NORMATIVA

USO DE REDES SOCIALES

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.27	DOCUMENTO:	NORMATIVA DE USO DE REDES SOCIALES

REVISIÓN NÚMERO:	1.0	FECHA DE ENTRADA EN VIGOR:	31 – Octubre - 2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
[ÁREA]	[ÁREA]	Comité de Seguridad de la Información
[NOMBRE – INICIALES]	[NOMBRE – INICIALES]	[NOMBRE – INICIALES]
FECHA:	FECHA:	FECHA:
FIRMA:	FIRMA:	FIRMA:

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

SEGURIDAD

PÚBLICA:	☐	PUBLICABLE	☐	USO INTERNO	☒	CONFIDENCIAL:	☐	SECRETA:	☐

PRIVACIDAD

NO IP	☐	IP A	☒	IP B	☐	IP C	☐

Confidencialidad Acerca de este documento

Excmo. Ayuntamiento de Baeza

Pje. Cardenal Benavides, 10
23440 Baeza, Jaén
ESPAÑA
http://www.baeza.es/baeza/extranet/

1) OBJETO

El objeto de la presente normativa es regular el uso de redes sociales en los sistemas de información del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento), posibilitando de esta manera la homogeneización de criterios dentro de los departamentos, áreas o servicios, y definiendo unas reglas de uso que serán conocidas y observadas por todos los usuarios del Ayuntamiento.

2) ALCANCE

Es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, presta sus servicios al Ayuntamiento, incluyendo proveedores externos cuando sean usuarios de los Sistemas de Información la entidad.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, Responsable de la Entidad, Responsable de Seguridad, Responsable del Sistema y de todos los actores intervinientes en la misma.

Cualquier modificación posterior entrará en vigor al día siguiente de su aprobación y publicación por parte del Comité de Seguridad. En este caso, la versión anterior quedará anulada por la última versión de esta normativa.

3) RESPONSABILIDADES

El responsable de la puesta en marcha de las medidas descritas en la presente normativa será el Responsable de Seguridad, que velará en todo momento por que el cumplimiento de lo referente en esta normativa junto con el Responsable del Sistema.

4) DESARROLLO NORMATIVO

Con carácter general, los usuarios del Ayuntamiento dispondrán de acceso a Internet como herramienta de productividad y conocimiento, para el desempeño de su actividad profesional.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet por los siguientes motivos:

- **Seguridad**: Debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- **Volumen del tráfico externo de datos**: Asegurando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias del Ayuntamiento.
- **Volumen del tráfico interno de datos**: Como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- **Ética**: Finalmente, es ineludible el compromiso que el Ayuntamiento debe mantener con la sociedad a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

4.1) REDES SOCIALES: BENEFICIOS Y RIESGOS

No es raro ver perfiles de ayuntamientos en redes sociales tales como Facebook, Twitter, Google+, Linkedin, Youtube, Flickr, Pinterest, Periscope, Instagram, Slideshare, etc.

La pretensión pública -siempre laudable- de compartir conocimientos, experiencias, información, etc., comporta no obstante ciertos riesgos que conviene conocer de antemano. Sólo siendo conscientes de su existencia podremos considerar la adopción de las medidas de mitigación del riesgo correspondientes y, en su consecuencia, decidir si, pese a todo, nos interesa "estar" en tal o cual red social.

Por la parte que ahora nos interesa en esta Norma, los riesgos más significativos en la utilización de las redes sociales devienen o están directamente relacionados con el cumplimento (incumplimiento, habría que decir) legal.

Efectivamente, la creación y el uso de perfiles "públicos" en las redes sociales obligan a la conformidad legal con distintas regulaciones, muy especialmente, las relativas a:

- La Protección de Datos de Carácter Personal, regulada, además de en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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 o RGPD), en la todavía vigente Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y Real Decreto 1720, Reglamento de Desarrollo de la LOPD2 .
- Los Derechos al Honor, la Intimidad y la Propia Imagen, regulados en la Ley Orgánica 1/1982 de Protección Civil del derecho al honor, a la intimidad y a la propia imagen.
- La Protección de los Derechos de Propiedad Intelectual, regulados en el Real Decreto Legislativo 1/1996, Texto Refundido de la Ley de Propiedad Intelectual.
- La Protección de los Derechos relativos a los Servicios de la Sociedad de la Información, regulados en la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico, y, por supuesto,
- La Protección de la Información y los Servicios Prestados por las entidades del Sector Público y privado, regulada en el Real Decreto 3/2010, Esquema Nacional de Seguridad (ENS).

