POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FIRMAS

	FECHA	FIRMA
ELABORADO POR: SISTEMAS / SECRETARÍA	**16/04/2024**	
APROBADO POR: PLENO		

VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
2.0	**25/04/2024**		**Aprobación de la política**

ÍNDICE

1. INTRODUCCIÓN

El Ayuntamiento de Barañain depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y la valoración de su coste, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

1.1 PRINCIPIOS BÁSICOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Ayuntamiento para conformar un todo coherente y eficaz.
- **Responsabilidad diferenciada:** En los sistemas TIC se diferenciará la persona responsable de la información y servicio, que determina los requisitos de seguridad de la información tratada y los requisitos de seguridad de los servicios prestados; la persona responsable del sistema, que tiene la responsabilidad sobre la explotación tecnológica de la información y los servicios, la persona responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

1.2 OBJETIVOS DE LA SEGURIDAD

El Ayuntamiento de Barañáin establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la **calidad** y protección de la información.
- Lograr la plena **concienciación** de las personas usuarias respecto a la seguridad de la información.
- **Gestión de activos de información:** Los activos de información se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- **Seguridad ligada a las personas:** Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- **Seguridad física:** Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- **Seguridad en la gestión de comunicaciones y operaciones:** Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- **Control de acceso:** Se limitará el acceso a los activos de información por parte de las personas usuarias, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- **Gestión de los incidentes de seguridad:** Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- **Garantizar la prestación continuada de los servicios:** Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios/as.
- **Protección de datos de carácter personal:** Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento, para cumplir la legislación de seguridad y privacidad.
- **Cumplimiento:** Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

2. MISIÓN

El Ayuntamiento de Barañain, para la gestión de sus intereses y de las funciones y competencias que tiene atribuidas en diferentes normas o convenios, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. Para ello pone a disposición de esta la realización de trámites online con el objetivo de impulsar la tramitación electrónica de los procedimientos administrativos, la mejora en la prestación de los servicios y la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la mejora de la eficacia y eficiencia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son:

fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

3. ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Barañain, que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS).

Esta política de seguridad es de obligado cumplimiento para todo el personal que acceda a los sistemas de información TIC del Ayuntamiento de Barañáin, 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.

4. ESTRUCTURA Y DESARROLLO DE LA POLÍTICA DE SEGURIDAD

La estructura jerárquica de la documentación de seguridad es la siguiente:

Política:

- Define las metas y expectativas de seguridad.
- Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos.
- Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.

Normativa:

- Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema.
- Es de carácter obligatorio.
- Debe ser escrita por personas expertas en la materia o por la persona Responsable de Seguridad y aprobada por el Comité de Seguridad.

Procedimiento:

- Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución.
- Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar.
- Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad.
- Debe ser elaborado por la persona Responsable del Sistema y aprobado por la persona Responsable de Seguridad.

Instrucciones técnicas:

- Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.).
- Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar.
- Una instrucción técnica debe ser clara y sencilla de interpretar.
- Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución.
- Pueden ser elaborados por la persona Responsable del Sistema o Administración del Sistema y deben ser aprobados por la persona Responsable de Seguridad.

Guías:

- Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad.
- Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.
- Deben ser aprobadas por la persona Responsable de Seguridad.

Otros Documentos, Registros: Además de los documentos citados, la documentación de seguridad podrá contar con otros adicionales, como son: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, presentaciones, etc.

5. MARCO NORMATIVO

El marco legal en materia de seguridad de la información en que se desarrollan las actividades de las Entidades en el ámbito de la prestación de los servicios electrónicos a las personas beneficiarias, viene establecido por el “Registro de Normas Jurídicas del Marco Legal y Regulatorio” (REG-001) aprobado por el Comité de Seguridad y que se mantendrá actualizado por el responsable de Seguridad.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Barañain derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política, entre otras.

6. MODELO DE GOBERNANZA

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información adaptada a las necesidades y

particularidad de este Ayuntamiento, se propone una designación de roles por bloques de responsabilidad: Gobierno, Supervisión y Operación.

De acuerdo con esta estructura, se han asignado las siguientes responsabilidades y funciones de seguridad:

- **Responsable de Gobierno,** cuyas funciones ejercita la Alcaldía-Presidencia del Ayuntamiento, que integra los siguientes roles y funciones ENS:
    - Responsable de la Información.
    - Responsable del Servicio.

  La Alcaldía-Presidencia puede delegar estos roles y/o funciones en un concejal o concejales.
- **Responsable de Supervisión,** cuyas funciones ejercita la secretaria del Ayuntamiento, y que integra el siguiente rol ENS:
    - Responsable de la Seguridad.

  Por otro lado, se considerará la figura del delegado/a de Protección de Datos, apoyando al responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos, que según la normativa es de obligada designación en las administraciones públicas, el nombramiento se ha realizado por el Ayuntamiento entre personal designado por el mismo o por medio de prestación por medio de contrato de servicios.
- **Responsable de Operación**, cuyas competencias ejercita el área de informática del Ayuntamiento y que integra el siguiente rol ENS:
    - Responsable del Sistema.

El Comité de Seguridad de la información estará formado por todos los miembros de los distintos bloques.

6.1 RESPONSABILIDADES ASOCIADAS AL ENS

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del responsable de la Información y de los Servicios:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del responsable de Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.

- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del Sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

Funciones del responsable del Sistema:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios/as del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

6.2 FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones propias de un Comité de Seguridad de la Información son las siguientes:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

6.3 PROCEDIMIENTOS DE DESIGNACIÓN

La designación de los responsables identificados en esta Política ha sido realizada por Alcaldía-Presidencia del Ayuntamiento de Barañain y comunicada a las partes afectadas.

Los roles de seguridad serán revisados cada cuatro años, en el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

7. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

El órgano superior competente deberá aprobar los cambios sobre la Política de Seguridad de la Información, según el artículo 11 del ENS.

Cualquier cambio sobre esta se difundirá a todas las partes afectadas.

8. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Barañain, en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

9. GESTIÓN DE RIESGOS

9.1 JUSTIFICACIÓN

Todos los sistemas sujetos a esta Política deberán someterse a un **análisis de riesgos**, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

9.2 CRITERIOS DE EVALUACIÓN DE RIESGOS

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que se elaborará, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios establecidos en el alcance.

9.3 PROCESO DE ACEPTACIÓN DEL RIESGO RESIDUAL

Los riesgos residuales serán determinados por la persona Responsable de Seguridad y serán presentados al Comité de Seguridad, para que proceda, en su caso a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

10. TERCERAS PARTES

Cuando se presten servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento de Barañain definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de

seguridad, así como el resto de las actuaciones que el Ayuntamiento lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de Barañain utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por los responsables de información y los servicios, con carácter previo al inicio de la relación con la tercera parte.