de vulnerabilidades utilizadas.

Tabla 14 - Métrica T-GV-OE1-02: Utilizar herramientas o mecanismos de identificación de vulnerabilidades en los activos.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE2-04**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Categorizar y priorizar las vulnerabilidades.
Descripción	La categorización de las vulnerabilidades es probablemente el paso más importante en un proceso de gestión de vulnerabilidades y también el paso más difícil y con mayor posibilidad de cometer errores. Durante esta etapa se deben clasificar las diferentes vulnerabilidades identificadas, determinando la probabilidad de explotación y las consecuencias que podrían generar. Así resulta más fácil ordenar su remediación de acuerdo a prioridades. Es conveniente para mayor claridad aplicar criterios bien conocidos, como CVE.
Pregunta planteada	¿Se categorizan y priorizan las vulnerabilidades que afectan a la provisión del servicio esencial para su gestión?
Correlación	UNE-ISO/IEC 27001:2017 [A.12.6.1] NIST SP 800-53 R4 [RA-2], [SA-10], [SA-11], [SI-2] ENS [op.pl.1] [mp.sw.2], [op.pl.1], [op.exp.3], artículo 20 Guía contenidos mínimos PSO (2.1)
CARACTERIZACIÓN	
Escala	**L0** - No se categorizan ni priorizan las vulnerabilidades. **L1** - Se ha iniciado la categorización y priorización de las vulnerabilidades. **L2** - Se ha establecido un procedimiento para la categorización y priorización de las vulnerabilidades, pero no está documentado. **L3** - Se ha documentado el procedimiento de categorización y priorización de vulnerabilidades y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica la categorización y priorización de vulnerabilidades. **L5** - Se aplican acciones de mejora en la categorización y priorización de vulnerabilidades.
OBTENCIÓN	
Método de recogida	Manual. Se recomienda la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.
Responsable	CSO o CISO
ANÁLISIS	

Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que las vulnerabilidades están categorizadas y se prioriza regularmente su remediación.
	Acciones correctivas	• Categorizar y priorizar las vulnerabilidades para reportarlas a los responsables. • Documentar y actualizar un procedimiento de categorización y priorización de vulnerabilidades.

Tabla 15 - Métrica T-GV-OE2-04: Categorizar y priorizar las vulnerabilidades.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE2-06**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Establecer y mantener un repositorio actualizado de vulnerabilidades-
Descripción	Mantener un repositorio actualizado de aquellas vulnerabilidades que afectan a la provisión del servicio esencial. Dicho repositorio debe contener información actualizada del ciclo de vida de las vulnerabilidades, con información específica de cada una de ellas, incluidas las medidas requeridas para atajarlas.
Pregunta planteada	¿Se establece y mantiene un repositorio actualizado de las vulnerabilidades que afectan a la provisión del servicio esencial?
Correlación	UNE-ISO/IEC 27001:2017 [A.12.6.1] NIST SP 800-53 R4 [RA-5], [SA-10], [SA-11], [SC-38], [SI-2], [SI-3] ENS [op.pl.1] [mp.sw.2]
CARACTERIZACIÓN	
Escala	**L0** - No se ha establecido un repositorio de vulnerabilidades con información sobre las mismas. **L1** - Se ha iniciado la elaboración de un repositorio de vulnerabilidades con información sobre las mismas y su resolución. **L2** - Se ha establecido un repositorio de vulnerabilidades con información sobre las mismas y su resolución. **L3** - Se ha documentado un repositorio de vulnerabilidades con información sobre las mismas y su resolución. **L4** - Se gestiona, actualiza y verifica un repositorio de vulnerabilidades con información sobre las mismas y su resolución. **L5** - Se aplican acciones de mejora en el repositorio de vulnerabilidades con información sobre las mismas y su resolución.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO
ANÁLISIS	
Medida Objetivo	L5

Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización mantiene un repositorio actualizado de todas las vulnerabilidades conocidas, almacenando información de las mismas y su resolución.
	Acciones correctivas	Establecer un repositorio de vulnerabilidades con información del ciclo de vida de las mismas. Dicho repositorio debe contener información básica como: • Identificador único para referencia interna de la vulnerabilidad en la organización. • Descripción de la vulnerabilidad. • Fecha de ingreso en el repositorio. • Referencias a la fuente de la vulnerabilidad. • Importancia de la vulnerabilidad para la organización (crítica, moderada, etc.) • Personas o equipos asignados para analizarla y solucionarla. • Registro de las acciones de resolución tomadas para disminuir o eliminar la vulnerabilidad.

Tabla 16 - Métrica T-GV-OE2-06: Establecer y mantener un repositorio actualizado de vulnerabilidades.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE3-01**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Elaborar y mantener un procedimiento de gestión de parches y actualización de los activos tecnológicos.
Descripción	Las actualizaciones, ya sean de seguridad o de funcionalidad, de los sistemas informáticos deben estar guiadas por un proceso de gestión de parches que identifique adecuadamente el ciclo de vida e indique su periodicidad. En el entorno de TO la gestión de parches en los sistemas industriales debe gestionar también la posibilidad de que determinados fabricantes, no tengan implantada una publicación de parches recurrente para solucionar problemas de seguridad. Lo cual puede conducir a determinar otras medidas para proteger los activos industriales (aislamiento o monitorización activa del entorno).
Pregunta planteada	¿Se ha elaborado y mantiene un procedimiento de gestión de parches y actualización de los activos tecnológicos?
Correlación	UNE-ISO/IEC 27001:2017 [A.11.2.4] [A.12.6.1] [A.14.2.2] [A.14.2.4] NIST SP 800-53 R4 [CM-8], [SI-2], [SI-3] [SI-8] ENS [op.exp.4] [op.exp.5] Guía contenidos mínimos PPE (4.4.2) NIS (Directiva 52)
CARACTERIZACIÓN	
Escala	**L0** - No se ha elaborado ningún procedimiento para la gestión de parches y actualización de los activos tecnológicos. **L1** - Se ha iniciado la definición de un procedimiento de gestión de parches y actualización de los activos tecnológicos, pero es incompleto y no se ha formalizado. **L2** - Se ha establecido un procedimiento de gestión de parches y actualización de los activos tecnológicos, está completo pero no se actualiza. **L3** - Se ha documentado un procedimiento de gestión de parches y actualización de los activos tecnológicos. Este plan se mantiene actualizado. **L4** - Se gestiona y verifica el procedimiento de gestión de parches y actualización de los activos tecnológicos. **L5** - Se aplican acciones de mejora en el procedimiento de gestión de parches y actualización de los activos tecnológicos.

OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización incluye en sus procesos la gestión de parches y actualización de los activos tecnológicos. Como resultado de este procedimiento, se podrá valorar objetivamente el impacto de aplicar o no una actualización sobre un determinado sistema.
	Acciones correctivas	Establecer un procedimiento de gestión de parches y actualización de los activos tecnológicos, que puede incluir las actividades: • Identificación de activos y software base así como el nivel de parches de cada uno en el inventario. • Disponibilidad: revisar el listado de parches actual e identificar cuál de ellos afecta a cada activo del proceso. • Aplicabilidad: verificar si la actualización en concreto es apta para los activos de nuestro proceso. • Adquisición: obtener los ficheros de actualización de una fuente fidedigna así como comprobar la veracidad del parche. • Validación: asegurar que la actualización no impacta en el proceso de forma adversa. • Despliegue: durante el proceso de validación se ha de crear un paquete de despliegue a toda la infraestructura.

Tabla 17 - Métrica T-GV-OE3-01: Elaborar y mantener un procedimiento de gestión de parches y actualización de los activos tecnológicos.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE3-04**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Monitorizar el estado de aquellas vulnerabilidades no resueltas que afectan a la provisión del servicio esencial.
Descripción	Existen múltiples causas por las que una vulnerabilidad puede no ser corregida: olvido, ausencia de parche, afecta a sistemas no críticos o prioridad no crítica. En este indicador se trata de conocer si se realiza un seguimiento periódico y si se notifican aquellas vulnerabilidades que no han sido resueltas. Por ejemplo, se puede medir el tiempo entre la detección de la vulnerabilidad y cuando es resuelta de manera definitiva.
Pregunta planteada	¿Se monitoriza el estado de las vulnerabilidades no resueltas que afectan a la provisión del servicio esencial?
Correlación	UNE-ISO/IEC 27001:2017 [A.12.6.1] NIST SP 800-53 R4 [RA-5], [SA-10], [SA-11], [SI-2], [SI-3] ENS [op.pl.1] [mp.sw.2], [op.exp.3] Guía contenidos mínimos SO (1.4) Guía contenidos mínimos PPE (1.4, 2.4) NIS (Directiva 69)
CARACTERIZACIÓN	
Escala	**L0** - No se monitoriza el estado de las vulnerabilidades no resueltas. **L1** - Se ha iniciado la monitorización de las vulnerabilidades no resueltas. **L2** - Se ha establecido un procedimiento para la monitorización de las vulnerabilidades no resueltas, pero no está documentado. **L3** - Se ha documentado el procedimiento de monitorización de vulnerabilidades no resueltas y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la monitorización de vulnerabilidades no resueltas. **L5** - Se aplican acciones de mejora en el procedimiento para la monitorización de vulnerabilidades no resueltas.
OBTENCIÓN	
Método de recogida	Manual. Se recomienda la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.
Responsable	CSO o CISO

ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que las vulnerabilidades no resueltas son monitorizadas y reportadas regularmente.
	Acciones correctivas	• Monitorizar las vulnerabilidades no resueltas y reportarlas a los responsables. Medir los tiempos que se tardan en reportar y resolver las vulnerabilidades. • Documentar y actualizar un procedimiento de vulnerabilidades no resueltas.

Tabla 18 - Métrica T-GV-OE3-04: Monitorizar el estado de aquellas vulnerabilidades no resueltas que afectan a la provisión del servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-GV-OE4-01**
Meta	RESISTIR
Dominio Funcional	GESTIÓN DE VULNERABILIDADES
Objetivo del indicador	Identificar y analizar las causas raíz de las vulnerabilidades.
Descripción	No todas las vulnerabilidades son fallos reportados por el fabricante, muchas son debidas a malas configuraciones o instalaciones poco acertadas (arquitectura de la red por ejemplo) y otras también por su administración y uso. Estas últimas indicarían carencias de formación o de políticas específicas para la instalación y mantenimiento de estos equipos o infraestructuras. Determinar el origen de las vulnerabilidades puede resultar muy útil para mejorar la protección de los sistemas que ayudan en la provisión del servicio esencial. Esto pasa por desarrollar procedimientos que ayuden a trazar la causa raíz de la vulnerabilidad en aquellos sistemas más críticos. En este caso habrá que aplicar medidas que nos ayuden a realizar una auditoría adecuada: aislamiento del sistema, planificación temporal del análisis y reporte de los hallazgos para valorar los riesgos y facilitar la toma de decisiones.
Pregunta planteada	¿Se investigan y analizan las causas que originan las vulnerabilidades?
Correlación	ISO/IEC 27001: 2013 [A.12.6.1] NIST SP 800-53 R4 [RA-5], [SA-10], [SA-11], [SI-2], [SI-3], [IR-6] ENS [op.pl.1] [mp.sw.2], [op.exp.3] NIS (Directiva 33)
CARACTERIZACIÓN	
Escala	**L0** - No se considera definir ningún procedimiento para investigar el origen de las vulnerabilidades. **L1** - Se ha iniciado la definición del procedimiento para investigar el origen de las vulnerabilidades. **L2** - Se ha establecido un procedimiento para investigar el origen de las vulnerabilidades, pero no se ha documentado. **L3** - Se documenta y actualiza el procedimiento para investigar el origen de las vulnerabilidades. **L4** - Se gestiona, actualiza y verifica el procedimiento para investigar el origen de las vulnerabilidades. **L5** - Se aplican acciones de mejora en el procedimiento para investigar el origen de las vulnerabilidades.
OBTENCIÓN	

Método de recogida	Manual Es recomendable la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un proceso mejorado para investigar el origen de las vulnerabilidades
	Acciones correctivas	• Establecer un procedimiento para investigar el origen de las vulnerabilidades sobre los sistemas más críticos. • En caso de vulnerabilidades ligadas a configuraciones defectuosas, se propone resolver las carencias de formación o de políticas específicas para la instalación y mantenimiento de estos equipos o infraestructuras.

Tabla 19 - Métrica T-GV-OE4-01: Identificar y analizar las causas raíz de las vulnerabilidades.

2.2.2. Supervisión continua (SC)

El objetivo general de este dominio funcional es recoger, recopilar y distribuir información sobre el comportamiento y las actividades de los sistemas y las personas para apoyar el proceso continuo de identificación y análisis de riesgos de los activos de la organización y los servicios esenciales que puedan afectar negativamente al funcionamiento y prestación de los mismos. Sus objetivos específicos son:

- Monitorizar las redes de comunicaciones de la organización.
- Monitorizar el entorno físico de la organización.
- Monitorizar la actividad del personal de la organización.
- Monitorizar la actividad de proveedores de servicios externos a la organización.
- Monitorizar accesos no autorizados a la organización.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-SC-OG1-03**
Meta	RESISTIR
Dominio Funcional	SUPERVISIÓN CONTINUA
Objetivo del indicador	Establecer y mantener un procedimiento específico de monitorización continua.
Descripción	Se trata de conocer si se realiza una supervisión continua (24x7) o si existe una estrategia de monitorización continua de la provisión del servicio esencial para detectar potenciales ciberincidentes.
Pregunta planteada	¿Se monitoriza permanentemente (24x7) la provisión del servicio esencial para detectar potenciales ciberincidentes?
Correlación	ISO/IEC 27001:2017 [A.12.1.3] NIST SP 800-53 R4 [RA-5], [CA-7], [PM-6], [SI-4] ENS [op.mon] Guía contenidos mínimos PSO (2.2.3) Guía contenidos mínimos PPE (4.2.2)
CARACTERIZACIÓN	

Escala	**L0** - No se realiza la monitorización 24x7 de la provisión del servicio esencial. **L1** - Se ha iniciado la monitorización 24x7 de la provisión del servicio esencial. **L2** - Se ha establecido un procedimiento de monitorización 24x7 de la provisión del servicio esencial, pero no se ha documentado. **L3** - Se ha documentado un procedimiento de monitorización 24x7 de la provisión del servicio esencial y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la monitorización 24x7 de la provisión del servicio esencial. **L5** - Se aplican acciones de mejora en el procedimiento para la monitorización 24x7 de la provisión del servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO o Director de Seguridad Física	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización monitoriza (24x7) el servicio esencial para detectar potenciales ciberataques.
	Acciones correctivas	• Establecer un procedimiento de monitorización continua sobre los activos y procesos que dan soporte a los servicios esenciales (redes de comunicaciones, sistemas, accesos, entorno físico, actividad del personal, proveedores de servicios externos, etc.) para detectar potenciales ciberataques. • Identificar a los responsables implicados en la monitorización continua y delimitar sus responsabilidades.

Tabla 20 - Métrica T-SC-OG1-03: Establecer y mantener un procedimiento específico de monitorización continua.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-SC-OE1-01**
Meta	RESISTIR
Dominio Funcional	SUPERVISIÓN CONTINUA
Objetivo del indicador	Monitorizar las redes de comunicaciones de la organización para detectar potenciales eventos de Ciberseguridad.
Descripción	Un evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. Supervisar las redes de comunicaciones que dan soporte al servicio esencial para detectar eventos de seguridad, como por ejemplo las conexiones no autorizadas del malware que pueden comprometer los activos de la organización (personas, procesos, tecnología o instalaciones). Para ello se puede usar un sistema de detección de intrusiones o un cortafuegos.
Pregunta planteada	¿Se supervisan las redes de comunicaciones que dan soporte al servicio esencial para detectar conexiones no autorizadas?
Correlación	ISO/IEC 27001: 2013 [A.12.1.3], [A.14.2.7] NIST SP 800-53 R4 [RA-5], [CA-7], [PM-6], [SI-4] ENS [op.mon] Guía contenidos mínimos PPE (4.2.2)
CARACTERIZACIÓN	
Escala	**L0** - No se realiza la monitorización de redes de comunicaciones para detectar conexiones no autorizadas. **L1** - Se ha iniciado la monitorización de redes de comunicaciones para detectar conexiones no autorizadas. **L2** - Se ha establecido un procedimiento de monitorización de redes de comunicaciones para detectar conexiones no autorizadas, pero no se han documentado. **L3** - Se ha documentado un procedimiento de monitorización de redes de comunicaciones para detectar conexiones no autorizadas y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la monitorización de redes de comunicaciones para detectar conexiones no autorizadas. **L5** - Se aplican acciones de mejora en el procedimiento para la monitorización de redes de comunicaciones para detectar conexiones no autorizadas.
OBTENCIÓN	

Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización monitoriza las redes de comunicaciones para detectar conexiones no autorizadas.
	Acciones correctivas	Documentar, actualizar, verificar y mejorar un procedimiento de monitorización continua de los eventos de ciberseguridad que se registran en las redes de comunicaciones.

Tabla 21 - Métrica T-SC-OE1-01: Monitorizar las redes de comunicaciones de la organización para detectar potenciales eventos de Ciberseguridad.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-SC-OE1-02**
Meta	RESISTIR
Dominio Funcional	SUPERVISIÓN CONTINUA
Objetivo del indicador	Supervisar la existencia de software y hardware no autorizados en los sistemas que soportan los servicios esenciales.
Descripción	La existencia de software o hardware no autorizado en la organización se debe en gran parte a empleados que no respetan los procedimientos para obtener la tecnología a través de canales corporativos, o desconocen las consecuencias que su instalación puede tener en el entorno organizativo. Por ejemplo: uso de USB no autorizados, plataformas de intercambio de ficheros no corporativo, o instalación de software pirata. Supervisar el sistema que da soporte al servicio esencial en busca de software o hardware no autorizado es crucial para combatir estas prácticas. Por ejemplo, pueden usarse herramientas de escaneo periódico del sistema que da soporte al servicio esencial.
Pregunta planteada	¿Se supervisa el sistema que da soporte al servicio esencial en busca de software o hardware no autorizado?
Correlación	ISO/IEC 27001:2017 [A.12.1.3], [A.14.2.7] NIST SP 800-53 R4 [RA-5], [CA-7], [PM-6], [SI-4] ENS [op.mon]
CARACTERIZACIÓN	
Escala	**L0 -** No se realiza la monitorización del sistema para detectar software o hardware no autorizado. **L1 -** Se ha iniciado la monitorización del sistema para detectar software o hardware no autorizado. **L2 -** Se ha establecido un procedimiento de monitorización del sistema para detectar software o hardware no autorizado, pero no se ha documentado. **L3 -** Se ha documentado un procedimiento de monitorización del sistema para detectar software o hardware no autorizado y se mantiene actualizado. **L4 -** Se gestiona, actualiza y verifica el procedimiento para la monitorización del sistema para detectar software o hardware no autorizado. **L5 -** Se aplican acciones de mejora en el procedimiento para la monitorización del sistema para detectar software o hardware no autorizado.
OBTENCIÓN	

Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización monitoriza los sistemas que dan soporte a los servicios esenciales en busca de software o hardware no autorizado.
	Acciones correctivas	• Documentar, actualizar, verificar y mejorar un procedimiento de monitorización continua sobre los sistemas que dan soporte a los servicios esenciales en busca de software o hardware no autorizado. • Establecer políticas sobre el uso permitido y no permitido de software y hardware; y comunicarlas a los empleados. • Seleccionar las herramientas que sirvan para detectar el uso de software o hardware no autorizado.

