Índice de Contenidos

	Fecha: 04012023 **Ref.:** NOR-020 **Ed.rev.:** 1.1 **Asunto:** Normativa de gestión del proceso de autorizaciones **Destinatario:** Entidades adheridas al Marco de Certificación conjunto del CIT

Fecha	Edición.Revisión	Cambios Realizados
19-07-2021	0.1	Borrador inicial del documento
01-09-2021	1.0	Revisión con CIT y versión definitiva
04-01-2023	1.1	Actualización referencias ENS (RD 311/2022)

	Fecha: 04012023 **Ref.:** NOR-020 **Ed.rev.:** 1.1 **Asunto:** Normativa de gestión del proceso de autorizaciones **Destinatario:** Entidades adheridas al Marco de Certificación conjunto del CIT

	Fecha: 04012023 **Ref.:** NOR-020 **Ed.rev.:** 1.1 **Asunto:** Normativa de gestión del proceso de autorizaciones **Destinatario:** Entidades adheridas al Marco de Certificación conjunto del CIT

Objeto

El objeto del presente documento es establecer las pautas que cada uno de los ayuntamientos de la Isla de Tenerife (en adelante, **el Ayuntamiento**) adheridos al Marco de Gobernanza Insular de Seguridad de la Información, promovido y asistido por el Cabildo de Tenerife debe seguir para que los usuarios/as soliciten autorización de acceso a todos aquellos recursos que lo necesiten, dentro del alcance del Esquema Nacional de Seguridad.

Se ha implantado la presente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de las Entidades, que resulten de la aplicación de las previsiones siguientes contempladas en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS):

- ENS Anexo II – Medidas de Seguridad – Marco organizativo:
  - Proceso de autorización [org.4]

Los requisitos que se recogen en la guía CCN-STIC 808 Verificación y cumplimiento del ENS son**:**

Org.4

Categoría	Requisito	Evidencia
Básica	Existe un proceso formal para las autorizaciones respecto a los sistemas de información.	La normativa de seguridad contempla, para cada tipo de componente o actuación, la persona o punto de contacto para su autorización. Existe un modelo de solicitud (formulario) en cualquier formato que contiene: Descripción del elemento (componente) o actuación para la que se solicita la autorización, las actividades para las que se requiere el nuevo componente (motivación), el tiempo para el que se solicita la autorización (que puede ser temporal o permanente), justificación de que no afecta a otras funcionalidades del sistema, un análisis de riesgo conforme a la categoría del sistema (si el nuevo componente introduce posibles vulnerabilidades), justificación de que no viola ninguna normativa de seguridad, información de los procedimientos que son de aplicación, así como de la necesidad de desarrollar nuevos si fuese necesario.
	Cubre la utilización de instalaciones, tanto habituales como alternativas.	La normativa contempla el proceso de autorización de utilización de instalaciones (p. ej.: acceso al CPD, uso de un local alternativo para los servidores de respaldo ante desastres, etc.), que cubre los requisitos antes indicados. Existe evidencia

		documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable pertinente antes de su entrada en explotación.
	Cubre la entrada de equipos en producción, en particular, equipos que involucren criptografía.	La normativa contempla el proceso de autorización de entrada de equipos en producción, que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre la entrada de aplicaciones en producción.	La normativa contempla el proceso de autorización de entrada de aplicaciones en producción (p. ej.: actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre el establecimiento de enlaces de comunicaciones con otros sistemas.	La normativa contempla el proceso de autorización de enlaces de comunicaciones con otros sistemas (p. ej.: para el intercambio de expedientes entre un organismo y otro), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre la utilización de medios telemáticos de comunicación (tanto habituales como alternativos)	La normativa contempla el proceso de autorización de utilización de medios de comunicación (p. ej.: uso de una línea de datos para el acceso a Internet), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre la utilización de soportes de información	La normativa contempla el proceso de autorización de utilización de soportes de información (p. ej.: cintas de backup, DVD, memorias USB, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre la utilización de equipos móviles	La normativa contempla el proceso de autorización de utilización de equipos móviles (p. ej.: ordenadores portátiles, PDA u otros de naturaleza análoga), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de

		solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.
	Cubre la utilización de servicios de terceros, bajo contrato o Convenio	La normativa contempla el proceso de utilización de servicios de terceros (p. ej.: gestión de incidentes, gestión del servicio, desarrollo, infraestructura, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.

Alcance

Este documento aplicará y será de obligado cumplimiento para los ayuntamientos de la Isla de Tenerife adheridos al Marco de Gobernanza Insular de Seguridad de la Información, promovido y asistido por el Cabildo de Tenerife en relación con todos los sistemas de información que éste les preste.

Este procedimiento es de obligado cumplimiento para todo el personal que acceda a los sistemas de información TIC, así como a la propia información gestionada por los diferentes organismos en cualquiera de sus formas y formatos. Aplica con independencia de cuál sea la relación o adscripción con el mismo.

Legislación y normativa aplicable

Las referencias tenidas en cuenta para la redacción de esta normativa han sido las indicadas en el documento marco: NOR-000: Legislación y Normativa Aplicable.

Roles y responsabilidades

Responsable de Seguridad del Ayto.	• Elaborar la normativa de gestión de autorizaciones.
Comité de Seguridad Insular	• Aprobar la normativa de gestión de autorizaciones.
Usuario	• Cumplir con la normativa de gestión de autorizaciones.

**Los roles concretos serán los definidos en el Marco de Gobernanza Insular de Seguridad de la Información para la Isla de Tenerife en función del ámbito concreto de aplicación*.