A la conformidad legal con esta última regulación se dirige el presente documento.

Pese a su variedad y a sus respectivas comunidades de usuarios (que se cuentan por millones, en todo el mundo), existen dos grandes tipos de redes sociales:

- **Personales:** donde el vínculo que une a sus usuarios se sustenta en las relaciones personales, (tales como Facebook, Twitter, Google+, LinkedIn, etc.) y
- **Basadas en Contenidos:** en las que prevalece el contenido que cada usuario comparte con el resto, (tales como YouTube, Slideshare, Instagram, etc.).

No es propósito del presente documento señalar cómo deben usarse las cuentas de titularidad pública de las redes sociales desde el punto de vista comunicacional, sino desde el punto de vista de la seguridad de la información, lo que, pese a todo y en algunos casos, nos obligará a tratar tangencialmente alguna cuestión de aquella naturaleza.

5) NORMATIVA EN MATERIA DE USO DE REDES SOCIALES

Con el despliegue de las TIC y, en particular, con el desarrollo de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que pueden poner en peligro los sistemas de información de las organizaciones.

En este sentido, la medida de seguridad [mp.per.2] del ENS señala:

Deberes y obligaciones [mp.per.2].
1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.
   A. Se especificarán las medidas disciplinarias a que haya lugar.
   B. Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
   C. Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.
2. En caso de personal contratado a través de un tercero:
   A. Se establecerán los deberes y obligaciones del personal.
   B. Se establecerán los deberes y obligaciones de cada parte.
   C. Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Por tanto, para minimizar los riesgos derivados del uso de Internet, resulta necesario adoptar un conjunto mínimo de medidas de seguridad dirigidas a propiciar su correcto uso.

Los siguientes epígrafes recogen el conjunto de medidas que deben tenerse en cuenta cuando se use o se pretendan usar las Redes Sociales como herramienta de comunicación y difusión de las funciones competencialmente del Ayuntamiento.

6) AUTORIZACIÓN PREVIA

Con carácter general, y salvo las excepciones que pudieran autorizarse en el Ayuntamiento, y que, en todo caso, deberán estar recogidas en la Política de Seguridad, ninguna persona que preste sus servicios en el Ayuntamiento podrá darse de alta en ninguna red social, en nombre o en representación del Ayuntamiento, salvo autorización expresa de La Alcaldía y con el conocimiento del Responsable de Seguridad. Por tanto, salvo en el supuesto señalado, la presencia en las redes sociales de un empleado público del Ayuntamiento será siempre a título personal.

7) MEDIDAS COMPORTAMENTALES

Una vez autorizado a darse de alta en una red social en representación del Ayuntamiento, el empleado usuario de la red social de que se trate debe observar las siguientes normas de comportamiento:

C1	Recordar en todo momento que las redes sociales constituyen un foro público. Por tanto, por el hecho de agregar cualquier dato, comentario o información, el usuario está asumiendo que éste puede ser visto por los restantes usuarios de tal red social, por el Ayuntamiento y, en general, por cualquier persona.
C2	Si el usuario está usando el perfil de la red social en representación del Ayuntamiento, conviene mostrar abiertamente tal representación, a menos que existan circunstancias excepcionales que no lo aconsejen, tales como una amenaza potencial a la seguridad personal. En cualquier caso, nunca deben proporcionarse detalles personales tales como la dirección o los números de teléfono personales.
C3	Es siempre recomendable hablar en primera persona, tratando de aportar valor en los comentarios vertidos, facilitando informaciones y perspectivas contrastadas y que no se encuentren tipificadas como información clasificada o cuya revelación pudiera ocasionar un perjuicio al Ayuntamiento o, en general, a cualquier persona o entidad, pública o privada. El usuario debe recordar que será siempre responsable de sus aportaciones y de las eventuales consecuencias en su reputación y, por ende, en el Ayuntamiento en donde presta sus servicios. En caso de dudas, lo mejor es abstenerse de hacer una contribución.
C4	Las redes sociales deben constituir un foro de intercambio de opiniones o para el debate constructivo, pero no es el ámbito apropiado para crear polémica, descalificar a otras personas o a terceros, ni para presentar quejas y reclamaciones que deben canalizarse a través de las vías específicas que el Ayuntamiento tiene establecidas para esa finalidad.
C5	El usuario debe tratar con respeto a los otros usuarios, usando un lenguaje apropiado y correcto y actuando siempre como si estuviera en presencia de la(s) otra(s) persona(s).
C6	Salvo autorización, el usuario no debe publicar material publicitario ni comunicacional del Ayuntamiento, ni debe hacer uso de su perfil en la red social para lucrarse o hacer negocio, ni para comparar las funciones, competencias o, en general, desenvolvimiento del Ayuntamiento con otras entidades.
C7	Los contenidos publicados en las redes sociales pueden estar sujetos a Derechos de Propiedad Intelectual, por lo que la publicación de cualquier contenido requiere tener la certidumbre de que se encuentra libre de estas cargas.
C8	La contribución del usuario en la red social debe presentar datos reales, concretos y argumentación consistente. Se permiten citas o la reproducción de pequeños fragmentos de textos, libros u obras de terceros en general, siempre y cuando se indique la fuente y el nombre del autor. Si el usuario realiza una contribución propia (texto, fotografías, gráficos, vídeos o audios) debe saber que otorga al Ayuntamiento autorización para reproducirla en cualquier medio físico o virtual donde se indicará el nombre del empleado público como autor, todo ello sin perjuicio de que otros usuarios también podrían guardarlos o reproducirlos.

C9	El logotipo del Ayuntamiento y, en general, cualquier otro logotipo o distintivo gráfico del Ayuntamiento constituyen marcas registradas. También son titularidad del Ayuntamiento los contenidos colgados en su portal y, por tanto,el Ayuntamiento se reserva todos los derechos de propiedad intelectual e industrial asociados a los mismos. El usuario debe comprometerse a respetarlos y a no utilizarlos sin la debida autorización, cualquiera que sea el medio.
C10	La descarga de contenidos, su copia o impresión requerirá autorización del Responsable de Seguridad.
C11	En ningún caso deberá usarse la red social para el intercambio de credenciales o contraseñas, de cualquier sistema y para cualquier finalidad.
C12	La información contenida en el perfil de la red social no deberá considerarse nunca como información oficial en relación con las funciones y competencias del Ayuntamiento.
C13	El perfil de la red social de que se trate puede contener manifestaciones sobre previsiones o estimaciones que incluyen comentarios sobre el desarrollo de las funciones del Ayuntamiento basadas en juicios actuales, pudiendo suceder que determinados riesgos, incertidumbres y otros factores relevantes, desconocidos o imprevisibles ocasionen que los resultados difieran materialmente de lo esperado. El usuario debe recordar que las declaraciones relativas a los resultados, funciones, competencias, etc., no pretenden dar a entender que el desempeño del Ayuntamiento será necesariamente el previsto. Nada en el perfil debe ser tomado como una previsión de resultados.
C14	El Ayuntamiento velará en todo momento por preservar el buen uso del perfil y, por ello, el Ayuntamiento, como administrador, se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que: Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales al Ayuntamiento, sus empleados, colaboradores o terceros. Incorpore datos de terceros sin su autorización. Contenga cualquier tipo de recomendación relativa a las funciones y competencias del Ayuntamiento privilegiada o material publicitario o de comunicación, personal o en beneficio de terceros, sean personas físicas o jurídicas. Sea redundante. No esté relacionada con la finalidad perseguida por el Ayuntamiento al darse de alta en la red social de que se trate.

8) USO DE MEDIOS SOCIALES CON FINES EXCLUSIVAMENTE PERSONALES

En ocasiones, el uso personal o profesional de una red social pueden llegar a confundirse. Por tanto, se debe ser consciente de las responsabilidades cuando se mezclan la vida personal y la laboral en estos medios.

Las personas que trabajan para el Ayuntamiento deben usar su buen juicio y asumir la responsabilidad personal y profesional de los contenidos que publican a través de los medios sociales.