Tabla 22 - Métrica T-SC-OE1-02: Supervisar la existencia de software y hardware no autorizados en los sistemas que soportan los servicios esenciales.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**T-SC-OE4-01**
Meta	RESISTIR
Dominio Funcional	SUPERVISIÓN CONTINUA
Objetivo del indicador	Establecer y mantener un procedimiento acordado con los proveedores externos (en los ANS) para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial.
Descripción	Los servicios especializados externos, por ejemplo de proveedores de consultoría, tecnología (*cloud* o *hosting* entre otros) pueden dar soporte a la provisión del servicio esencial de la organización. En este tipo de situaciones, de nada servirá contar con un alto nivel de exigencia en seguridad en la propia organización, si no se exige ese mismo nivel a los proveedores externos. Es necesario establecer cláusulas en el Acuerdo de Nivel de Servicio (siglas ANS) y en los contratos que nos ayuden a fijar el nivel acordado de calidad y seguridad, así como determinar los mecanismos de monitorización y control necesarios para reaccionar rápidamente en caso de que el servicio prestado pueda verse comprometido por la presencia de eventos de ciberseguridad.
Pregunta planteada	¿Existe un procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial?
Correlación	ISO/IEC 27001: 2013 [A.12.6.1] NIST SP 800-53 R4 [[SA-9] ENS [op.pl.1] [mp.sw.2], [op.exp.3] [op.exp.9] [mp.s.8] Guía de contenidos mínimos PPE 3.2, 3,3 NIS (Directiva 27, Artículo 16)
CARACTERIZACIÓN	

Escala	**L0** - No se ha establecido ningún procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. **L1** - Se ha iniciado el establecimiento de un procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. **L2** - Se ha establecido un procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. **L3** - Se ha documentado el procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. **L4** - Se gestiona, actualiza y verifica el procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. **L5** - Se aplican acciones de mejora en la definición del procedimiento acordado con los proveedores externos para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual Se recomienda la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un proceso mejorado para que los proveedores externos reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial.
	Acciones correctivas	• Identificar, documentar y mantener actualizado un procedimiento acordado para que los proveedores externos reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial. • Implementar acciones de mejora para la reducción de los tiempos de reporte de eventos de ciberseguridad desde proveedores externos.

Tabla 23 - Métrica T-SC-OE4-01: Establecer y mantener un procedimiento acordado con los proveedores externos (en los ANS) para que reporten los potenciales eventos de ciberseguridad que afecten al servicio esencial.

2.3. Recuperar

A continuación, se detallan las fichas para las métricas correspondientes a la meta de Recuperar.

2.3.1. Gestión de incidentes (GI)

El objetivo general de este dominio funcional es establecer procesos para identificar y analizar los eventos, detectar incidentes, y determinar una respuesta de la organización. Un **evento de seguridad** de la información es una ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. Los objetivos específicos son:

- Establecer un proceso para detectar, reportar, priorizar y analizar eventos.
- Identificar y analizar los ciberincidentes
- Establecer un proceso para responder y recuperarse de los ciberincidentes.
- Analizar la información de los ciberincidentes.
- Coordinación con otros organismos en la respuesta a los ciberincidentes.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE1-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Establecer un procedimiento para detectar, reportar y notificar eventos.
Descripción	Debe existir un procedimiento para la detección de eventos y su notificación al personal a cargo de la gestión de incidentes. Se trata de conocer si se identifican eventos, es decir, sucesos inesperados o no deseados (por ejemplo, intentos de accesos no autorizados, tiempos de respuesta altos, incremento en volumen de archivos), en las infraestructuras que soportan el servicio esencial y si se notifican a los responsables, quienes procederán a su inmediato o posterior análisis. Por ejemplo, indique si existen herramientas o servicios con mecanismos de detección automática de eventos en tiempo real.
Pregunta planteada	¿Se lleva a cabo la detección de eventos y su notificación al personal a cargo de la gestión de incidentes?
Correlación	ISO/IEC 27001:2017 [A.16.1.2], [A.16.1.3], [A.16.1.4] NIST SP 800-53 R4 [AR-4], [IR-4], [IR-5], [IR-6], [PE-6] ENS [op.exp.7]

	Guía contenidos mínimos PPE (2.3) NIS (Directiva 4, 69)	
CARACTERIZACIÓN		
Escala	**L0** - No se realiza una detección y notificación de eventos. **L1** - Se ha iniciado la detección y notificación de eventos. **L2** - Se ha establecido un procedimiento de detección y notificación de eventos, pero no se han documentado. **L3** - Se ha documentado un procedimiento de detección y notificación de eventos y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la detección y notificación de eventos. **L5** - Se aplican acciones de mejora en el procedimiento para la detección y notificación de eventos.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización dispone de un procedimiento actualizado para capturar y analizar eventos, de manera que puede determinar si el evento se convertirá (o se ha convertido) en un ciberincidente que requiere la acción de la organización y notificar a los responsables oportunos para proceder a su análisis.
	Acciones correctivas	Establecer un procedimiento de reporte de eventos para detectarlos y proporcionar informes al personal de gestión de incidentes y a los responsables interesados. Incidir en el Plan de Concienciación a los usuarios en la necesidad de comunicar a los responsables, cuanto antes, cualquier anomalía o evento de seguridad detectado, enseñándoles a reconocer las situaciones anómalas que pueden iniciar un incidente (mal funcionamiento, lentitud de procesos, comportamientos fuera de lo normal,…).

Tabla 24 - Métrica R-GI-OE1-01: Establecer un procedimiento para detectar, reportar y notificar eventos.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE2-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Establecer y mantener un procedimiento para clasificar y valorar los ciberincidentes.
Descripción	Disponer de un procedimiento para clasificar y valorar ciberincidentes, basado en una tipificación predefinida de los mismos permitirá además de mejorar la gestión de incidentes, demostrar el cumplimiento normativo de la organización de cara al reporte de los mismos. Por ejemplo, se ha de registrar para los ciberincidentes datos tales como fecha de detección, fecha de notificación, fecha de resolución y fecha de cierre. La notificación de incidentes puede ser obligatoria o potestativa y ha de seguir unos criterios homogéneos como indica la Guía nacional de notificación y gestión de incidentes (véase apartado Referencias).
Pregunta planteada	¿Se dispone de un procedimiento para la clasificación y valoración de los ciberincidentes, basado en una tipificación predefinida de los mismos?
Correlación	ISO/IEC 27001:2017 [A.16.1.2], [A.16.1.3], [A.16.1.4] NIST SP 800-53 R4 [IR-4] ENS [op.exp.7] Guía contenidos mínimos PPE (4.2.2) NIS (Directiva 2)
CARACTERIZACIÓN	

Escala	**L0** - No existe un procedimiento para clasificar y evaluar los ciberincidentes de acuerdo con una tipificación de los mismos. **L1** - Se ha iniciado el establecimiento de un procedimiento para clasificar y evaluar los ciberincidentes basado en una tipificación definida. **L2** - Se ha establecido un procedimiento para clasificar y evaluar los ciberincidentes basado en una tipificación de los mismos, pero no se han documentado. **L3** - Se ha documentado un procedimiento para clasificar y evaluar los ciberincidentes basado en una tipificación de los mismos y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la clasificar y valoración de los ciberincidentes basada en su tipificación. **L5** - Se aplican acciones de mejora en el procedimiento para la clasificación y valoración de ciberincidentes basada en su tipificación.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización clasifica y valora los ciberincidentes de acuerdo con un proceso establecido, utilizando una clasificación de incidentes definida, para obtener métricas que permitan sustentar el cumplimiento normativo.
	Acciones correctivas	Establecer un procedimiento para la clasificación y valoración de ciberincidentes utilizando una tipificación predefinida, como la propuesta por la Guía de Seguridad de las TIC CCN-STIC 817 o la Guía Nacional de Notificación y Gestión de Ciberincidentes (véase apartado Referencias).

Tabla 25 - Métrica R-GI-OE2-01: Establecer y mantener un procedimiento para clasificar y valorar los ciberincidentes.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE2-02**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Documentar y transmitir los criterios para identificar y reconocer ciberincidentes.
Descripción	Se trata de conocer si se han documentado y transmitido los criterios que facilitan a los miembros del personal de la organización la identificación y reconocimiento de un ciberincidente para su reporte.
Pregunta planteada	¿Se han establecido los criterios para identificar y reconocer los ciberincidentes, están accesibles y son conocidos por todo el personal?
Correlación	ISO/IEC 27001:2017 [A.16.1.2], [A.16.1.3], [A.16.1.4] NIST SP 800-53 R4 [IR-4] ENS [op.exp.7] Guía contenidos mínimos PPE (4.2.2) NIS (Directiva 2)
CARACTERIZACIÓN	
Escala	**L0** - No se han establecido los criterios de identificación y reconocimiento de ciberincidentes. **L1** - Se ha iniciado la definición de los criterios de identificación y reconocimiento de ciberincidentes. **L2** - Se han establecido los criterios de identificación y reconocimiento de ciberincidentes, pero no se han documentado ni transmitido a todos los miembros de la organización. **L3** - Se han documentado los criterios de identificación y reconocimiento de ciberincidentes, se han transmitido a todos los miembros de la organización y se mantienen actualizados. **L4** - Se gestionan, actualizan y verifican los criterios de identificación y reconocimiento de ciberincidentes. **L5** - Se aplican acciones de mejora en la definición de los criterios de identificación y reconocimiento de ciberincidentes.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO
ANÁLISIS	
Medida Objetivo	L5

Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha definido y documentado los criterios de identificación y reconocimiento de ciberincidentes y esta información está disponible para todo el personal que pueda necesitarlo.
	Acciones correctivas	Definir y documentar los criterios de identificación y reconocimiento de ciberincidentes y hacer que esta información esté disponible para todo el personal.

Tabla 26 - Métrica R-GI-OE2-02: Documentar y transmitir los criterios para identificar y reconocer ciberincidentes.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE2-03**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Analizar los ciberincidentes para determinar una respuesta apropiada.
Descripción	Se trata de conocer si se sigue algún procedimiento de análisis de incidentes que permita identificar las acciones necesarias para su resolución, en el menor tiempo posible. Por ejemplo, respondiendo a las siguientes preguntas: ¿qué ha pasado?, ¿a quién afecta (usuarios/clientes/proveedores)?, ¿qué debo decirles?, ¿a quién tengo que avisar?, ¿tiene repercusiones legales o contractuales? o ¿tenemos bajo control los servicios y sistemas afectados?
Pregunta planteada	¿Se analizan los ciberincidentes para determinar la respuesta más apropiada en el menor tiempo posible?
Correlación	ISO/IEC 27001:2017 [A.16.1.2], [A.16.1.3], [A.16.1.4] NIST SP 800-53 R4 [AR-4], [IR-4], [IR-5], [IR-6], [PE-6] ENS [op.exp.7] Guía contenidos mínimos PSO (2.2.3,4.1,4.4) Guía contenidos mínimos PPE (1.1,4.2, 4.4) NIS (Directiva 27, 28, 34)
CARACTERIZACIÓN	
Escala	**L0** - No se realiza un análisis de ciberincidentes para determinar la respuesta más apropiada. **L1** - Se ha iniciado el análisis de ciberincidentes para determinar la respuesta más apropiada. **L2** - Se ha establecido un procedimiento de análisis de ciberincidentes para determinar la respuesta más apropiada, pero no se ha documentado. **L3** - Se ha documentado y se actualiza un procedimiento de análisis de ciberincidentes para determinar la respuesta más apropiada. **L4** - Se gestiona, actualiza y verifica el procedimiento de análisis de ciberincidentes para determinar la respuesta más apropiada. **L5** - Se aplican acciones de mejora en el procedimiento de análisis de ciberincidentes para determinar la respuesta más apropiada.
OBTENCIÓN	
Método de recogida	Manual

Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización dispone de un procedimiento de análisis de ciberincidentes estandarizado para formular una respuesta en el menor tiempo posible.
	Acciones correctivas	Establecer un procedimiento de análisis de ciberincidentes con el que definir correctamente el tipo de incidente y preparar la respuesta más adecuada en el menor tiempo posible. También debería ayudar a determinar si el incidente tiene repercusiones legales y a quién hay que comunicárselo. En el caso de brechas de seguridad de datos de carácter personal, la entidad de referencia es la AEPD.

Tabla 27 - Métrica R-GI-OE2-03: Analizar los ciberincidentes para determinar una respuesta apropiada.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE3-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Establecer una estructura de respuesta a incidentes para el escalado a los responsables encargados de su resolución.
Descripción	Establecer una estructura organizativa de respuesta a ciberincidentes, así como un protocolo formal de escalado de los mismos a los responsables pertinentes. Por ejemplo, indique si existe documentación que especifique a quienes se debe notificar.
Pregunta planteada	¿Se dispone de una estructura de respuesta a ciberincidentes que permita que éstos sean escalados a los responsables encargados de su resolución?
Correlación	ISO/IEC 27001:2017 [A.16.1.5] NIST SP 800-53 R4 [IR-4], [IR-9], [SE-2] ENS [op.exp.7] Guía contenidos mínimos PSO (1.5) NIS (Artículo 4, punto 1)
CARACTERIZACIÓN	
Escala	**L0** - No existe una estructura de respuesta a ciberincidentes. **L1** - Se ha iniciado la definición de una estructura de respuesta a ciberincidentes. **L2** - Se ha establecido una estructura de respuesta a ciberincidentes, pero no se ha documentado. **L3** - Se ha documentado una estructura de respuesta a ciberincidentes y se mantiene actualizada. **L4** - Se gestiona, actualiza y verifica la estructura de respuesta a ciberincidentes. **L5** - Se aplican acciones de mejora en el diseño de la estructura de respuesta a ciberincidentes.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO
ANÁLISIS	
Medida Objetivo	L5

Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe una estructura de escalado completa y clara que facilita una mayor coordinación, interna y externa, para dar respuesta a ciberincidentes.
	Acciones correctivas	• Establecer una estructura de respuesta a incidentes y un protocolo de escalado para asegurar que los incidentes abordan lo más rápido posible por las personas responsables, pues de no hacerlo, se impedirá la diligente respuesta de la organización, aumentando así el impacto del ciberincidente. • Enviar comunicaciones periódicas a los usuarios insistiendo en la necesidad de comunicar cuanto antes cualquier anomalía o evento de seguridad detectado, enseñándoles a reconocer las situaciones anómalas que pueden iniciar un incidente (mal funcionamiento, lentitud de procesos, comportamientos fuera de lo normal, etc.). • Ofrecer canales de comunicación a los usuarios para el reporte de detección de incidentes.

Tabla 28 - Métrica R-GI-OE3-01: Establecer una estructura de respuesta a incidentes para el escalado a los responsables encargados de su resolución.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE3-04**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Controlar los ciberincidentes hasta su resolución.
Descripción	El control de ciberincidentes permite gestionar adecuadamente los potenciales eventos de seguridad. En función del tipo de incidente, éste se asignará y escalará a las personas que procedan para asegurar, en la medida de lo posible, su correcto análisis, resolución, notificación y cierre. La obtención de indicadores como el tiempo que se emplea a la resolución del ciberincidente es, además, vital para asegurar el cumplimiento legal en caso de que el ciberincidente esté relacionado con datos de carácter personal.
Pregunta planteada	¿Se mantiene un control de los ciberincidentes hasta su resolución?
Correlación	ISO/IEC 27001:2017 [A.16.1.2], [A.16.1.3], [A.16.1.4] NIST SP 800-53 R4 [IR-1], [IR-4], [IR-5], [IR-6], [IR-8] ENS [op.exp.7] [op.exp.9] NIS (Directiva 27)
CARACTERIZACIÓN	
Escala	**L0** - No se realiza ningún control de los ciberincidentes hasta su resolución. **L1** - Se ha iniciado el control de los ciberincidentes hasta su resolución, pero no se ha establecido. **L2** - Se ha establecido un procedimiento para el control de los ciberincidentes hasta su resolución, pero no se ha documentado. **L3** - Se ha documentado y se actualiza el procedimiento para el control de los ciberincidentes hasta su resolución. **L4** - Se gestiona, actualiza y verifica el procedimiento para el control de los ciberincidentes hasta su resolución. **L5** - Se aplican acciones de mejora en el procedimiento para el control de los ciberincidentes hasta su resolución.
OBTENCIÓN	
Método de recogida	Manual Se recomienda la entrevista personal o telefónica, para poder interpretar los resultados con mayor nivel de detalle.
Responsable	CSO o CISO

ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un procedimiento mejorado para el control de los ciberincidentes hasta su resolución. Conviene aumentar la vigilancia y control especialmente si estas actividades de detección dependen de terceros.
	Acciones correctivas	• Establecer y mejorar el proceso midiendo los tiempos entre que son detectados los eventos y su resolución. • Registrar las lecciones aprendidas para cada tipo de evento.

Tabla 29 - Métrica R-GI-OE3-04: Controlar los ciberincidentes hasta su resolución.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE3-06**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Establecer un proceso para estimar la capacidad de respuesta y recuperación de los ciberincidentes.
Descripción	Estimar con indicadores de eficacia la capacidad de respuesta y recuperación ante un ciberincidente, es decir, la capacidad de detectar ataques y amenazas, minimizar las pérdidas o la destrucción de activos tecnológicos o de información, mitigar la explotación dañina de los puntos débiles de las infraestructuras y recuperar los servicios a la mayor brevedad posible. Entre otros factores se puede medir el tiempo medio en responder a los distintos incidentes o el uso de recursos (horas de los técnicos). Una manera de medir el tiempo en resolver incidentes es registrar el momento en el que se detecta un ciberataque y en el que es desactivado y valorar el tiempo transcurrido de media para cada tipo de incidente. En caso de no haberse sufrido nunca un ciberincidente, pueden considerarse, por ejemplo, los tiempos obtenidos en la recuperación de sistemas en las pruebas del plan de continuidad realizadas. Pueden seguirse métricas e indicadores estandarizados como los indicados en la Guía de Seguridad de las TIC CCN-STIC 817 (véase apartado Referencias).
Pregunta planteada	¿Se tiene una estimación de la capacidad de respuesta y de recuperación ante un ciberincidente?
Correlación	ISO/IEC 27001:2017 [A.16.1.5] NIST SP 800-53 R4 [IR-4], [IR-9], [SE-2] ENS [op.exp.7] Guía contenidos mínimos PPE (4.2) NIS (Directivas 27, 33)
CARACTERIZACIÓN	

Escala	**L0** - No se estima la capacidad de respuesta y de recuperación ante un ciberincidente. **L1** - Se ha iniciado la definición de un procedimiento para estimar la capacidad de respuesta y de recuperación ante un ciberincidente. **L2** - Se ha establecido un procedimiento para medir la capacidad respuesta y de recuperación ante un ciberincidente, pero no se ha documentado. **L3** - Se ha documentado y se actualiza el procedimiento para estimar la capacidad de respuesta y de recuperación ante un ciberincidente. **L4** - Se gestiona, actualiza y verifica el procedimiento para estimar la capacidad de respuesta y de recuperación ante un ciberincidente. **L5** - Se aplican acciones de mejora en el procedimiento para la definición y estimación de la capacidad de respuesta y de recuperación ante un ciberincidente.	
OBTENCIÓN		
Método de recogida	Manual Se recomienda la entrevista personal o telefónica para poder interpretar los resultados con mayor nivel de detalle.	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que se ha estimado el número de horas entre la ocurrencia de un ciberincidente y la resolución.
	Acciones correctivas	• Establecer un procedimiento para estimar el tiempo medio de respuesta a un ciberincidente y el uso de recursos en horas de técnicos en su resolución. • Documentar, actualizar y verificar el procedimiento para estimar el tiempo medio de resolución.

Tabla 30 - Métrica R-GI-OE3-06: Establecer un proceso para estimar la capacidad de respuesta y recuperación de los ciberincidentes.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE4-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Investigar las causas de los ciberincidentes.
Descripción	En lo relativo a la respuesta frente a incidentes, determinar las causas de los ciberincidentes puede resultar muy útil para valorar qué lo ha ocasionado; determinar y depurar responsabilidades; y aprender lecciones. Esto se puede realizar apoyándose en procedimientos que ayuden a trazar la causa raíz del ciberincidente. En este caso habrá que aplicar medidas que nos ayuden a realizar una investigación adecuada: establecimiento del dispositivo de investigación, aislamiento del sistema, planificación temporal del análisis y reporte de los hallazgos para valorar los riesgos y facilitar la toma de decisiones.
Pregunta planteada	¿Se investigan las causas de los ciberincidentes?
Correlación	ISO/IEC 27001:2017 [A.16.1.6] NIST SP 800-53 R4 [IR-4], [IR-9], [SE-2] ENS [op.exp.7] [op.exp.8] Guía contenidos mínimos PPE (4.2) NIS (Directivas 27, 33)
CARACTERIZACIÓN	
Escala	**L0** - No se investiga el origen de los ciberincidentes. **L1** - Se ha iniciado la definición de un procedimiento para investigar el origen de los ciberincidentes. **L2** - Se ha establecido el procedimiento para investigar el origen de los ciberincidentes, pero no se han documentado. **L3** - Se documenta y actualiza el procedimiento para investigar el origen de los ciberincidentes. **L4** - Se gestiona, actualiza y verifica el procedimiento para investigar el origen de los ciberincidentes. **L5** - Se aplican acciones de mejora en el procedimiento para investigar el origen de los ciberincidentes.
OBTENCIÓN	
Método de recogida	Manual Se recomienda realizar una entrevista personal o telefónica, para interpretar los resultados con mayor nivel de detalle.
Responsable	CSO o CISO
ANÁLISIS	

Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un procedimiento para investigar las causas de los ciberincidentes.
	Acciones correctivas	• Establecer un procedimiento para la investigación de ciberincidentes, usando por ejemplo guías como Guía de Seguridad de las TIC CCN-STIC 817. • Documentar, revisar y verificar el procedimiento para investigar las causas de los ciberincidentes.

Tabla 31 - Métrica R-GI-OE4-01: Investigar las causas de los ciberincidentes.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-GI-OE5-03**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE INCIDENTES
Objetivo del indicador	Coordinar con otros organismos, como las FCSE, la respuesta a los ciberincidentes.
Descripción	Se trata de conocer si existen vías formales de comunicación con las Fuerzas y Cuerpos de Seguridad del Estado y si se hace uso de ellas para notificar aquellos incidentes graves que hayan ocurrido en la organización. Si el servicio esencial está soportado por un Sistema de Control Industrial (SCI), debe prestarse especial atención a los incidentes relacionados con la seguridad física de los elementos SCADA distribuidos geográficamente fuera de la sede de la organización (plantas industriales, al aire libre, etc.)
Pregunta planteada	¿Se comunican a las Fuerzas y Cuerpos de Seguridad del Estado los ciberincidentes graves que se producen en la organización?
Correlación	ISO/IEC 27001:2017 [A.16.1.6], [A.16.1.7] NIST SP 800-53 R4 [IR-4], [IR-9] ENS [op.exp.7] Guía contenidos mínimos PSO (2.2.1, 2.2.4) Guía contenidos mínimos PPE (2.1, 2.3, 4.2.1)
CARACTERIZACIÓN	
Escala	**L0 -** No existe un procedimiento para comunicar ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado. **L1** - Se ha iniciado el procedimiento para la comunicación de ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado. **L2** - Se ha establecido un procedimiento para comunicar ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado, pero no se han documentado. **L3** - Se ha documentado y se mantiene actualizado un procedimiento para comunicar ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado. **L4** - Se gestiona, actualiza y verifica el procedimiento para la comunicación de ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado. **L5** - Se aplican acciones de mejora al procedimiento para la comunicación de ciberincidentes a las Fuerzas y Cuerpos de Seguridad del Estado.

OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	Se comunican **todos** los ciberincidentes graves a las Fuerzas y Cuerpos de Seguridad del Estado.	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización comunica todos los ciberincidentes graves a las fuerzas y cuerpos de seguridad del estado (FCSE).
	Acciones correctivas	Fomentar la coordinación y comunicación con las Fuerzas y Cuerpos de Seguridad del Estado en la respuesta a ciberincidentes. Documentar, revisar y actualizar el procedimiento de comunicación con las Fuerzas y Cuerpos de Seguridad del Estado.

Tabla 32 - Métrica R-GI-OE5-03: Coordinar con otros organismos, como las FCSE, la respuesta a los ciberincidentes.

2.3.2. Gestión de continuidad del servicio (CS)

El objetivo general de este dominio funcional es establecer procesos para identificar y analizar los eventos, detectar incidentes, y determinar una respuesta de la organización. Sus objetivos específicos son:

- Desarrollar planes de continuidad de los servicios esenciales.
- Revisar los planes de continuidad.
- Probar los planes de continuidad.
- Ejecutar y revisar los planes de continuidad.
- Establecer procesos para gestionar un nivel adecuado de controles que aseguren la protección de los servicios esenciales y activos críticos que dependen de las acciones de entidades externas.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE1-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Desarrollar un Plan de Continuidad para garantizar la provisión del servicio esencial.
Descripción	Se trata de conocer si la provisión del servicio esencial está respaldada por un Plan de Continuidad, si éste sigue una disciplina de actualización periódica y si se actualiza también cuando se conocen nuevos riesgos o cambios en el entorno organizativo u operativo.
Pregunta planteada	¿Se ha definido un Plan de Continuidad que garantice la provisión permanente del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.17.1.1], [A.17.1.2] NIST SP 800-53 R4 [CP-1], [CP-2], [CP-13], [PM-11] ENS [op.cont.2] Guía contenidos mínimos PPE (2.3) NIS (Directiva 69)
CARACTERIZACIÓN	

Escala	**L0** - No existe un Plan de Continuidad para garantizar la provisión del servicio esencial. **L1** - Se ha iniciado el desarrollo de un Plan de Continuidad para garantizar la provisión servicio esencial. **L2** - Se han establecido las acciones del Plan de Continuidad para la provisión del servicio esencial, pero no se han documentado. **L3** - Se ha documentado el Plan de Continuidad del servicio esencial y se mantiene actualizado. **L4** - Se gestiona, actualiza y revisa el Plan de Continuidad de continuidad del servicio esencial. **L5** - Se aplican acciones de mejora en el Plan de Continuidad del servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización desarrolla el Plan de Continuidad del servicio esencial, es decir, que contempla la protección, dependencias o reemplazos de los activos esenciales que intervienen en la prestación de dicho servicio (personas, información, tecnología e instalaciones).

	Acciones correctivas	• Revisar si los planes de continuidad de los servicios esenciales contemplan los activos críticos involucrados (personas, información, tecnología, instalaciones) en el servicio esencial. • Comprobar que los planes de continuidad tienen en cuenta aspectos como la reubicación de las actividades y recursos, la existencia de procesos alternativos o redundancia, el reemplazo de los recursos y actividades y soluciones temporales de contingencia. • Adecuar los Planes de continuidad a estándares establecidos (por ejemplo, ISO 22313). • Desarrollar, actualizar y verificar las actuaciones del Plan de Continuidad del servicio esencial para el cual estamos haciendo la encuesta. • Poner a disposición de todos los involucrados los Planes de Continuidad y conservar versiones. • Se revisan los planes de continuidad para garantizar que no existen conflictos con otros planes.

Tabla 33 - Métrica R-CS-OE1-01: Desarrollar un Plan de Continuidad para garantizar la provisión del servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE1-06**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Definir los RTO en el Plan de Continuidad.
Descripción	El tiempo objetivo de recuperación o RTO por sus siglas en inglés es el tiempo definido dentro del nivel de servicio en el que un proceso de negocio **debe** ser recuperado después de un desastre o pérdida para así evitar consecuencias debido a la ruptura de continuidad de servicio. El RTO establece los límites técnicos temporales de toda la estrategia de gestión de la continuidad del negocio. El RTO (tiempo objetivo de recuperación) debe ser inferior al MTD (máximo tiempo tolerable de interrupción). Hay que asegurar que el tiempo objetivo de recuperación (*RTO*) no solo está documentado, sino que se emplea para garantizar la continuidad del servicio. Además, se verifica que el *RTO* se ajusta a las exigencias de continuidad del servicio esencial. Este dato se determina generalmente por el personal técnico.
Pregunta planteada	Los planes de continuidad, ¿documentan el tiempo objetivo de recuperación (*RTO*) del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.17.1.1], [A.17.1.2] NIST SP 800-53 R4 [CP-1], [CP-2], [CP-13], [PM-11] ENS [op.cont.1] Guía contenidos mínimos PPE (4.2) NIS (Directivas 69)
CARACTERIZACIÓN	

Escala	**L0 -** No se ha definido el *RTO* ni se ha identificado como necesario para la continuidad de la provisión del servicio esencial. **L1 -** Se ha identificado la necesidad de establecer el *RTO* para la provisión del servicio esencial y se ha iniciado su definición. **L2** - Se ha establecido un procedimiento para definir el *RTO* para la continuidad de la provisión del servicio esencial, pero no se han documentado. **L3** - Se ha documentado y se mantiene actualizado un procedimiento para definir el *RTO* en todos los planes de continuidad para la provisión del servicio esencial. **L4** - Se gestiona, actualiza y revisa el procedimiento para definir el *RTO* en los planes de continuidad para la provisión del servicio esencial. **L5** - Se aplican acciones de mejora en el procedimiento para la definición del *RTO* documentado en los planes de continuidad para la provisión del servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización documenta los tiempos objetivos de recuperación (*RTO*) del servicio esencial en su plan de continuidad.

	Acciones correctivas	Identificar los RTO para la continuidad del servicio esencial. Para ello se puede considerar la suma de: • el tiempo de detección y decisión; • el tiempo para restaurar los equipos/servidores dañados o inactivos; • el tiempo en localizar la copia de seguridad adecuada y segura y restaurarla; • el tiempo necesario en reanudar la operación. Para valorar el RTO se han de tener en cuenta el equilibrio con los costes pues si es muy bajo implicará costes mayores al tener equipos/servicios de contingencia más rápidos Además, se debe especificar un periodo mínimo de revisión del RTO y los cambios del sistema que hacen necesaria su revisión. Se puede ampliar esta información en la Guía de Seguridad de las TIC CCN-STIC 803.

Tabla 34 - Métrica R-CS-OE1-06: Definir los RTO en el Plan de Continuidad.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE3-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Probar los planes de continuidad para garantizar que cumplen los objetivos de recuperación.
Descripción	Se trata de conocer si se dispone de protocolos de prueba para el Plan de continuidad del servicio esencial y si es verificado regularmente a fin de: • Determinar la viabilidad, exhaustividad y precisión del Plan de Continuidad con respecto al servicio esencial. • Recabar información sobre el grado de preparación de la organización. Si el servicio esencial se basa en un Sistema de Control Industrial (SCI), que no permite la realización de una parada completa para la ejecución de pruebas del Plan de continuidad, puede plantearse la realización de paradas parciales o por fases; la realización de pruebas sobre una réplica del mismo; o incluso su simulación.
Pregunta planteada	¿Se ha probado el Plan de Continuidad para la provisión del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.17.1.3] NIST SP 800-53 R4 [CP-3], [CP-4] ENS [op.cont.3] Guía contenidos mínimos PPE (2.3) NIS (Directiva 69)
CARACTERIZACIÓN	
Escala	**L0** - No se prueba el Plan de continuidad para ningún servicio esencial. **L1** - Se ha iniciado la definición de las pruebas del Plan de continuidad para el servicio esencial. **L2** - Se han establecido pruebas periódicas del Plan de continuidad para el servicio esencial, pero no se han documentado. **L3** - Se han documentado todos los planes de pruebas del Plan de continuidad del servicio esencial y se mantienen actualizados. **L4** - Se gestionan, actualizan y revisan los planes de pruebas del Plan de continuidad del servicio esencial. **L5** - Se aplican acciones de mejora en el Plan de continuidad como resultado de las pruebas.
OBTENCIÓN	

Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización prueba el Plan de Continuidad del servicio esencial para el cual estamos haciendo la encuesta.
	Acciones correctivas	• Establecer un procedimiento de prueba para el Plan de Continuidad del servicio esencial identificado. • Probar los planes de continuidad para garantizar que cumplen los objetivos de recuperación. • Establecer una planificación para la prueba de los planes de continuidad y una frecuencia para su repetición. • Probar los procedimientos de restauración de copias de seguridad de la información sensible. • Evaluar la capacidad de continuidad de los proveedores de servicios externos a la organización, en caso de que existan. • Evaluar la capacidad para desplegar recursos redundantes, localizar recursos y restaurar copias.