	Fecha: 04012023 **Ref.:** NOR-020 **Ed.rev.:** 1.1 **Asunto:** Normativa de gestión del proceso de autorizaciones **Destinatario:** Entidades adheridas al Marco de Certificación conjunto del CIT

Normativa de Gestión de Autorizaciones

Características generales

Los sistemas de información no deben admitir elementos que no hayan sido previamente autorizados puesto que su libre incorporación quebrantaría de raíz la confianza en el sistema, al modificar la superficie de ataque y dar pie a nuevas vulnerabilidades susceptibles de ser explotadas.

Es por ello que el Ayuntamiento debe garantizar la seguridad, utilidad y acceso adecuado a todos los recursos y sistemas que éste gestione, evitando intrusiones no autorizadas que perjudiquen la actividad profesional y avalen la seguridad del Ayuntamiento.

El ENS indica que se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

a. Utilización de instalaciones, habituales y alternativas (CPD, uso de un local alternativo para los servidores de respaldo ante desastres, etc.);
b. Entrada de equipos en producción, en particular, equipos que involucren criptografía;
c. Entrada de aplicaciones en producción (actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.);
d. Establecimiento de enlaces de comunicaciones con otros sistemas;
e. Utilización de servicios de terceros, bajo contrato o Convenio (gestión de incidentes, gestión del servicio, desarrollo, infraestructura, etc.).
f. Utilización de medios de comunicación, habituales y alternativos y/o terminales móviles;
g. Utilización de soportes de información (cintas de backup, DVD, memorias USB, etc);

Responsables de autorizar

La asignación de responsabilidades en esta materia la realizará el Responsable de Seguridad del Ayuntamiento.

Los Administradores de Seguridad serán las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

La figura de Administrador de la Seguridad del Sistema coincidirá con la de Responsable de Sistemas del Ayuntamiento, que, respecto al objeto de la presente normativa, serán aquellas personas responsables de gestionar las autorizaciones concedidas a los usuarios del sistema, los privilegios concedidos a los mismos, así como los cambios de configuración de dichas autorizaciones.

Mecanismo de autorización

A) Escenario 1: Para la autorización de los siguientes casos:

a. Utilización de instalaciones, habituales y alternativas (CPD, uso de un local alternativo para los servidores de respaldo ante desastres, etc.);

b. Entrada de equipos en producción, en particular, equipos que involucren criptografía;

c. Entrada de aplicaciones en producción (actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.);

d. Establecimiento de enlaces de comunicaciones con otros sistemas;

e. Utilización de servicios de terceros, bajo contrato o Convenio (gestión de incidentes, gestión del servicio, desarrollo, infraestructura, etc.).

Los usuarios realizarán la solicitud, al Responsable de Sistemas del Ayuntamiento. Se realizará a través de correo electrónico, remitiendo el formulario que consta en el Anexo siguiendo el canal habitual de comunicación. Éste tramitará su solicitud bajo el procedimiento general.

La solicitud realizada deberá contener los siguientes datos (siempre que puedan ser aportados. En caso contrario, podrá consultarse al Responsable de Seguridad del Ayuntamiento por los mismos):

- Descripción precisa del elemento o actuación para el que se solicita autorización,
- Descripción precisa de las actividades para las que se requiere el nuevo componente,
- Justificación de que nuevo componente no afecta a otras funcionalidades del sistema,
- Si el nuevo componente introduce posibles vulnerabilidades (es decir, si expone al sistema a nuevas o renovadas amenazas), deberá anexarse un análisis de riesgos y las medidas que se toman para gestionarlo; este análisis de riesgos tendrá la intensidad proporcionada a la categoría del sistema,
- Justificación de que no se viola ninguna normativa de seguridad,
- Información de los procedimientos de seguridad que son aplicables al caso o, si fuere necesario, la necesidad de desarrollar algún nuevo procedimiento específico.

Por último, se dará por culminado el procedimiento de autorización con la aprobación del Responsable de Seguridad del Ayuntamiento con una firma electrónica, siempre previa a la actuación del usuario.

B) Escenario 2: Para la autorización de los siguientes casos:

e. Utilización de medios de comunicación, habituales y alternativos y/o terminales móviles;

f. Utilización de soportes de información (cintas de backup, DVD, memorias USB, etc);

El responsable correspondiente autorizará y solicitará por correo-e a informática del ayuntamiento (Responsable de Sistemas del Ayuntamiento) el recurso correspondiente indicando:

- Descripción precisa del elemento o actuación para el que se solicita autorización,
- Descripción precisa de las actividades para las que se requiere el nuevo componente

Por último, se dará por culminado el procedimiento de autorización con la aprobación del Responsable de Sistemas del Ayuntamiento, autorizando por correo-e y tratando la petición a continuación. La evidencia del procedimiento se guardará en el buzón de correo-e de informática del ayuntamiento.

Anexo

FORMULARIO DE SOLICITUD DEL PROCESO DE AUTORIZACIONES	
Descripción del elemento o actuación para la que se solicita autorización:	
Actividades para las que se requiere el nuevo componente:	Justificación de que nuevo componente no afecta a otras funcionalidades del sistema:
*** Si el nuevo componente introduce posibles vulnerabilidades, anexar un análisis de riesgos y las medidas que se toman para gestionarlo.**	
Justificación de que no se viola ninguna normativa de seguridad:	
Información de los procedimientos de seguridad que son aplicables al caso o, si fuere necesario, la necesidad de desarrollar algún nuevo procedimiento específico:	

	Fecha: 04012023 **Ref.:** NOR-020 **Ed.rev.:** 1.1 **Asunto:** Normativa de gestión del proceso de autorizaciones **Destinatario:** Entidades adheridas al Marco de Certificación conjunto del CIT

Solicitante:	Autorizante: