AYUNTAMIENTO DE CHICLANA DE LA FRONTERA.

Decreto

Organización y Calidad

Visto el informe de don José Antonio Domínguez Martínez, Jefe del Servicio de Organización y Calidad del Excmo. Ayuntamiento de Chiclana de la Frontera (en adelante: S. O. C.), de 21 de agosto del corriente, en el que pone de manifiesto que en la definición del objeto del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se incluye "*determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos (...)*" y, en su ámbito de aplicación a las Entidades que integran la Administración Local.

Visto que en su informe, el Jefe del S. O. C. cita el Anexo II del R. D. 3/2010 -Medidas de seguridad- para indicar que como elemento del marco organizativo del E. N. S., la 'Política de seguridad' *"(…) será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito (...)";* y que en dicho artículo el R. D. 3/2010 establece que "*Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente*", considerando como 'órgano superior' a los responsables directos de la ejecución de la acción del gobierno central, autonómico o local.

Visto el documento denominado 'Política de Seguridad' elaborado por la empresa Ingeniería e Integración Avanzadas, S. A. (CIF: A29584315), en coordinación con el Servicio de Organización y Calidad de este Ayuntamiento y que se reproduce en la parte resolutiva del presente.

En uso de las facultades que a esta Alcaldía-Presidencia confiere la Ley Reguladora de Bases del Régimen Local, de 2 de abril de 1985, y de conformidad con lo dispuesto en el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, **HE RESUELTO:**

ÚNICO.- Aprobar la política de seguridad de este Ayuntamiento contenida en el documento denominado 'Política de Seguridad' elaborado por la empresa Ingeniería e Integración Avanzadas, S. A. (CIF: A29584315), en coordinación con el Servicio de Organización y Calidad de este Ayuntamiento y cuyo tenor literal es el que sigue:

Política de Seguridad V.1.0

1. Introducción

El Ayuntamiento de Chiclana de la Frontera, (en adelante, el Ayuntamiento), como muestra de compromiso con la seguridad de la información de sus sistemas[1] ha desarrollado la presente "**Política de Seguridad de la Información y Protección de Datos**", (en adelante

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

Política de Seguridad), de conformidad con lo establecido en el "**Esquema Nacional de Seguridad**" (en adelante ENS) e incluye, asimismo, los principios básicos que permiten garantizar el cumplimiento de la legislación en materia de protección de datos vigente acorde con el "**Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo**", de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, (en adelante RGPD), así como la Ley Orgánica 3/2018, de Protección de Datos de Carácter Personal y garantía de derechos digitales.

La Política de Seguridad, es una declaración ética, responsable y de estricto cumplimiento, en todo el Ayuntamiento, la cual es desplegada a través de las diferentes Normativas y Procedimientos, con los que se procura que los riesgos, sean tratados adecuadamente.

El uso de los Activos de información, debe estar en consonancia con las buenas prácticas y procedimientos de trabajo profesionales, así como con los requisitos legales, reglamentarios y contractuales, que deben garantizar la Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad de la información y los servicios.

2. Objetivo y ámbito de aplicación

- Este documento constituye el establecimiento de un marco organizativo y tecnológico en el Ayuntamiento.
- Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.
- Debe ser conocida y cumplida por todo el personal del Ayuntamiento, independientemente del puesto, cargo y responsabilidad dentro del mismo, en virtud del artículo 12 del ENS.

3. Legislación y normativa de referencia

El marco normativo de las actividades del Ayuntamiento en el ámbito de esta Política de Seguridad está integrado por las siguientes normas:

- Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Reglamento Europeo de Firma Electrónica (eIDAS). Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ordenanza Reguladora de la Administración Electrónica del Ayuntamiento de Chiclana de la Frontera.

4. Principios y directrices

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen o en caso de materializarse, no afecten gravemente a la información que maneja, o los servicios que se prestan.

4.1 Prevención

Se debe 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, deberán implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- 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.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

4.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar el funcionamiento de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.
La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.3 Respuesta

Se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.
Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

4.5 Otros principios generales:

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tienen acceso a la información del Ayuntamiento deben de protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas, según lo establecido en el artículo 22 del ENS.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el ENS, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Además, el Ayuntamiento de Chiclana exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
- Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves o códigos.
- En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se estará a lo dispuesto en el artículo 18 del ENS.
- Los sistemas deben diseñarse y configurarse de forma que se garantice la seguridad por defecto tal y como se exige en el artículo 19 del ENS.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importante el RGPD.

5. Organización de la Seguridad de la Información

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la seguridad de la información del Ayuntamiento está compuesta por los siguientes agentes:

a) Comité de Gestión de la Seguridad de la Información (CS).

b) Responsable de Seguridad (RS).

c) Responsables de la Información y de los Servicios (RISS).

d) Responsables del Sistema de Información (RSI).

e) Delegado de Protección de Datos (DPD).

f) Responsable del Tratamiento (RT).