Tabla 35 - Métrica R-CS-OE3-01: Probar los planes de continuidad para garantizar que cumplen los objetivos de recuperación.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE3-03**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación a un nivel mínimo aceptable.
Descripción	Esta respuesta se puede medir calculando el tiempo requerido entre el momento en que se produce una interrupción en la provisión del servicio esencial y el instante en que éste vuelve a estar disponible con un **mínimo nivel aceptable de funcionalidad.** Este nivel mínimo aceptable se puede fijar porcentualmente por ejemplo cuando se ha recuperado un 70% de la actividad. Estos indicadores se pueden obtener sumando los tiempos invertidos en el respaldo de los datos desde dependencias externas e internas más los tiempos necesarios para que vuelvan a estar operativos los servicios a un nivel mínimo. Este tiempo hasta alcanzar la recuperación mínima aceptable se puede comparar con el tiempo de recuperación objetivo RTO para evaluar la desviación real y seguir mejorando en el futuro.
Pregunta planteada	¿Se evalúa la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación a un nivel mínimo aceptable?
Correlación	ISO/IEC 27001:2017 [A.17.1.1], [A.17.1.2] NIST SP 800-53 R4 [CP-1], [CP-2], [CP-13], [PM-11] ENS [op.cont.1] Guía contenidos mínimos PPE (4.2) NIS (Directivas 27, 33)
CARACTERIZACIÓN	

Escala	**L0** - No se mide la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo. **L1** - Se ha iniciado la definición del procedimiento para medir la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo. **L2** - Se ha establecido el procedimiento para medir la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo, pero no se ha documentado. **L3** - Se ha documentado el procedimiento para medir la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para medir la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo**.** **L5** - Se aplican acciones de mejora en el procedimiento para medir la respuesta de la organización desde la interrupción del servicio esencial hasta que este se restaura a un nivel de funcionalidad mínimo.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que se dispone, actualiza y mejora un procedimiento para estimar el número de horas entre que se produce una interrupción en la provisión del servicio y este está disponible con un mínimo nivel de funcionalidad.
	Acciones correctivas	Establecer los mecanismos necesarios (tecnológicos, logísticos y físicos) para valorar el tiempo necesario para que el servicio esencial vuelva a estar disponible a un nivel mínimo tras el evento de interrupción. Esto se puede realizar, por ejemplo, apoyándose en los ejercicios de simulación de interrupción del servicio esencial.

Tabla 36 - Métrica R-CS-OE3-03: Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación a un nivel mínimo aceptable.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE4-04**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación completa y funcionamiento normal.
Descripción	Valorar la respuesta de la organización a una interrupción de la provisión del servicio esencial hasta que recupera su funcionalidad **completa** habitual.
Pregunta planteada	¿Se evalúa la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación completa y funcionamiento normal?
Correlación	ISO/IEC 27001:2017 [A.17.1.1], [A.17.1.2] NIST SP 800-53 R4 [CP-1], [CP-2], [CP-13], [PM-11] ENS [op.cont.1] Guía contenidos mínimos PPE (4.2) NIS (Directivas 27, 33)
CARACTERIZACIÓN	
Escala	**L0** - No se ha mide la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual. **L1** – Se ha iniciado la definición del procedimiento para medir la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual. **L2** - Se ha establecido un procedimiento para medir la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual, pero no se ha documentado. **L3** - Se ha documentado el procedimiento para valorar la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual. Se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para valorar la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual. **L5** - Se aplican acciones de mejora en el procedimiento para valorar la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual.

OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que se dispone de un procedimiento, actualizado y optimizado para valorar la respuesta de la organización a una interrupción en la provisión del servicio esencial hasta que recupera su funcionalidad completa habitual.
	Acciones correctivas	Establecer los mecanismos necesarios (tecnológicos, logísticos y físicos) que permitan valorar cómo se ha conseguido recuperar la normalidad del servicio esencial para que éste vuelva a estar disponible de forma completa en el menor tiempo posible pasado el evento de interrupción. Una manera constructiva consiste en registrar los tiempos cuando están ocurriendo los hitos de: interrupción, recuperación mínima del servicio, y recuperación completa del servicio.

Tabla 37 - Métrica R-CS-OE4-04: Evaluar la respuesta de la organización desde la interrupción del servicio esencial hasta su recuperación completa y funcionamiento normal

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE5-02**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Identificar y priorizar las dependencias externas relacionadas con la provisión del servicio esencial.
Descripción	Identificar y priorizar las dependencias externas (dependencias de terceros) de modo que se asegure que la organización dirige sus esfuerzos de ciberresiliencia prioritariamente hacia aquellas que contribuyan en mayor medida, y de forma más directa, a la provisión del servicio esencial. Determinando el impacto en la organización de las dependencias de servicios públicos o de suministros básicos. Por ejemplo servicios de emergencia o sanitarios, proveedores de seguridad física, seguridad lógica, operadores tecnológicos, servicios de *hosting*, servicios en *cloud*, etc.
Pregunta planteada	¿Se identifican y priorizan las dependencias externas relacionadas con la provisión del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.15.1.1], [A.15.1.2], [A.15.1.3] NIST SP 800-53 R4 [PL-8] ENS [op.ext.1] Guía contenidos mínimos PSO (3.4,4.3) Guía contenidos mínimos PPE (3.2,3.3)
CARACTERIZACIÓN	
Escala	**L0** - No se identifican ni priorizan las dependencias externas relacionadas con la provisión del servicio esencial. **L1** - Se ha iniciado la identificación y asignación de prioridades a las dependencias externas relacionadas con la provisión del servicio esencial. **L2** - Se identifican y se asignan prioridades a las dependencias externas relacionadas con la provisión del servicio esencial, pero no se han documentado. **L3** - Se ha documentado un procedimiento para identificar y asignar prioridades a las dependencias externas relacionadas con la provisión del servicio esencial y se mantienen actualizadas. **L4** - Se gestiona, actualiza y revisa el procedimiento para identificar y asignar prioridades a las dependencias externas relacionadas con la provisión del servicio esencial. **L5** - Se aplican acciones de mejora en el procedimiento para identificar y asignar prioridades a las dependencias externas relacionadas con la provisión del servicio esencial.

OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización dispone de una lista priorizada de todas las dependencias externas que afectan al servicio esencial y esa lista es actualizada.
	Acciones correctivas	Establecer unos criterios para identificar y priorizar las dependencias externas. Mantener los criterios y prioridades documentados, actualizados y revisarlos periódicamente.

Tabla 38 - Métrica R-CS-OE5-02: Identificar y priorizar las dependencias externas relacionadas con la provisión del servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE6-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Identificar y gestionar los riesgos asociados a dependencias externas.
Descripción	Identificar y gestionar adecuadamente los riesgos asociados a las dependencias externas que contribuyen, directa o indirectamente, a la provisión del servicio esencial. Priorizar y actualizar los riesgos identificados.
Pregunta planteada	¿Se identifican y gestionan adecuadamente los riesgos asociados a las dependencias externas relacionadas con la provisión del servicio esencial?
Correlación	ISO/IEC 27001: 2013 [A.15.1.1], [A.15.1.2], [A.15.1.3] NIST SP 800-53 R4 [SA-21], [SC-38] ENS [op.ext.1] Guía contenidos mínimos PSO (3.4,4.3) Guía contenidos mínimos PPE (3.2,3.3)
CARACTERIZACIÓN	
Escala	**L0** - No se realiza una gestión de riesgos asociados a dependencias externas. **L1 -** Se ha iniciado la gestión de riesgos asociados a dependencias externas. **L2** - Se ha establecido una gestión de riesgos asociados a dependencias externas, pero no se han documentado. **L3** - Se ha documentado la gestión de riesgos asociados a dependencias externas y se mantiene actualizada. **L4** - Se gestionan, actualizan y verifican los riesgos asociados a dependencias externas. **L5** - Se aplican acciones de mejora en la gestión de riesgos asociados a dependencias externas.
OBTENCIÓN	
Método de recogida	Manual
Responsable	CSO o CISO
ANÁLISIS	
Medida Objetivo	L5

Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización ha identificado los riesgos asociados a las dependencias externas y que esta lista ha sido priorizada y está actualizada.
	Acciones correctivas	Identificar y evaluar los riesgos debidos a dependencias externas para que puedan ser gestionados eficazmente y así mantener la capacidad de recuperación del servicio esencial que proporciona la organización.

Tabla 39 - Métrica R-CS-OE6-01: Identificar y gestionar los riesgos asociados a dependencias externas.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE7-04**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Establecer acuerdos específicos de ciberresiliencia con aquellos terceros que estén implicados en la provisión del servicio esencial.
Descripción	Se trata de conocer si, para cada dependencia externa (para cada tercero que contribuya directa o indirectamente en la provisión del servicio esencial), la organización ha establecido y documentado un conjunto detallado de los requisitos que aquella ha de cumplir con el fin de dar soporte y mejorar la capacidad de recuperación de las operaciones de la organización. Adicionalmente, se trata de conocer si dichos requisitos han sido recogidos como parte de las cláusulas que conforman los acuerdos de prestación de servicios externalizados, o Acuerdos de Nivel de Servicio (ANS), alcanzados con dichas entidades. Por ejemplo: el tiempo máximo de no disponibilidad de la infraestructura de los servidores o las penalizaciones en caso de incumplimiento.
Pregunta planteada	¿Se incluyen requisitos de ciberresiliencia en los acuerdos con aquellos terceros que contribuyen, directa o indirectamente, a la provisión del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.15.1.1], [A.15.1.2], [A.15.1.3] NIST SP 800-53 R4 [SA-12], [SA-13] ENS [op.ext.1] Guía contenidos mínimos PPE (2.3,3.2) NIS (48, 50, 52, 54, 69)
CARACTERIZACIÓN	

Escala	**L0 -** No se incluyen requisitos de ciberresiliencia en los acuerdos de nivel de servicio con proveedores (dependencias externas). **L1** - Se ha iniciado la inclusión de requisitos de ciberresiliencia en los acuerdos con dependencias externas. **L2** - Se han establecido los requisitos de ciberresiliencia en las relaciones con dependencias externas, pero no se han documentado. **L3** - Se han documentado los requisitos de ciberresiliencia en los acuerdos con dependencias externas y se mantienen actualizados. **L4** - Se gestionan, actualizan y verifican los requisitos de ciberresiliencia en los acuerdos con dependencias externas. **L5** - Se aplican acciones de mejora en los requisitos de ciberresiliencia en los acuerdos con dependencias externas.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización verifica y actualiza requisitos de ciberresiliencia en todos los acuerdos con entidades externas con los que se contratan servicios que dan soporte al servicio esencial.
	Acciones correctivas	Definir, actualizar y revisar los requisitos de ciberresiliencia en los Acuerdos de Nivel de Servicio (ANS) con entidades externas, de modo que: • sean exigibles por la organización; • incluyan especificaciones detalladas y completas de lo que debe cumplirse por la entidad externa; • incluyan los estándares de rendimiento requeridos; • se actualicen cuando sea oportuno y periódicamente, de modo que reflejen los cambios necesarios durante la vigencia de la relación.

Tabla 40 - Métrica R-CS-OE7-04: Establecer acuerdos específicos de ciberresiliencia con aquellos terceros que estén implicados en la provisión del servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**R-CS-OE8-01**
Meta	RECUPERAR
Dominio Funcional	GESTIÓN DE CONTINUIDAD DEL SERVICIO
Objetivo del indicador	Supervisar y gestionar la operación de las dependencias externas.
Descripción	Supervisar y gestionar la operación de las dependencias externas que dan soporte a la provisión del servicio esencial de acuerdo con los requisitos de ciberresiliencia acordados con la organización. Se trata de conocer si se realiza con regularidad una supervisión de las operaciones de los terceros que contribuyen, directa o indirectamente, a la provisión del servicio esencial, de modo que quede verificado el cumplimiento de los requisitos de ciberresiliencia pactados entre las partes. Adicionalmente, ello permitirá conocer si se solucionan los problemas de operación que puedan encontrarse durante la prestación de los servicios externalizados.
Pregunta planteada	Para aquellos terceros que participan, directa o indirectamente en la provisión del servicio esencial, ¿se supervisan y gestionan sus operaciones de acuerdo con los requisitos de ciberresiliencia acordados con la organización?
Correlación	ISO/IEC 27001: 2013 [A.15.2.1] NIST SP 800-53 R4 [AR-4], [SA-3], [SA-9], [SA-12], [SA-13] ENS [op.ext.2] Guía contenidos mínimos PPE (2.3,3.2) NIS (48, 50, 52, 54, 69)
CARACTERIZACIÓN	
Escala	**L0** - No se realiza una supervisión y gestión de la operación de las dependencias externas. **L1** - Se ha iniciado la supervisión y gestión de la operación de las dependencias externas. **L2** - Se ha establecido un procedimiento para la supervisión y gestión de la operación de las dependencias externas, pero no se han documentado. **L3** - Se ha documentado el procedimiento para la supervisión y gestión de la operación de las dependencias externas y se mantiene actualizada. **L4** - Se monitoriza y verifica el procedimiento para la supervisión y gestión de la operación de las dependencias externas. **L5** - Se aplican acciones de mejora en el procedimiento para supervisar y gestionar la operación de las dependencias externas.

OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización monitoriza periódicamente la operación de las dependencias externas que dan soporte al servicio esencial para verificar que cumplen los requisitos de ciberresiliencia establecidos.
	Acciones correctivas	Establecer un procedimiento, que será actualizado y mejorado, para monitorizar periódicamente la operación de las dependencias externas al servicio esencial y analizar las desviaciones respecto de los requisitos de ciberresiliencia establecidos para comprender el impacto potencial sobre la organización.

Tabla 41 - Métrica R-CS-OE8-01: Supervisar y gestionar la operación de las dependencias externas.

2.4. Evolucionar

A continuación, se detallan las fichas para las métricas correspondientes a la meta de Evolucionar.

2.4.1. Gestión de configuración y de los cambios (CC)

El objetivo general de este dominio funcional es establecer procesos que garanticen la integridad de los activos que soportan los servicios esenciales, de modo que cambios en dichos activos afecten lo menos posible a la organización. Sus objetivos específicos son:

- Gestionar el ciclo de vida de los activos críticos que soportan los servicios esenciales.
- Gestionar la integridad de los activos de información y tecnológicos.
- Establecer líneas base de configuración de los activos.

Además, le corresponden el siguiente indicador:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**E-CC-OE2-01**
Meta	EVOLUCIONAR
Dominio Funcional	GESTIÓN DE LA CONFIGURACIÓN Y DE LOS CAMBIOS
Objetivo del indicador	Gestionar la configuración de los activos de información y tecnológicos.
Descripción	Establecer un procedimiento de gestión de la configuración de los componentes y equipos informáticos o tecnológicos asociados al sistema que hace posible la provisión del servicio esencial de forma que se facilite su restablecimiento aceptable, tras un ciberincidente de consecuencias graves. Adicionalmente debe garantizarse una gestión de los cambios en esos mismos componentes y equipos, de manera que se impidan potenciales impactos negativos en la provisión del servicio esencial debidos a dichos cambios.
Pregunta planteada	¿Se sigue un procedimiento de gestión de configuración de los equipos asociados al sistema que hace posible la provisión del servicio esencial?
Correlación	ISO/IEC 27001:2017 [A.12.1.2] NIST SP 800-53 R4 [CM-1], [CM-2], [CM-3], [CM-6], [CM-9], [SA-5], [SA-10] ENS [op.exp.2] Guía contenidos mínimos PPE (4.2.3)
CARACTERIZACIÓN	

Escala	**L0** - No existe ningún procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos. **L1** - Se ha iniciado el establecimiento de un procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos. **L2** - Se ha establecido el procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos, pero no se ha documentado. **L3** - Se ha documentado el procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos, y este se mantiene actualizado. **L4** - Se gestiona, actualiza y revisa el procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos. **L5** - Se aplican acciones de mejora en el procedimiento de gestión de la configuración de los equipos informáticos y tecnológicos.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización lleva a cabo la gestión de la configuración de los equipos informáticos y tecnológicos que soportan los servicios esenciales. Esto proporciona un nivel de control para evitar alterar el soporte que da a los servicios esenciales. El procedimiento debe garantizar el restablecimiento del servicio, de forma aceptable, tras un ciberincidente de consecuencias graves.

	Acciones correctivas	• Establecer un procedimiento de gestión de configuración de los activos tecnológicos que dan soporte al servicio esencial. • Identificar e informar a los responsables implicados en la gestión del cambio. • Evaluar los requisitos de ciberresiliencia que provocan los cambios realizados en los activos que soportan los servicios esenciales (información, tecnología, instalaciones). • Implementar mecanismos para detectar cambios en los activos tecnológicos, ya sea a nivel de políticas y procedimientos, técnicos (software de gestión de cambios), o físicos (inspecciones y auditorías).

Tabla 42 - Métrica E-CC-OE2-01: Gestionar la configuración de los activos de información y tecnológicos.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**E-CC-OE2-06**
Meta	EVOLUCIONAR
Dominio Funcional	GESTIÓN DE LA CONFIGURACIÓN Y DE LOS CAMBIOS
Objetivo del indicador	Probar los cambios en los activos tecnológicos antes de pasar a producción.
Descripción	Los cambios aplicados en los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios. La fase de producción es una de las más importantes, puesto que soporta la operación de activos que intervienen en la provisión del servicio esencial. La revisión técnica de las aplicaciones antes de cambios en la plataforma de operación es sumamente importante para asegurar degradaciones o interrupciones del servicio esencial. Cada vez que se identifique un cambio que afecte a los activos de producción (integración de un nuevo componente, modificación de la configuración, o eliminación de un activo), se deberían diseñar y ejecutar el conjunto de pruebas para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización, antes de efectuar el cambio.
Pregunta planteada	¿Se prueban los cambios en los activos tecnológicos antes de pasar a producción?
Correlación	ISO/IEC 27001:2017 [A.12.1.2], [A.12.1.4] , [A.14.2.9], [A.14.2.2], [A.14.2.3] NIST SP 800-53 R4 [CM-1], [CM-2], [CM-3], [CM-6], [CM-9], [SA-5], [SA-10] ENS [op.pl.3], [op.exp.3], [op.exp.4] [op.exp.5] Guía contenidos mínimos PPE (4.2.3)
CARACTERIZACIÓN	

Escala	**L0** - No existe ningún procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción. **L1** - Se ha iniciado el establecimiento de un procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción. **L2** - Se ha establecido el procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción, pero no se ha documentado. **L3** - Se ha documentado el procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción, y este se mantiene actualizado. **L4** - Se gestiona, actualiza y revisa el procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción. **L5** - Se aplican acciones de mejora en el procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización lleva a cabo un procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción. Esto proporciona un nivel de control para evitar alterar el soporte que da a los servicios esenciales. El procedimiento debe garantizar que el sistema funciona perfectamente en presencia de los nuevos cambios en los activos.
	Acciones correctivas	• Establecer un procedimiento para probar los cambios en los activos tecnológicos antes de pasar a producción. • Establecer un entorno de preproducción similar al de producción donde validar la integración de los cambios y la estabilidad del entorno. • Identificar y documentar las pruebas pertinentes (rendimiento, consumo, seguridad, etc.) y los responsables de ejecutarlas.

Tabla 43 - Métrica E-CC-OE2-06: Probar los cambios en los activos tecnológicos antes de pasar a producción.

2.4.2. Comunicación (CM)

El objetivo general de este dominio funcional es establecer procesos que garanticen la comunicación entre responsables involucrados en la operación de los servicios esenciales, tanto internos como externos a la organización. Sus objetivos específicos son:

- Establecer mecanismos de comunicación, internos y externos a la organización.
- Garantizar la disponibilidad de los medios de comunicación.
- Comunicar la estrategia de continuidad a toda la organización.
- Comunicar problemas, debilidades, y cambios.

Además, le corresponden los siguientes indicadores:

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**E-CM-OE1-02**
Meta	EVOLUCIONAR
Dominio Funcional	COMUNICACIÓN
Objetivo del indicador	Establecer mecanismos de comunicación externos a la organización en materia de ciberresiliencia.
Descripción	Definir y establecer mecanismos de comunicación externa en materia de ciberresiliencia con entre otros: clientes, proveedores, medios de comunicación, Fuerzas y Cuerpos de Seguridad del Estado, servicios de emergencia, etc. Debe evaluarse si estos mecanismos resultan eficaces y si se emplean con regularidad.
Pregunta planteada	¿Se han definido y establecido mecanismos eficaces de comunicación externa en materia de ciberresiliencia? Por ejemplo, con clientes, proveedores, medios de comunicación, Fuerzas y Cuerpos de Seguridad del Estado o servicios de emergencia.
Correlación	NIST SP 800-53 R4 [IR-7], [SA-9] Guía contenidos mínimos PSO (2.2.1, 2.2.4) Guía contenidos mínimos PPE (2.1, 2.3, 4.2.1)
CARACTERIZACIÓN	

Escala	**L0** - No se establece ninguna comunicación con entidades externas en materia de ciberresiliencia. **L1** - Se ha iniciado la comunicación con entidades externas en materia de ciberresiliencia. **L2** - Se han establecido mecanismos de comunicación con entidades externas en materia de ciberresiliencia, pero no se han documentado. **L3** - Se han documentado en un procedimiento los mecanismos de comunicación con entidades externas en materia de ciberresiliencia y se mantienen actualizados. **L4** - Se gestiona, actualiza y verifica el procedimiento para la comunicación con entidades externas en materia de ciberresiliencia. **L5** - Se aplican acciones de mejora en el procedimiento para la comunicación con entidades externas en materia de ciberresiliencia.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización establece procedimientos, los actualiza y mejora, para gestionar los mecanismos en materia de comunicación externa de manera formal y regular con, entre otros: clientes, proveedores, medios de comunicación, Fuerzas y Cuerpos del Estado, servicios de emergencia, etc.
	Acciones correctivas	• Establecer mecanismos eficaces de comunicación externa a través de los canales habilitados. • Crear las buenas prácticas para comunicar los ciberincidentes.

Tabla 44 - Métrica E-CM-OE1-02: Establecer mecanismos de comunicación externos a la organización en materia de ciberresiliencia.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**E-CM-OE2-02**
Meta	EVOLUCIONAR
Dominio Funcional	COMUNICACIÓN
Objetivo del indicador	Garantizar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial.
Descripción	El objetivo es garantizar que, en caso de interrupción, los mecanismos necesarios para establecer las comunicaciones oportunas con los actores que sean necesarios para recuperar la provisión del servicio esencial existen y funcionan. Se trata de verificar, por ejemplo, que se puede comunicar el incidente a quién corresponda para su resolución. En todo caso existirán canales de comunicación alternativos en el caso de que fallen los habituales que ofrecen las mismas garantías de protección de la comunicación que el canal habitual; y garantizan un tiempo máximo de entrada en funcionamiento.
Pregunta planteada	¿Se ha verificado la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial?
Correlación	NIST SP 800-53 R4 CP-2(2)[2] , CP-8, SC-1 ENS [mp.com.9] Guía contenidos mínimos PSO (2.2.1, 2.2.4) Guía contenidos mínimos PPE (2.1, 4.2.1)
CARACTERIZACIÓN	

Escala	**L0** - No se verifica la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial. **L1** - Se han iniciado las pruebas para la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial. **L2** - Se ha establecido un procedimiento para verificar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial, pero no se ha documentado. **L3** - Se ha documentado un procedimiento para verificar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para verificar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial. **L5 -** Se aplican acciones de mejora en el procedimiento para verificar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial.	
OBTENCIÓN		
Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización tiene un procedimiento para verificar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial. Por ejemplo se comprueba que se puede comunicar el ciberincidente a quién corresponda, en caso de interrupción de la operación normal de los servicios esenciales.

	Acciones correctivas	• Establecer un procedimiento para verificar que se puede comunicar el ciberincidente a quién corresponda en caso de interrupción de la operación normal del servicio esencial para el cual estamos haciendo la encuesta. • Probar las capacidades de comunicación a utilizar en caso de interrupción de la operación normal de los servicios esenciales. • Verificar que los problemas potenciales o reales, y las debilidades detectadas se comunican de manera oportuna para evitar una mayor ocurrencia de los mismos.

Tabla 45 - Métrica E-CM-OE2-02 Garantizar la disponibilidad de los canales de comunicación internos o externos requeridos por el servicio esencial.

CAMPO	INFORMACIÓN
IDENTIFICACIÓN	
Código	**E-CM-OE3-02**
Meta	EVOLUCIONAR
Dominio Funcional	COMUNICACIÓN
Objetivo del indicador	Comunicar la estrategia de continuidad a toda la organización.
Descripción	Se trata de conocer si las delegaciones de autoridad y asignaciones de responsabilidad (tanto internas como externas) que hayan podido establecerse en el marco del programa de ciberresiliencia se han realizado con la publicidad y transparencia requeridas, a fin de que todo el personal involucrado en el programa conozca su papel particular y reconozca en quién o quiénes recae la autoridad en cada momento**.**
Pregunta planteada	El plan de continuidad del servicio esencial, ¿recoge la asignación de las respectivas delegaciones de autoridad y comunica estas responsabilidades a todos los implicados (tanto internos como externos)?
Correlación	ISO/IEC 27001:2017 [A.17.1.3] NIST SP 800-53 R4 [CP-2(a)(3)], [CP-3] ENS [op.cont.2] Guía contenidos mínimos PSO (2.2.1) Guía contenidos mínimos PPE (4.2, 4.2.2)
CARACTERIZACIÓN	
Escala	**L0 -** No se asignan y comunican las responsabilidades al personal implicado en los planes de continuidad. **L1** - Se ha iniciado la asignación y comunicación de responsabilidades al personal implicado en los planes de continuidad. **L2** - Se ha establecido un procedimiento para asignar y comunicar las responsabilidades al personal implicado en los planes de continuidad, pero no se han documentado. **L3** - Se ha documentado el procedimiento para asignar y comunicar las responsabilidades al personal implicado en los planes de continuidad y se mantiene actualizado. **L4** - Se gestiona, actualiza y verifica el procedimiento para asignar y comunicar las responsabilidades al personal implicado en los planes de continuidad. **L5** - Se aplican acciones de mejora en el procedimiento para asignar y comunicar las responsabilidades al personal implicado en los planes de continuidad.
OBTENCIÓN	

Método de recogida	Manual	
Responsable	CSO o CISO	
ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización garantiza la asignación y comunicación de responsabilidades y autoridades dentro del Plan de Continuidad a todo el personal implicado, tanto interno como proveedores implicados, con el objetivo de que conozca sus funciones y responsabilidades.
	Acciones correctivas	• Establecer, verificar y mejorar un procedimiento para la asignación y comunicación de responsabilidades y autoridades dentro del Plan de Continuidad a todo el personal implicado. • Garantizar la comunicación de responsabilidades y autoridades dentro del plan de continuidad a todo el personal implicado, que conoce sus funciones y responsabilidades. • Garantizar que la estrategia de continuidad es comunicada y entendida dentro de la organización, así como la importancia de cumplir con dicha estrategia. • Comprobar que los cambios o variaciones de requisitos legales son comunicados a los empleados y otras partes interesadas.

Tabla 46 - Métrica E-CM-OE3-02: Comunicar la estrategia de continuidad a toda la organización.

3. Acrónimos

BIA: *Business Impact Analysis*.
CISO: *Chief Information Security Officer*.
CSO: *Chief Security Officer*.
CVSS: *Common Vulnerability Score System*.
ENS: Esquema Nacional Seguridad.
ISO: *International Organization for Standardization*.
MTD: *Maximum Tolerable Downtime*.
NIST: *National Institute of Standards and Technology*.
PPE: Planes de Protección Específicos.
PSO: Planes de Seguridad del Operador.
RPO: Punto objetivo de recuperación, del inglés *Recovery Point Objetive*.
RTO: Tiempo objetivo de recuperación, del inglés *Recovery Time Objetive.*

4. Referencias

- CNPIC. Guía de buenas prácticas - Plan de protección específico (PPE)
  http://www.cnpic.es/Biblioteca/Noticias/GUIA_BUENAS_PRACTICAS_PPE.pdf

- CCN (2018). Guía de Seguridad de las TIC CCN-STIC 817
  https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

- CCN (2017). Guía de Seguridad de las TIC CCN-STIC 803
  https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html

- INCIBE (2020). Guía Nacional de Notificación y Gestión de Ciberincidentes
  https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

- NIST. *Special Publication* 800-53 Rev.4
  https://nvd.nist.gov/800-53

- AENOR (2017). UNE-EN ISO: 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.
  https://www.iso.org/isoiec-27001-information-security.html
  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058428

- ISO (2018). ISO/IEC 27005:2018 *Information technology – Security techniques – Information security risk management*
  https://www.aenor.com/normas-y-libros/buscador-de-normas/ISO?c=075281

- AENOR (2018). UNE ISO: 31000:2018 Gestión del riesgo. Directrices
  https://www.iso.org/iso-31000-risk-management.html
  https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0059900

- ISO (2015). ISO/TS 22317:2015 *Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)*
  https://www.aenor.com/normas-y-libros/buscador-de-normas/iso?c=050054

- España. BOE. Código de Derecho de la Ciberseguridad

  https://www.boe.es/legislacion/codigos/codigo.php?id=173&modo=1&nota=0&tab=2

  Incluye (entre otros):

  - España (2017). **Estrategia de Seguridad Nacional**.
  - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la **protección de las infraestructuras críticas**.
  - 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.
  - Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los **Planes de Seguridad del Operador y de los Planes de Protección Específicos**.
  - Real Decreto-ley 12/2018, de 7 de septiembre, de **seguridad de las redes y sistemas de información**.

- UE (2016). Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

  https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA&toc=OJ:L:2016:194:TOC

- España (2019). Guía nacional de Notificación y gestión de ciberincidentes

  http://www.interior.gob.es/documents/10180/9814700/Gu%C3%ADa+Nacional+de+notificaci%C3%B3n+y+gesti%C3%B3n+de+ciberincidentes/f01d9ed6-2e14-4fb0-b585-9b0df20f2906

incibe cert_

GOBIERNO DE ESPAÑA

VICEPRESIDENCIA TERCERA DEL GOBIERNO

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD