Ayuntamiento de Burgos

Política de Seguridad de la Información del Ayuntamiento de Burgos

Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad

Esquema Nacional de Seguridad

Ayuntamiento de Burgos

Política de Seguridad de la Información del Ayuntamiento de Burgos
Esquema Nacional de Seguridad

Última Modificación:	22 de diciembre de 2022
Modificaciones:	Realizadas adecuaciones por cambios normativos debidos a la entrada en vigor de un nuevo Esquema Nacional de Seguridad según RD 311/2022 de 3 de Mayo. Se ha revisado la calificación de la información y la responsabilidades y funciones de los distintos roles.
Versión:	Versión 2
Clasificación:	Pública
Documento:	Política de Seguridad del Ayuntamiento de Burgos

Ayuntamiento de Burgos

Índice

Ayuntamiento de Burgos

1. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la Información fue aprobada inicialmente el 4 de marzo de 2021 y posteriormente modificada por la Junta de Gobierno Local del Ayuntamiento de Burgos con fecha 29 de diciembre de 2022.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea remplazada por una nueva Política, sin perjuicio de los cambios o modificaciones que se realicen sobre la misma.

Ayuntamiento de Burgos

2. INTRODUCCIÓN

El Ayuntamiento de Burgos (en adelante, el Ayuntamiento) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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 calidad 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 todas las áreas del Ayuntamiento 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.

Las diferentes Concejalías, áreas de gobierno o departamentos del Ayuntamiento 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 las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Todas las Concejalías, áreas de gobierno y departamentos del Ayuntamiento deben estar preparadas para cumplir con sus objetivos utilizando sistemas de información, por lo que deben asegurarse de que se cumplen en todo momento los principios básicos establecidos en el Esquema Nacional de Seguridad.

Ayuntamiento de Burgos

3. PRINCIPIOS BÁSICOS

Todos los servicios deben estar preparados para cumplir con sus objetivos utilizando sistemas de información, por lo que deben asegurar que se cumplen los siguientes principios:

3.1. SEGURIDAD INTEGRAL

La seguridad de la información será entendida como un proceso integral en el que todos los elementos técnicos, humanos, materiales y organizativos del Ayuntamiento formarán parte de él. En este sentido, se prestará la máxima atención a la formación y concienciación de las personas que intervienen en el proceso de seguridad y concretamente en sus responsables, que deberán recibir formación específica, para que la falta de organización, instrucciones y coordinación no sean una fuente de riesgo para la información manejada por el Ayuntamiento.

El Ayuntamiento formará e informará a todo su personal acerca de los deberes y obligaciones en materia de seguridad y garantizará que la atención, revisión y auditoría de los sistemas de seguridad se llevará a cabo por personal cualificado, bajo criterios de profesionalidad, exigiendo además que las organizaciones que le presten servicios cuenten con profesionales cualificados y con niveles idóneos en la gestión y madurez en los servicios prestados.

3.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

La gestión de los riesgos deberá ser parte fundamental para el proceso de seguridad. El Ayuntamiento, a través de los responsables en materia de seguridad, deberán implementar mecanismos de gestión del riesgo, minimizándolos hasta niveles aceptables mediante el despliegue de medidas de seguridad y buscando el equilibrio entre la naturaleza de la información, los riesgos a los que se expone y las medidas de seguridad a adoptar.

3.3. PREVENCIÓN

Todas las Concejalías, áreas o departamentos del Ayuntamiento deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Ayuntamiento de Burgos

Para garantizar el cumplimiento de la Política de Seguridad, las Concejalías, áreas o departamentos municipales deben:

- Configurar y diseñar los sistemas de información de forma que se garantice la seguridad y protección de datos por defecto.
- Autorizar los sistemas antes de entrar en operación.
- Controlar y limitar los accesos a los sistemas de información atendiendo al mínimo privilegio.
- Conocer el estado de seguridad de los sistemas en relación a especificaciones de fabricantes, vulnerabilidades y actualizaciones que le afecten, reaccionando con diligencia para gestionar el riesgo.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.4. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del Esquema Nacional de Seguridad.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del Esquema Nacional de Seguridad. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan prestablecido como normales.