5.1 Comité de Gestión de la Seguridad de la Información (CS)

Para la gestión de la Seguridad de la Información, se crea el "**Comité de Gestión de la Seguridad de la Información**", (en adelante el Comité de Seguridad) (CS), dentro del ámbito de

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en el Ayuntamiento y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad.

Son funciones del Comité de Seguridad (CS):

a) Identificar los objetivos del Ayuntamiento en el ámbito de la Seguridad de la Información.

b) Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en el Ayuntamiento.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnicos y de control, los sistemas y servicios del Ayuntamiento.

e) Garantizar que la seguridad, forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Comunicar a los terceros que colaboren en la explotación de los sistemas de información, la realización de dicha explotación, conforme a los requisitos exigidos en el ENS.

g) Proponer los nombramientos y ceses de responsables y responsabilidades en materia de seguridad de la información.

h) Valorar el grado de conformidad de los procedimientos implantados en el Ayuntamiento con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

i) Aprobar y supervisar las normativas y procedimientos de seguridad, que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

j) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

k) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

l) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.

m) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

n) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc., que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas del Ayuntamiento.

o) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en el Ayuntamiento.

El Comité de Seguridad (CS), se reunirá con carácter ordinario, al menos una vez al año, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

Para la celebración de las reuniones del Comité de Seguridad (CS) será preciso la presencia de, al menos, el 51% de los miembros permanentes.

5.2 Responsable de Seguridad (RS)

Es el responsable de que los servicios y sistemas de información del Ayuntamiento, se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) **Confidencialidad**: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.

b) **Integridad**: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.

c) **Disponibilidad**: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

Son funciones del Responsable de Seguridad (RS):

a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Respecto a la documentación, son funciones del Responsable de Seguridad(RS):

a) Proponer al Comité de Seguridad (CS) la documentación de seguridad de segundo nivel (Normativas de Seguridad) de obligado cumplimiento.

b) Supervisar la documentación de tercer nivel (Procedimientos de Seguridad) de obligado cumplimiento.

c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Respecto a la protección de datos de carácter personal, son funciones del Responsable de Seguridad (RS):

a) Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Ayuntamiento.

b) Colaborar con el Responsable del Tratamiento (RT), en la difusión de las normativas, procedimientos e instrucciones.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

c) Realizar los controles periódicos establecidos para verificar el cumplimiento de las normativas, procedimientos e instrucciones.

d) Analizar los informes de auditoría y proponer al Responsable del Tratamiento (RT), las medidas correctoras oportunas.

e) Autorizar la recuperación de datos tratados.

f) Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

El Responsable de Seguridad (RS), es la figura que determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos. Deberá ser una persona física, jerárquicamente superior e independiente de los "Responsables del Sistema de Información" (RSI).

El nombramiento y cese del Responsable de Seguridad (RS) será a propuesta del Comité de Seguridad (CS).

5.3 Responsables de la Información y de los Servicios (RISS)

Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione.

Son los responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables, dentro del marco establecido en el Anexo I del ENS.

Son los responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

Son los encargados, contando con la participación y asesoramiento del Responsable de Seguridad (RS) y de los "Responsables del Sistema de Información" (RSI), de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

Son los responsables de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

El nombramiento y cese de los "Responsables de información y de los servicios" (RISS) será a propuesta del Comité de Seguridad (CS).

5.4 Responsables del Sistema de Información (RSI)

Personal designado perteneciente al Servicio de Organización y Calidad cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.

c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema que le corresponda.

d) Elaborar procedimientos de seguridad de los sistemas de información.

Podrá acordar la suspensión del manejo de determinada 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 deberá ser acordada con el "Responsable de la Información y de los servicios" (RISS) afectado y el Responsable de Seguridad (RS) antes de ser ejecutada.

El nombramiento y cese de los "Responsables del Sistema de Información" (RSI) será a propuesta del Comité de Seguridad (CS), pudiendo ser delegadas determinadas tareas de seguridad, en uno de los "Responsables de la Información y de los Servicios" (RISS).

5.5 Delegado de Protección de Datos (DPD)

El Delegado de Protección de Datos (DPD) será único para todos los órganos y organismos del Ayuntamiento, se informará de su nombramiento y cese a la Agencia Española de Protección de Datos.

Son funciones del Delegado de Protección de Datos (DPD):

- Informar y asesorar al Ayuntamiento y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del RGPD y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del RGPD en el Ayuntamiento.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control.
- Actuar como punto de contacto de la Autoridad de Control.