Es frecuente que se admita el uso de una cuenta personal para comentar sobre asuntos no relacionados con el trabajo, aunque no debiera permitirse, de manera general, que el uso de tales cuentas se lleve a cabo en horario laboral ni, por motivos de seguridad, usando los medios electrónicos del Ayuntamiento.

En cualquier caso, el uso de plataformas de redes sociales nunca debe interferir con las funciones principales, con la excepción de aquellos puestos de trabajo que incluyan entre sus tareas precisamente el uso de estas herramientas sociales.

Debemos recordar que el uso de una cuenta privada no exime de cumplir los códigos de buena conducta generalmente admitidos y los específicamente contemplados en la Política de Seguridad de la Información del Ayuntamiento.

Por todo ello, no deben publicarse opiniones personales a través de cuentas oficiales y tampoco promover las cuentas personales a través de cuentas oficiales.

No debe comentarse en redes sociales aquello que no se debe ser de dominio público, aunque exista una única persona a la que se desee dejar al margen. Las redes sociales pueden actuar de amplificador y comprometer a sus usuarios.

Aquellas personas que tienen responsabilidades de gobierno, en virtud de su posición, deben tener en cuenta si los comentarios personales que publican, incluso en lugares claramente personales, pueden ser mal interpretados como declaraciones realizadas por el Ayuntamiento.

9) MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, es preciso identificar claramente los canales oficiales del Ayuntamiento que ya pudieran existir y, en la medida de lo posible, diferenciar los canales verdaderos (mediante el uso de TL) e impulsar la vigilancia y el cierre de canales falsos.

10) MEDIDAS DE ORDEN NORMATIVO

Siempre resulta conveniente que el Ayuntamiento disponga de una norma jurídica (bajo la forma pertinente: Resolución, Instrucción, Orden, …) que regule la creación y gestión de los canales digitales del Ayuntamiento (portales institucionales y redes sociales, esencialmente), como vehículos estratégicos de comunicación, y otorgue consistencia jurídica a su modelo de gobernanza.

Dicha regulación deberá contener reglas precisas sobre la estructura de este nuevo modelo de gobernanza, que se concreta en dos ámbitos:

- Gestión diaria de los canales digitales, siendo frecuente que, para agilizar el mantenimiento y la actualización de los contenidos, se distribuyan las responsabilidades entre las diversas unidades sectoriales en función de sus respectivas competencias. Así, los responsables de los contenidos serán los encargados del mantenimiento y actualización de la información recogida en cada uno de los portales y perfiles de redes sociales y tendrán autonomía para designar una persona y asignarle que lleve a cabo esas tareas como “Community Manager” bajo su supervisión. Estas designaciones deberán comunicarse al Comité de Seguridad.

Por último, el apoyo técnico a los medios institucionales dependerá de las distintas unidades con competencias en materia de TIC, que ejercerán las funciones de apoyo técnico a la dirección y coordinación de los medios institucionales, en sus respectivos ámbitos materiales de competencia.

Todo esto se llevará a cabo bajo el principio de coordinación y ausencia de duplicidades, con el objetivo de que, como regla general, el contenido de medio institucional sea único y no reescrito en otro, con independencia de que se establezcan los enlaces necesarios.

En el epígrafe siguiente se contiene un Modelo de Política de Seguridad de Redes Sociales.

11) MEDIDAS DE SEGURIDAD TECNOLÓGICA

Las medidas de seguridad esenciales son las siguientes:

S1	Las cuentas en redes sociales del Ayuntamiento se crearán desde correos electrónicos corporativos, delegándose la gestión de las mismas en las Unidades designadas para cada una de ellas. El Responsable de Seguridad del Ayuntamiento extenderá sus competencias a los perfiles de redes sociales que pudieran crearse.
S2	La custodia de las contraseñas de los perfiles de las redes o de sus administradores que así lo requieran, estará centralizada y será responsabilidad de la persona administradora.
S3	Cualquier instalación de aplicaciones de terceros que tenga algún tipo de permisos sobre cuentas de las redes sociales deberá ser previamente autorizada por el Responsable de Seguridad del Ayuntamiento, para verificar que esta aplicación no pone en riesgo ni los datos ni la seguridad de la cuenta.

S4	La modificación de cualquiera de las opciones de privacidad o publicación de comentarios deberá autorizarse previamente por el Ayuntamiento, contando con la opinión del Responsable de Seguridad.
S5	Como norma general, las contraseñas de las plataformas de gestión deberán ser robustas.
S6	Siempre que sea posible, es conveniente mantener las cuentas desde una herramienta de gestión que pueda otorgar permisos diferentes de publicación y que su acceso no se realice a través de la propia contraseña de la red social de que se trate. El responsable de cada cuenta definirá quiénes son las personas que la gestionarán, velando y haciendo respetar la confidencialidad de las contraseñas de acceso.
S7	Siempre que sea posible, el acceso a las cuentas se realizará desde sistemas corporativos. En caso de necesitar publicar contenidos desde un dispositivo móvil, se hará desde una aplicación diferente a la que se utiliza de modo personal.

12) MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Cada Política de Seguridad de Redes Sociales podrá variar en función del Ayuntamiento de que se trate (especialmente si forman parte de grupos diferenciados, tales como las entidades que pertenecen a las Administraciones Públicas de aquellas otras encuadradas en el Sector Público Institucional). Esta realidad podría hacer aconsejable, ocasionalmente, la presencia de elementos de política de seguridad diferentes.

Se presenta seguidamente un esquema básico que cada Organismo o Entidad puede adaptar para desarrollar su propia Política de Seguridad de Redes Sociales.

1. Introducción (De qué trata la Política).

a) Gestión de la Política (Mecanismos del Ayuntamiento para cambiar y actualizar la Política).

b) Fecha de entrada en vigor.

c) Objetivos (Cuales son los objetivos perseguidos por la Política: fijación de pautas de comportamiento, determinación de responsabilidades, gestión de la reputación, etc.)

d) Propósito (Cuál es el propósito del documento y quién debe aplicarlo).

e) Ámbito (Cuál es la aplicabilidad de la Política a la tecnología, a los empleados, a los subcontratistas y a los partners del Ayuntamiento.

2. ¿Cómo se usan las Redes Sociales en el Ayuntamiento?

a) Redes Sociales contempladas (Facebook, Flickr, LinkedIn, Twitter, YouTube, etc.)

b) Beneficios del uso de las redes sociales (comunicación, servicio a los administrados, desarrollo de nuevos servicios, respuesta de los usuarios, etc.)

c) Objetivos del Community Manager (¿Quién es el Community Manager del Ayuntamiento?, ¿Cuáles son sus funciones y responsabilidades?)

d) Responsabilidades del Servicio TIC del Ayuntamiento (Definición de la Seguridad TIC, identificación de procesos para autenticar y autorizar en cada plataforma de red social, definición de responsabilidades de implementación, definición de responsabilidades de notificación, definición de responsabilidades de monitorización).

e) Responsabilidades del Servicio/Asesoría Jurídico/a (Definición del papel de la Seguridad TIC como soporte al Servicio Jurídico para desarrollar sus funciones de manera segura.)

3. Políticas Generales para Redes Sociales.

a) Publicidad institucional.

b) Requisitos legales.

c) Gestión de la comunidad.

d) Confidencialidad (¿Qué información puede compartirse?)

e) Divulgaciones (Los empleados del Ayuntamiento y los terceros: ¿qué información puede revelar y cual no?)

f) Cuestiones legales (¿Es necesario aplicar alguna restricción en la red social de que se trate?)

g) Nivel de compromiso (¿Cuáles son las expectativas de compromiso con la comunidad y qué recursos internos y externos deben usarse?)

h) Cómo gestionar los comentarios negativos.

i) Preguntas de la prensa (definición de responsabilidades en lo relativo a las relaciones con la prensa).

j) Empleados de terceras partes (Identificar procesos para la gestión de las relaciones con terceros).

k) Restricciones sobre el uso de marcas o, en general, derechos de propiedad intelectual (¿Cómo habrán de gestionarse las marcas o cualesquiera otros derechos sujetos a propiedad intelectual?)