3.5. RESPUESTA

El Ayuntamiento debe, a través de sus Concejalías y áreas:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Ayuntamiento de Burgos

3.6. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, se desarrollarán Análisis de Impacto y planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de los servicios y actividades de recuperación, incluyendo la copia de seguridad de los sistemas de información.

3.7. EXISTENCIA DE LÍNEAS DE DEFENSA

El Ayuntamiento deberá de disponer de una estrategia de protección formada por múltiples capas de seguridad que permitan reaccionar ante incidentes inevitables; reducir la probabilidad de que el sistema quede comprometido y minimizar el impacto. En este sentido, serán de especial importancia para la seguridad de la información las siguientes cuestiones:

- El acceso a los sistemas de información, que el Ayuntamiento deberá controlar y limitar, así como el registro de las actividades de los usuarios, identificando conductas indebidas o no autorizadas.
- La protección física de las instalaciones, a través de áreas controladas y separadas.
- La adquisición de productos de seguridad que cumplan con las garantías de seguridad necesarias en atención a la categoría de los sistemas y nivel de seguridad de la información.
- Protección de la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, periféricos, soportes de información y comunicaciones.
- Protección de la información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica.
- Protección del perímetro y análisis de los riesgos derivados de la interconexión del sistema con otros sistemas a través de redes.

3.8. REEVALUACIÓN PERIÓDICA Y VIGILANCIA CONTINUA

El Ayuntamiento incluirá el proceso de seguridad en un ciclo de actualización y mejora continua. En este sentido, el Ayuntamiento reevaluará y actualizará las medidas de seguridad periódicamente, adecuando su eficacia a la evolución de los riesgos y sistemas de protección, bien por la aparición o incremento de los riesgos o bien en cumplimiento de la normativa vigente.

3.9. DIFERENCIACIÓN DE RESPONSABILIDADES

A través de la presente Política de Seguridad y la normativa que la desarrolle se definirán los distintos roles intervinientes en el sistema de información, distinguiendo en cualquier caso, entre responsable de la información, el responsable del servicio, el responsable de seguridad y el responsable del

sistema, así como se indicarán las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos, existiendo en todo momento una obligación de cooperación y colaboración entre los distintos roles y responsables.

4. ALCANCE

Esta Política de Seguridad de la información es de aplicación y de obligado cumplimiento para todo el personal del Ayuntamiento, incluyendo todas sus Concejalías, áreas de gobierno, distritos, departamentos y órganos internos, así como será de aplicación y obligado cumplimiento en todos los sistemas de información, servicios, información y procesos del Ayuntamiento.

Del mismo modo, esta Política de Seguridad de la Información será de aplicación y de obligado cumplimiento para todo el personal, sistemas y servicios de los servicios municipalizados del Ayuntamiento, así como al personal de terceros que preste sus servicios al mismo.

5. MISIÓN

5.1. OBJETIVOS Y MISIÓN DEL AYUNTAMIENTO

El Ayuntamiento, para la gestión de sus intereses y en el ámbito de sus competencias, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población de Burgos.

El Ayuntamiento ejerce sus competencias, en los términos previstos en la legislación del Estado y de la Comunidad Autónoma de Castilla y León. Para ejercer las competencias municipales el Ayuntamiento hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

5.2. OBJETIVOS Y MISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Ayuntamiento ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, reconociendo, así como activos estratégicos la información y los sistemas que la soportan.

Ayuntamiento de Burgos

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el asentar las bases sobre las cuales los empleados públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La Política de Seguridad de la Información protege a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Ayuntamiento.

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y objetivos establecidos por el Ayuntamiento.
2. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
3. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
4. Proteger los recursos de información del Ayuntamiento y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

6. MARCO NORMATIVO

El marco que afecta al desarrollo de las actividades y competencias del Ayuntamiento, está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de los datos de naturaleza personal.

Las normas que constituyen dicho marco, se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado, siendo las principales el RD 311/2022 de 3 mayo que regula el Esquema Nacional de seguridad y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

También podrán formar parte del referido marco, aquellas normas aplicables a la Administración Electrónica del Ayuntamiento, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de esta Política.

7. REVISIÓN DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad ha sido aprobada por la Junta de Gobierno Local, consciente de la necesidad de dotar de impulso a la seguridad de la información desde los más altos órganos de dirección del Ayuntamiento.

Esta Política será revisada al menos una vez al año y siempre que se hayan producido cambios relevantes en la organización municipal, con el fin de asegurar que esta se adecua a la estrategia y necesidades de la organización.

La Política será revisada en lo sucesivo por el Comité de Seguridad, quien podrá aprobar nuevas versiones de la Política de Seguridad que no afecten de forma significativa al alcance, misión y objetivos de la misma y para los que no requiera la aprobación por parte de la Junta de Gobierno Local.

El Comité de Seguridad será quien plasmará los cambios necesarios para reflejar el estado actual de la organización y los servicios municipales, además de difundirla para que la conozcan y esté a disposición de todas las partes afectadas.

La resolución de conflictos de intereses y de interpretación de la Política de Seguridad será competencia del Comité de Seguridad.

Ayuntamiento de Burgos

8. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad del Ayuntamiento, se establece partiendo de la identificación de diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información del Ayuntamiento son responsables de la seguridad de la información, así como de los recursos y medios puestos a su disposición para el manejo de dicha información. En ellos recae la responsabilidad de un uso correcto, siempre de acuerdo a las atribuciones profesionales y competencias.

Como extensión a la estructura de seguridad del Ayuntamiento, se establecerán relaciones de cooperación en materia de seguridad con las autoridades competentes, autonómicas o estatales, proveedores de servicios informáticos o de comunicación, así como organismos públicos y privados dedicados a promover la seguridad de los sistemas de información.

8.1. DEFINICIÓN DE ROLES DE SEGURIDAD

A continuación, se identifican los roles que participaran en la Seguridad de la Información del Ayuntamiento:

Rol	Funciones
Junta de Gobierno Local	Es el órgano colegiado que establece la misión y los objetivos de la Organización. Se ocupa del nombramiento de los componentes del Comité de Seguridad.
Comité de Seguridad de la Información	Es el órgano colegiado encargado de tomar decisiones que concretan cómo alcanzar los objetivos marcados por los órganos de gobierno. Podrá nombrar Comités delegados o subcomités para la toma de decisiones diaria.
Comité Técnico de Seguridad de la Información	Es el órgano colegiado encargado de dar apoyo técnico al Comité de Seguridad de la Información y al Responsable de Seguridad.
Responsable de la Información	Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por el Ayuntamiento.
Responsable de Servicio	Tiene la responsabilidad última de determinar los niveles de servicio aceptables por el Ayuntamiento.
Responsable de Seguridad	Cumplirá las funciones como supervisor de la operación del sistema y vehículo de reporte y comunicación al Comité de Seguridad de la Información.
Responsable del Sistema	Es el responsable de la toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.
Técnico de Sistemas	Implementa, ejecuta y mantiene las medidas de seguridad aplicables al sistema de información.

Delegado de Protección de Datos	Es la persona/as encargadas de asesorar a los Responsables en materia de seguridad (Dirección, Comité de Seguridad, Responsable de la Información, Responsable de Servicio, Responsable de Seguridad, Responsable del Sistema) acerca del cumplimiento de la normativa de protección de datos personales. Su nombramiento es obligatorio para el Ayuntamiento y sus funciones vienen recogidas en el RGPD.

En el Ayuntamiento, con el objetivo de buscar la eficacia y la eficiencia de las medidas de seguridad que se adopten en torno a la información, los sistemas de información y los procedimientos administrativos, el rol de Responsable de la Información y Responsable del Servicio serán asumidos por la misma persona u órgano, en razón de la materia de su competencia.

8.2. PROCESO DE TOMA DE DECISIONES Y COORDINACIÓN

Los diferentes roles de seguridad de la información se articularán mediante la siguiente jerarquía: el Comité de Seguridad de la Información o los Comités que le apoyen, dará instrucciones al Responsable de la Seguridad que se encargará de cumplimentar, supervisando que los responsables y técnicos de sistemas implementan las medidas de seguridad según lo establecido en la Política de Seguridad del Ayuntamiento.

El Responsable del Sistema:

- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable de la Información/Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad en las siguientes materias:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad:

- Informar al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de

riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

- Informar al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad de la Información, como **secretario**:
    - Resumen consolidado de actuaciones en materia de seguridad y de las actuaciones llevadas a cabo en el resto de Comités.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

8.3. PROCEDIMIENTO DE DESIGNACIÓN Y RESOLUCIÓN DE CONFLICTOS

La Junta de Gobierno Local nombrará formalmente y de acuerdo a su régimen de funcionamiento interno:

- Al Responsable de la Seguridad.
- Al Delegado de Protección de Datos.
- Miembros del Comité de Seguridad de la Información.

La resolución de conflictos entre los distintos roles y responsabilidades del sistema, así como las posibles incompatibilidades serán analizadas por el Comité de Seguridad.

8.4. DETALLE DE LOS ROLES

8.4.1. DIRECCIÓN (JUNTA DE GOBIERNO LOCAL)

La función de Dirección la desempeñará la Junta de Gobierno del Ayuntamiento, quien entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que se alcancen.

Función	Detalle
Nombrar	Designa los diferentes roles encargados de la gestión de la seguridad, así como los miembros del Comité de Seguridad.
Objetivos	Fija y aprueba anualmente unos objetivos de nivel de riesgo aceptable. El Comité de Seguridad apoyará a la Junta de Gobierno Local en la fijación y aprobación de estos objetivos y reportará anualmente la evolución de dichos objetivos.

Aprobar	Aprobar el Plan de Adecuación al ENS. Aprobar la Política de Seguridad. Aprobar, tras cada proceso de Apreciación del Riesgo que se realice, del Plan de Tratamiento del Riesgo que se elabore.
Recursos	Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

8.4.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información del Ayuntamiento coordina la seguridad de la información a nivel de dirección y organización.

Composición. Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

Presidente	Concejal delegado de Modernización Administrativa
Secretario	Responsable de Seguridad
Vocales	Concejal delegado de Hacienda
	Concejal delegado de Personal
	Delegado de Protección de Datos
	Jefe Servicio de Personal
	Jefe Asesoría Jurídica
	Secretario General del Pleno
	Viceinterventor

A requerimiento del Comité de Seguridad se convocará cualesquiera otros responsables, propios o de terceras organizaciones subcontratadas para la prestación de los servicios, cuya intervención sea precisa por estar afectados por el Esquema Nacional de Seguridad y por la regulación en materia de Protección de Datos.

Funciones del Secretario. Corresponden al Responsable de Seguridad las funciones de Secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones de los Vocales. Corresponde a los vocales del Comité de Seguridad de la Información:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Funciones del Comité. Corresponde al Comité de Seguridad de la Información:

Función	Detalle
Informar	Atender las inquietudes de la Junta de Gobierno Local y de los diferentes departamentos/áreas municipales. Informar regularmente del estado de la seguridad de la información a la Junta de Gobierno Local.
Promover	Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
Coordinar	Coordinar los esfuerzos de las diferentes áreas municipales, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas, elevando aquellos casos en los que no tenga suficiente autoridad para decidir. Coordinar las acciones de mejora continua y evaluación del cumplimiento de la normativa en los sistemas de información, incluyendo la realización de Auditorías periódicas. Coordinar las actividades de formación y concienciación de técnicos, operadores y usuarios desde el punto de vista de seguridad de la información
Elaborar	Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada en su caso por la Junta de Gobierno Local. Elaborar la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información. Elaborar o apoyar en la elaboración de normativas de seguridad o procedimientos técnicos de seguridad a petición del Responsable de Seguridad.

Ayuntamiento de Burgos

Aprobar	Aprobar la normativa de seguridad de la información que afecten al conjunto de la organización o procedimientos técnicos de seguridad de la información Elaborar y aprobar los requisitos de formación y cualificación de técnicos y usuarios desde el punto de vista de seguridad de la información Aprobar planes de mejora de la seguridad de la información. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas. Aprobar los procedimientos técnicos que correspondan a un sistema o conjunto de sistemas de seguridad de la información o aquellos que afecten a distintas áreas de la seguridad.
Controlar	Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

8.4.3. COMITÉ TÉCNICO DE SEGURIDAD DE LA INFORMACIÓN

Como apoyo técnico del Comité de Seguridad de la Información y del Responsable de Seguridad se crea el Comité Técnico sobre aspectos relacionados con las TIC y la seguridad de la información.

El Comité Técnico en Seguridad de la Información estará compuesto por los siguientes roles:

Presidente	Responsable de Seguridad
Secretario	Técnico de aplicaciones/sistemas
Vocales	Responsable de Sistemas
	Responsables de la Información y Servicio (convocados por razón de la materia)

El secretario del Comité Técnico de Seguridad de la Información se encargará de convocar las reuniones del comité, elaborar y custodiar las actas que se realicen y comprobar la efectividad de los acuerdos adoptados.

Los vocales del Comité de Técnico de Seguridad de la información aportarán información sobre sus respectivas áreas de competencia y que guarden relación con el sistema de gestión de seguridad de la información.

Las funciones del Comité Técnico en Seguridad de la Información se centrarán en tomar decisiones relacionadas con la operativa diaria de los sistemas de información y vigilar el cumplimiento de las decisiones que se tomen a nivel directivo. Concretamente, sus funciones serán las siguientes:

Función	Detalle
Informar	Informar regularmente del estado de la seguridad de la información al Comité de Seguridad de la Información a través de los informes recopilados por el Comité o por el Responsable de Seguridad.
Coordinar	Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades. Coordinar las acciones de mejora continua y evaluación del cumplimiento de la normativa en los sistemas de información, incluyendo la realización de Auditorías periódicas. Coordinar en las actividades que ejecuten la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información. Coordinar las actividades de formación y concienciación de técnicos, operadores y usuarios desde el punto de vista de seguridad de la información.
Elaborar	Elaborar o apoyar en la elaboración de procedimientos técnicos de seguridad a petición del Responsable de Seguridad.
Aprobar	Aprobar los procedimientos técnicos que correspondan a un sistema o conjunto de sistemas de seguridad de la información o aquellos que afecten a distintas áreas de la seguridad o instrucciones. Aprobar planes de mejora de la seguridad de la información para mitigar riesgos.
Controlar	Obtendrá la información sobre el estado y desempeño de las medidas de seguridad aplicadas en los sistemas de información y recopilará la información necesaria para elevarla al Comité de Seguridad de la Información. Recopilarán información sobre el desempeño del sistema de gestión de la seguridad de la información a través del Responsable de Seguridad. Obtendrá información periódica sobre la ejecución de medidas de mejora continua y controlará los resultados de las auditorías de seguridad y cumplimiento que se realicen. Elaborarán informes técnicos a petición del Comité de Seguridad de la información.

El Comité Técnico de Seguridad de la Información podrá incorporar a su composición a aquellos responsables/roles del sistema que se vean afectados por la toma de decisiones para recopilar ideas u opiniones de los mismos.

En especial, los Responsables de Servicio/Información o los Responsables del Sistema afectados podrán incorporarse al Comité Técnico de Seguridad de la Información para dar sus opiniones y proponer soluciones al Comité Técnico.

8.4.4. RESPONSABLE DE LA INFORMACIÓN

En el Ayuntamiento, el Rol de Responsable de la Información se situará a nivel de gerencia o jefatura de servicio/sección. Este rol estará unificado con el de Responsable de Servicio.

Compatibilidades. Este rol coincidirá con el del Responsable de Servicio.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Sistema.

Las **funciones** del Responsable de la Información son las siguientes:

Función	Detalle
Establecer requisitos de seguridad sobre la información	Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
Determinar niveles de seguridad en cada dimensión	Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
Adoptar medidas sobre los datos personales	Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
Responder del uso	Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
Responder ante errores	El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Ayuntamiento de Burgos

8.4.5. RESPONSABLE DEL SERVICIO

En el Ayuntamiento, el rol de Responsable del Servicio se situará a nivel de Jefatura de Gerencia o Servicio/Sección. Este rol estará unificado con el de Responsable de la Información.

Compatibilidades. Coincidirá con el rol de Responsable de la Información. La diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Seguridad, ni con el de Responsable de Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

Las **funciones** del Responsable del Servicio son las siguientes:

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
Riesgos	Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).
Gestionar el correcto tratamiento de los datos personales	En cuanto a lo dispuesto en el RGPD y la normativa relacionada, por delegación del Responsable del Tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.

8.4.6. RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad de la Información es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información.

Ayuntamiento de Burgos

Las **funciones** del Responsable de Seguridad son las siguientes:

Función	Detalle
Política, Normativa y Procedimientos	Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política y Normativa de Seguridad de la Información, para su aprobación por Dirección. Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información e instrucciones.
Documentación RGPD	Coordinará y controlará las medidas de seguridad tanto técnicas como organizativas que apliquen en virtud a lo dispuesto por el RGPD y la normativa relacionada. Coordinará la elaboración de la Documentación de Seguridad del Sistema.
Formación y concienciación	Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información
Gestión de la Seguridad	Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización. Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema. Realizará el Análisis de Riesgos. Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos. Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información. Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas. Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

Comité de Seguridad	Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

8.4.7. RESPONSABLE DEL SISTEMA

El Responsable del Sistema es la persona que toma las decisiones operativas y será designado entre el personal perteneciente a la Sección de Tecnologías de la Información y Comunicación.

Compatibilidades. Este rol podrá coincidir con el de Técnico del Sistema.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad Corporativa o de la Información.

Las **funciones** del Responsable del Sistema son las siguientes:

Función	Detalle
Gestionar el Sistema	Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
Establecer directrices y medidas	Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema. Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. Determinar la configuración autorizada de hardware y software a utilizar en el Sistema. Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
Elaborar	Elaborar procedimientos operativos de seguridad e instrucciones. Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

Aprobar	Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema. Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
Monitorizar	Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

8.4.8. TÉCNICO DE SISTEMAS

Es la persona/as encargadas a de la implementación, gestión y mantenimiento de las medidas de seguridad que sean de aplicación a los sistemas de información. De igual modo se encargará de la gestión, mantenimiento, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

Por una parte, se encargarán de elaborar procedimientos operativos de seguridad e instrucciones.

Por otra parte, se encargarán de gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de la actividad, de forma que ésta se ajuste a lo autorizado.

Aplicarán los Procedimientos de Seguridad aprobados, monitorizando el estado de seguridad e informando al Responsable del Sistema o el Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

8.4.9. DELEGADO DE PROTECCIÓN DE DATOS

Es la persona u órgano que se ocupa de vigilar el cumplimiento de la normativa de protección de datos, de acuerdo a las funciones recogidas en el Reglamento Europeo de Protección de Datos (2016/679) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LO 3/2018).

Llevará a cabo funciones de asesoramiento e información sobre el cumplimiento de la normativa de protección de datos y responderá ante el más alto nivel jerárquico del Ayuntamiento.

Colaborará y asesorará a los responsables en materia de seguridad de la información en el cumplimiento de las obligaciones previstas en materia de protección de datos.

Será nombrado por la Junta de Gobierno Local y sus datos de contacto serán públicos, de modo que pueda atender las reclamaciones y cuestiones planteadas como consecuencia del cumplimiento de la normativa de protección de datos.

Ayuntamiento de Burgos

9. DATOS DE CARÁCTER PERSONAL

El Ayuntamiento trata datos de carácter personal en el ejercicio de sus competencias y de acuerdo a la normativa vigente. El tratamiento de datos personales se ajustará a las obligaciones y principios recogidos en el Reglamento Europeo de Protección de Datos 2016/679, así como en lo recogido por la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.

Todos los sistemas de información del Ayuntamiento que traten datos de carácter personal se ajustarán a la normativa y asignarán las medidas de seguridad técnicas y organizativas necesarias para la correcta protección de los datos personales en base al riesgo que implique cada tratamiento y siempre en defensa de los derechos y libertades de los interesados.

Por otra parte, el Ayuntamiento ha nombrado un Delegado de Protección de Datos, cuyas funciones recoge el RGPD y que estará a disposición de los ciudadanos para atender cualquier cuestión relacionada con la aplicación de la normativa de protección de datos.

10. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Responsable de la Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Responsable de la Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Ayuntamiento de Burgos

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

11.1. INSTRUMENTOS DE DESARROLLO

La **Política de Seguridad** de la Información del Ayuntamiento se desarrollará a través de los siguientes instrumentos:

- **Normativa de seguridad (NOR):** Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

- **Procedimientos Técnicos de Seguridad (PRO):** Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.

Al margen de estos instrumentos, podrán incorporarse guías informativas o instrucciones técnicas susceptibles de revisión por parte del Responsable de Seguridad, del Comité de Seguridad y/o del Comité Técnico de Seguridad y que se dirijan a aspectos concretos sobre la aplicación de medidas concretas sobre seguridad de la información.

11.2. ESTRUCTURA GENERAL

El desarrollo de la normativa de seguridad en su conjunto se llevará a cabo basándose en el análisis de riesgos y aspectos específicos de la Seguridad de la Información tales como las medidas de seguridad indicadas en el Anexo II del Esquema Nacional de Seguridad (ENS):

- **Marco organizativo:** orientado a administrar la seguridad de la información dentro de la organización municipal y establecer un marco gerencial para controlar su implementación. Partiendo de la presente Política de Seguridad se desarrollará el resto del marco normativo de seguridad.
- **Marco operacional:** constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
    - ✓ **Planificación**: Mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes entre otros aspectos.
    - ✓ **Control de Acceso:** Orientado a controlar el acceso lógico a la información.
    - ✓ **Explotación**: Medidas para la gestión de la seguridad en explotación; partiendo del inventario de activos y controlando la gestión de incidencias, cambios, gestión de la configuración, registros de actividad, entre otros.

- ✓ **Servicios externos:** Medidas de seguridad orientadas a garantizar que empresas y personas terceras que realicen servicios de cualquier clase contratados por el Ayuntamiento o que de alguna manera se presten bajo el control y/o la dirección del Ayuntamiento cumplan las políticas y normas de seguridad de la información establecidas por parte del Ayuntamiento.
- ✓ **Continuidad del servicio:** Acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.
- ✓ **Monitorización del sistema**: Orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos de los efectos de fallas significativas o desastres.

- **Medidas de protección**: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.
  - ✓ **Protección de las instalaciones e infraestructuras:** destinado a impedir accesos no autorizados, daños e interferencias a las instalaciones e infraestructuras del Ayuntamiento.
  - ✓ **Gestión del personal:** orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos.
  - ✓ **Protección de los equipos:** medidas para la protección de los equipos.
  - ✓ **Protección de las comunicaciones:** dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y elementos y sistemas de comunicación.
  - ✓ **Protección de los soportes de información:** para garantizar la información que contienen.
  - ✓ **Protección de las aplicaciones informáticas:** orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
  - ✓ **Protección de la información:** cumpliendo lo dispuesto en la Ley Orgánica de protección de datos de carácter personal.
  - ✓ **Calificación de la Información**: Estableciendo los requisitos, tipos y flujos de información que se producen, así como los procesos de elaboración, aprobación y acceso a la documentación.

Ayuntamiento de Burgos

- ✓ **Protección de los servicios:** definiendo las medidas necesarias para mantener la seguridad de los servicios TI.

La normativa de seguridad estará a disposición de todos los miembros de la organización municipal que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Esta normativa deberá ir firmada y avalada por un cargo de máxima responsabilidad para que su cumplimiento sea lo más estricto posible.

11.3. GESTIÓN DE LA DOCUMENTACIÓN

La gestión de la documentación relacionada con la seguridad de la información tendrá en cuenta el ciclo de vida de la misma (generación, aprobación, modificación), de modo que se establezcan distintas responsabilidades en cada fase del ciclo de vida.

En este sentido, la gestión de la documentación contará con los siguientes roles relacionados:

- Junta de Gobierno Local (Dirección)
- Comité de Seguridad de la Información (CSI)
- Comité Técnico de Seguridad de la Información (CTSI)
- Responsable de Seguridad de la Información (RSI)
- Responsables del Sistema (RS)
- Técnicos del Sistema y Desarrolladores (TS)
- Usuarios (US)

De acuerdo a lo anterior, en función del tipo de documento y el ciclo de vida, se ha establecido la siguiente matriz:

	Creación/Modificación	**Aprobación**
Política de Seguridad de la Información	CSI	Dirección
Normativas	CSI/RSI	Dirección/CSI
Procedimientos	CSI/CTSI/RSI/RS/TS	CSI/RSI/CTSI
Instrucciones	RSI/RS/TS/US	RSI/CTSI

Ayuntamiento de Burgos

11.4. SANCIONES PREVISTAS POR INCUMPLIMIENTO

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los preceptos incumplidos.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

12. SEGURIDAD DE LA INFORMACIÓN

Aunque la seguridad de la información no es lo mismo que la seguridad de las TIC la relación entre ambas es fuerte y crítica.