Además, asesorará y supervisará en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- En la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Ayuntamiento – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características del Ayuntamiento y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
- Implantación de programas de formación y sensibilización del personal del Ayuntamiento en materia de protección de datos.

El nombramiento y cese del Delegado de Protección de Datos (DPD) será a propuesta del Comité de Seguridad (CS).

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

5.6 Responsable del Tratamiento (RT)

Según el artículo 4.7 del RGPD, "El Responsable del Tratamiento (RT) es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento", es decir, el Ayuntamiento de Chiclana.

El Ayuntamiento de Chiclana debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como Responsable de Seguridad (RS), quien deberá coordinar y controlar las medidas de seguridad definidas.
- Designar al Delegado de Protección de Datos (DPD), cuando corresponda.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar 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. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en el Ayuntamiento.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Tratamiento (RT), que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

5.7 Resolución de conflictos

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad (RS).

5.8 Obligaciones del Personal

Todo el personal, interno y externo, del Ayuntamiento de Chiclana tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad (CS) disponer de los mecanismos necesarios para que la información llegue a todo el personal indicado.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Todo el personal relacionado con la información y los sistemas deberá regirse según las estipulaciones del art. 14 del ENS, relativo a la gestión del personal.

6. Asesoramiento especializado en materia de seguridad

6.1 Asesoramiento especializado

El Responsable de Seguridad (RS) será el encargado de coordinar los conocimientos y las experiencias disponibles en el Ayuntamiento de Chiclana con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

6.2 Cooperación entre organismos y otras Administraciones Públicas

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, el Ayuntamiento de Chiclana mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

6.3 Revisión independiente de la Seguridad de la Información

El Comité de Seguridad (CS) propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en el Ayuntamiento reflejan adecuadamente sus disposiciones.

7. Protección de Datos de Carácter Personal

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como lo establecido en la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

8. Formación y concienciación

El objetivo principal es lograr la plena conciencia respecto a que “la Seguridad de la Información afecta a todo el personal del Ayuntamiento y a todas las actividades”, de acuerdo al principio de seguridad integral recogido en el art. 5 del ENS. A estos efectos, el Ayuntamiento, propondrá y organizará sesiones formativas y de concienciación para que todas

las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

9. Análisis y gestión de riesgos.

El Ayuntamiento asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigente bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad.
Para ello, con el objetivo de conocer el nivel de exposición de los activos de información a los riesgos y amenazas en materia de seguridad, los "Responsables de los Sistemas de Información" (RSI) realizarán, con periodicidad al menos bianual, un análisis de riesgos cuyas consecuencias se plasmarán en actuaciones para tratar y mitigar el riesgo, o incluso, replantear la seguridad de los sistemas en caso necesario.

Se realizará un análisis de riesgos:

- Cuando sea preceptivo según la normativa vigente.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas, que no hubieran sido tenidas en cuenta o vulnerabilidades graves, que no estén contrarrestadas por las medidas de protección implantadas.

Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad (RS) y éste al Comité de Seguridad (CS).

10. Estructura normativa.

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

10.1. Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, del Ayuntamiento, recogido en el presente documento y aprobado mediante Decreto.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

10.2 Segundo Nivel: Normativas de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad (CS), a propuesta del Responsable de Seguridad (RS).

10.3 Tercer Nivel: Procedimientos de Seguridad

Documentos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos es del Responsable de Seguridad (RS), a propuesta de los Responsables del Sistema de información (RSI).

10.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los "Responsables de los Sistemas de Información" (RSI) en su ámbito.

Con la finalidad exclusiva de lograr el cumplimiento del objeto del ENS, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

10.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

11. Publicación de la política de seguridad

La presente Política, además de en el "Boletín Oficial de la Provincia", en la página web del Ayuntamiento (https://www.chiclana.es/)

12. Entrada en vigor

La Política de Seguridad, aprobada por decreto será aplicable a partir del día siguiente al de su publicación en el Boletín Oficial de la Provincia de Cádiz.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23

Organización y Calidad

Del contenido de la presente resolución se dará traslado a todos los empleados públicos de este Ayuntamiento, a través de los responsables de las diferentes áreas de la administración municipal.

En Chiclana de la Fra., al día de la fecha de la firma electrónica. Cándida Verdier Mayoral. Teniente de Alcalde, Delegada de Régimen Interior, Decreto de la Alcaldía número 7.095, de 8 de noviembre de 2019. Transcríbase al Libro de Resoluciones. Francisco Javier López Fernández, Secretario General.

Documento firmado por:	Fecha/hora:
LOPEZ FERNANDEZ FRANCISCO JAVIER	24/08/2020 21:22:12
VERDIER MAYORAL CANDIDA	24/08/2020 10:07:23