NORMATIVA

SEGURIDAD DE LA RED, SERVICIOS DE RED Y PERÍMETRO

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.08	DOCUMENTO:	NORMATIVA DE SEGURIDAD DE LA RED, SERVICIOS DE RED Y PERÍMETRO

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

Esta normativa recoge como objeto las medidas a aplicar, en cuanto a seguridad se refiere, para el control de las redes, servicios de red y perímetro del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

Esta normativa será de obligado cumplimiento para todo el personal del Ayuntamiento y todos los terceros que, previa autorización al efecto por parte del Ayuntamiento, utilicen o sean usuarios de red o servicios de red o accedan de forma puntual a los mismos.

Esta normativa ha sido aprobada por el Comité de Seguridad, atendiendo a las recomendaciones del Responsable de la Información, 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 todo lo dispuesto en la presente normativa será el Responsable del Sistema, que asegurará que se llevan a cabo todas las medidas descritas en la presente.

4) DESARROLLO NORMATIVO

4.1) SEGURIDAD DEL PERÍMETRO

Todas las conexiones que se intenten realizar entre la red interna del Ayuntamiento y las redes externas de uso público o privado o resto de redes de la organización, deben ser monitorizadas y filtradas, debiendo realizarse a través de una VPN. Se establecerán las reglas de filtrado mediante el uso de cortafuegos para cada tipo de usuario, o grupo de usuarios, y/o sistema de manera que exclusivamente se permita la conexión o entrada a aquellos servicios para los que se esté autorizado.

Todo el tráfico intercambiado entre las redes internas y externas deberá ser chequeado contra software malicioso (conforme a lo establecido en la Normativa de Explotación). Igualmente deberá ser analizado para detectar posibles patrones de ataque que puedan dañar los servicios ofrecidos o acceder a información no autorizada.

Es recomendable que todas las operaciones de seguridad perimetral sean realizadas por equipos dedicados a estas tareas, de forma que no impacte negativamente en la velocidad del tráfico o de otros servicios.

En el ámbito de la seguridad perimetral, se guardará registro de todos aquellos tipos de eventos que se consideren relevantes para la seguridad. En especial, los que ocasionen algún incidente de seguridad y aquellos que resulten útiles para determinar su origen y operaciones realizadas.

4.2) SEGMENTACIÓN DE REDES

Atendiendo a la red interna, ésta debe segmentarse en varias subredes que se comunicarán entre ellas cuando sea necesario. De este modo, se minimiza el riesgo de seguridad ante intentos de acceso, accidentales o intencionados, por parte del personal interno y, sobre todo, en el eventual caso de que algún sistema interno haya sido comprometido.

La segmentación física o lógica se realizará en base a los siguientes criterios:

- Tipo de usuarios con acceso permitido a sus servicios: separar usuarios internos (personal) de externos o público en general.
- Servicios: necesidades de interrelación entre los distintos servicios.

4.3) PROTECCIÓN DE LA INFORMACIÓN A TRAVÉS DE LA RED

El transporte de la información a través de la red se realizará siguiendo la NR.03.Normativa de Intercambio de Información.

Se emplearán redes privadas virtuales (VPN) cuando la comunicación discurre entre diferentes redes.

4.4) RED WIFI

En caso de que se necesitara acceso inalámbrico a la red corporativa se establecerá una red segura. La instalación de una red inalámbrica, o cualquier ampliación de la existente, mediante la instalación de nuevos puntos de acceso debe estar autorizada por el Responsable del Sistema. Además, se deberán tener en cuenta los siguientes requerimientos de seguridad generales:

- Toda la información debe viajar cifrada por la red inalámbrica y todas las conexiones deben estar autenticadas por ambas partes.
- Mecanismos de autenticación y autorización de los clientes inalámbricos.
- Un control de acceso sólido que permita el acceso de red a clientes autorizados y lo deniegue a clientes no autorizados.
- Un cifrado robusto (mínimo de 128 bits) del tráfico, por la posibilidad de que viajen datos sensibles.
- Una administración segura de las claves de cifrado.

Para cumplir dichos requerimientos, se llevarán a cabo las siguientes acciones:

- Cambiar el SSID y la clave de administrador por defecto de los puntos de acceso.
- Restringir el acceso a la interfaz Web de configuración de los puntos de acceso, cambiar la clave “SNMP” y limitar el acceso “Telnet” a determinadas direcciones IP (las de los administradores). Si el equipo cuenta con acceso por “SSH” se usará éste en lugar de “Telnet”.
- Se intentará que el radio de cobertura no exceda los límites del perímetro físico del Ayuntamiento.

4.5) OTROS ASPECTOS DE SEGURIDAD

Toda la red deberá ser, preferiblemente, conmutada, de manera que no sea posible, desde ningún equipo, la captura de información destinada a otro.

Las rutas configuradas en las tablas de los equipos (ya sean de red o servidores) deber ser las estrictamente necesarias para su funcionamiento. Para aquellos equipos que no lo requieran, debe evitarse crear rutas por defecto, de modo que se restrinja los equipos externos que pueden alcanzar a estos sistemas.

Todo cambio en la configuración de la red, se llevará a cabo de acuerdo al Procedimiento de Gestión de Cambios y Versiones.

Estará totalmente prohibida la conexión temporal de nuevos equipos a la red interna sin la correspondiente aprobación del Responsable de Seguridad, quién deberá revisarlo y estudiar los riesgos. Para la conexión de equipos con conexión temporal se habilita una red de invitados, separada de la red interna, a la cual se podrán conectar sin la aprobación del Responsable de Seguridad.

No se podrá:

- Modificar la configuración de red de ningún servidor sin la debida autorización.
- La creación o transmisión de datos que causen congestión en la red, mediante programas concebidos a tal fin.
- Realizar escuchas del tráfico que se transmite por la red.

5) RESPONSABLE DEL CUMPLIMIENTO

Será responsabilidad del Responsable de la Entidad velar por el cumplimiento de la presente normativa, bajo la supervisión y vigía del Responsable de Seguridad.

6) 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.
- NR.03.Normativa de Intercambio de Información.
- Procedimiento de Gestión de Cambios y Versiones.

7) REGISTROS/ANEXOS