4. Políticas de Seguridad TIC

A. Sobre la base de la que ya dispone en el Ayuntamiento, en función de lo exigido por el ENS.
B. Autenticación de acceso a las Redes Sociales (contraseñas).
C. Aplicaciones de redes sociales implementadas en el Ayuntamiento:
    1. Inicio de sesión fallido: Reiterados errores en el inicio de sesión pueden indicar un intento de romper una contraseña y acceder de forma subrepticia a una cuenta de la red. Con el fin de protegerse contra la adivinación de la contraseña y los intentos por fuerza bruta, el Ayuntamiento debe bloquear la cuenta de un usuario después de un número finito de inicios de sesión sin éxito.
    2. Logging: Las necesidades de logging varían dependiendo del tipo de sistema de red y del tipo de datos que contiene el sistema. Las siguientes secciones detallan los requisitos del Ayuntamiento para el logging y la revisión de registros.
        I. Servidores de aplicaciones: Los registros de los servidores de aplicaciones son del máximo interés ya que estos servidores suelen permitir conexiones desde un gran número de fuentes internas y/o externas. Como mínimo, se registrarán los errores o fallos en el inicio de sesión.
        II. Dispositivos de red: Los registros de dispositivos de red que protegen los servidores de aplicaciones son de interés ya que estos dispositivos controlan todo el tráfico de red y pueden tener un enorme impacto en la seguridad de la compañía. Como mínimo, se registrarán los errores o fallos en el inicio de sesión.
        III. Gestión de logs.
    1. Revisión de logs. Las aplicaciones de gestión de logs pueden ayudar a resaltar eventos importantes, sin embargo, un miembro del equipo TIC del Ayuntamiento (Responsable de Seguridad) debe revisar los registros con la frecuencia que sea razonable.
    2. Retención de logs: Los registros deben ser retenidos de acuerdo con la Política de Retención del Ayuntamiento.
        I. Detección de Intrusión / Prevención de Intrusión: el Ayuntamiento precisará usar un IDS o IPS en servidores de aplicaciones críticas.
        II. Pruebas de seguridad: Las auditorías de seguridad, incluyendo las pruebas de penetración, son una parte importante del mantenimiento de la seguridad de la red del Ayuntamiento, y deberán realizarse conforme a lo dispuesto en el ENS y en las Instrucciones Técnicas de Seguridad que lo desarrollan.
        III. Documentación de aplicaciones de redes sociales: La documentación proporcionada por las redes sociales, especialmente cuando trata de la seguridad de la información, es de suma importancia para una adecuada gestión de aplicaciones.
        IV. Antivirus / Antimalware.
        V. Todos los servidores de aplicaciones y sistemas de usuario final que se conectan a los servidores de aplicaciones deben tener el software antivirus/antimalware en ejecución.
        VI. Política de uso de software:
    1. Las aplicaciones de software pueden ser fuente de riesgos de varias maneras y, por lo tanto, ciertos aspectos del uso del software deben ser cubiertos por esta Política.
    2. Todo el software y las aplicaciones de redes sociales para usuarios finales que puedan descargarse en los ordenadores corporativos o en los dispositivos móviles deben ser aprobados por el Comité de Seguridad.
        I. Incidentes de seguridad:
            1) Ante la sospecha de un incidente de seguridad que pueda afectar a un dispositivo de red, deberá seguirse la norma de respuesta a incidentes del Ayuntamiento.
A. Aplicaciones hospedadas en terceros:
    I. Acuerdo de nivel de servicio: Es necesario revisar todos los acuerdos de nivel de servicio con sitios y proveedores de aplicaciones.

II. Actualizaciones: Se deben realizar todas actualizaciones que sean necesarias para solucionar problemas de seguridad.

III. Pruebas:

1. Los terceros deben aportar evidencias de las pruebas de seguridad realizadas o permitir al Ayuntamiento someter a los sistemas implicados a las adecuadas pruebas de seguridad.

2. Los terceros deben proporcionar pruebas de seguridad de la infraestructura usada, así como políticas que mantengan un entorno seguro para los datos de sus clientes.

e) Educación y entrenamiento:

I. El Responsable de Seguridad del Ayuntamiento es responsable de proponer acciones de formación a los usuarios finales sobre los requisitos de seguridad para todos los recursos de hardware y software.

II. El Servicio de Recursos Humanos es responsable de ejecutar los programas de formación propuestos.

III. Realizar un programa anual de formación/concienciación para alertar a los usuarios de nuevos riesgos y de las medidas de seguridad que los mitigan.

5. ¿Qué se puede hacer con las redes sociales y qué no se puede hacer?