La clasificación de la información de carácter personal no se decide por criterios TIC o STIC, puesto que la seguridad de la información de carácter personal viene establecida en base al riesgo que implique el tratamiento de la misma, y de acuerdo a la metodología elegida por el Ayuntamiento para la valoración de dicho riesgo. No obstante, hay un vínculo entre el nivel de riesgo que tiene el tratamiento de datos personales con el nivel de seguridad asignado a los sistemas que alojan dicha información.

Para el resto de información, fuera del marco de la normativa sobre protección de datos, se realizará una clasificación atendiendo a la criticidad o sensibilidad de la misma.

De lo dicho se deduce que la existencia de datos personales será transversal a las otras categorías, pudiéndose encontrar datos personales en cualquier documento de tipo público, interno o interno confidencial.

Se dispondrá un sistema de etiquetado o nombrado para los documentos para que el destinatario de la información pueda conocer qué tipo de información contiene el documento, por ejemplo, a qué departamento o área pertenece, que categoría de información contiene, existencia de datos personales y a qué nivel etc.

12.1. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información que obra en los sistemas de información responsabilidad del Ayuntamiento, deberá contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la protección respecto a todas las dimensiones de la seguridad.

Ayuntamiento de Burgos

Estas medidas de seguridad se establecerán de acuerdo a unos criterios basados en el acceso a la información, su difusión y la materia que aborden.

En este sentido, se ha establecido un cuadro de calificación de documentos, que se indica a continuación, basado en los siguientes criterios, sin perjuicio de su desarrollo a través de la normativa o procedimientos técnicos pertinentes:

- (R) Requisitos legales, como los derivados de la normativa sobre secretos oficiales.
- (D) Difusión de la información, esto es, las personas autorizadas para acceder a la información.

R	D	Descripción	Ejemplos
Pública		Información de difusión para el público general. Apto para difusión entre todo tipo de organismos y entidades. La información no es confidencial y puede ser hecha pública sin ninguna implicación para la Organización. La pérdida de la disponibilidad debido al tiempo de inactividad del sistema es un riesgo aceptable. La integridad es importante pero no vital	• Catálogos de servicios ampliamente distribuidos. • La información disponible en el dominio público, incluyendo las áreas de acceso público del sitio web. • Descargas de software del Ayuntamiento. • Informes financieros requeridos por las autoridades. • Información publicada al amparo de la normativa de Transparencia o aquella originada por obligación legal y siguiendo los principios de la normativa de protección de datos.

Ayuntamiento de Burgos

R	D	Descripción	Ejemplos
Uso oficial	Interna	Documento de difusión parcialmente controlada no apto para su difusión pública y protegido del acceso externo. Su uso se restringe únicamente al personal interno del organismo y entidades y colaboradores. Para acceder internamente a esta información hace falta un permiso explicito por parte de un superior. El acceso no autorizado podría influenciar la eficacia operacional de la Organización, causar un importante daño. La integridad de la información es vital. Estará dirigida a los usuarios internos de la organización, así como a los responsables, comités y órganos de dirección.	• La información sobre los procedimientos de seguridad del Ayuntamiento que así se consideren. • Información interna de los departamentos del Ayuntamiento que así se considere. • Procedimientos normalizados de trabajo utilizados en todas las áreas. • Todo el código y aplicaciones, así como portales web desarrollados por y para la Organización.
	Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a aquellos empleados que necesiten conocerla para desempeñar sus funciones. Se entenderá dentro de esta clasificación la información recopilada y utilizada por la Organización en la contratación de personas, prestación de servicios a los ciudadanos o gestión de las finanzas. El acceso a esta información debe ser muy restringido dentro de la Organización.	• La información sobre los procedimientos de seguridad del Ayuntamiento que así se consideren. • Planes futuros del Ayuntamiento. • Contraseñas. • Información interna de los departamentos del Ayuntamiento que así se considere. • Datos económicos y otros datos personales de empleados o ciudadanos. • Información con datos de origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos, salud, vida

R	D	Descripción	Ejemplos
			sexual, orientación sexual o condenas e infracciones penales.

Toda la documentación, digital o impresa, debe indicar la clasificación de la información que contiene, salvo la información catalogada como pública.

13. OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo competencia del Responsable de la Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

14. TERCERAS PARTES

Cuando el Ayuntamiento preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán

canales para reporte y coordinación de los respectivos Responsables de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.