A. Con las redes sociales SE PUEDE… Añadir valor, promover en el Ayuntamiento una actitud positiva, formar e informar, responder a los usuarios, participar en conversaciones, ser un recurso de conocimiento, construir relaciones, conocer las restricciones sobre el contenido, entender los riesgos de los medios, comprobar todos los hechos, proporcionar divulgaciones, obtener retroalimentación, comprobar el riesgo normativo, comprender ramificaciones legales, asegurar las comunicaciones, proteger la información de los usuarios, entender los requisitos de privacidad, etc.
B. Con las redes sociales NO SE PUEDE… Discutir información confidencial, compartir información privada de los usuarios, compartir comentarios despectivos, acceder a canales no seguros o no cifrados (si resulta de aplicación), discutir la actividad de los usuarios, publicar información interna, asociar la vida personal con las cuentas corporativas, desacreditar a otros, desacreditar a otras personas o instituciones, etc.

6. Política de "la Marca"

A. ¿Cuál es la política de "la marca" del Ayuntamiento y cuáles son las directrices para discutir y promover "la marca"?

7. Política de uso de Twitter

A. Identificar para qué se desea usar Twitter.
B. Identificar objetivos (acceso, seguimiento de "la marca", gestión de identidad, investigación, comunicaciones con los usuarios, cobertura de los medios de comunicación, etc.).
C. Identificar quién puede crear y publicar tweets.
D. Directrices respecto del contenido (Identificar requisitos de contenido tales como frecuencia, contexto, contenido, tono, uso del hashtag, seguidores, seguimiento, política de enlaces cortos, etc.)
E. Re-tuiteo y seguimiento (Áreas principales: sector público, investigación, socios, noticias de la industria, estadísticas, otros contenidos relevantes).
F. Gestión de cuentas de servicios específicos (Vincular cuentas a servicios, monitorizar cuentas específicas).

8. Política de uso de Facebook

A. Identificar para qué pretende usarse Facebook.
B. Identificar objetivos (monitorización de "la marca", marketing, compromiso con la comunidad, desarrollo de alianzas, etc.).
C. Identificar quién puede usar Facebook y publicar en las cuentas del Ayuntamiento.
D. Directrices de contenido
    1. ¿Qué contenido es adecuado y está permitido?
    2. Tipos de contenido y fuentes (tales como eventos, noticias, encuestas, fotos, etc.)
    3. Tono del compromiso e interacción con la comunidad (personal, corporativo, amistoso, profesional)
    4. Directrices generales desde una perspectiva de seguridad.

9. Política de blogs del Ayuntamiento

A. Definir el propósito de los blogs corporativos.
B. Objetivos.
C. Identificar quién es responsable de los blogs.
D. Directrices de contenido:
    1. Definir qué contenido se permite en los blogs.
    2. Identificar la política de vídeo para los blogs.

10. Política de Blogs personales

A. Identificar cómo se permite a los empleados utilizar la información del Ayuntamiento en blogs personales y en mensajes de redes sociales, y cuándo y dónde se puede acceder a los blogs personales.
    1. ¿Cuáles son las limitaciones?
    2. ¿Qué IP corporativa se puede utilizar?
    3. ¿Qué se puede decir de los servicios del Ayuntamiento?
    4. Identificar políticas relevantes de Recursos Humanos que restrinjan la difusión de información del Ayuntamiento por parte de los empleados, en cualquier forma.
    5. ¿Qué tipo de información del Ayuntamiento u otra información puede publicarse?
A. Proceso de aprobación
B. Renuncia a responsabilidades (¿Qué renuncias deben usar los empleados?)
C. Revelación o divulgación (¿Qué deben y no deben divulgar los empleados en sus blogs?
D. Aprobaciones.

14) RESPONSABLE DEL CUMPLIMIENTO

Será responsabilidad del Responsable de la Entidad velar por el cumplimiento de la presente normativa.

15) REFERENCIAS

- 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.
- Guía de Seguridad CCN-STIC 821: Normas de Seguridad.
- Guía de Seguridad de las TIC CCN-STIC 883: Guía de Implantación del ENS para Entidades Locales.
- Guía de Seguridad CCN-STIC 804: Guía de Implantación.
- 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.
- RGPD (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.
- Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales.

16) REGISTROS/ANEXOS