NORMATIVA

CONTROL DE ACCESO A SISTEMAS,REDES Y APLICACIONES

Excmo. Ayuntamiento de Baeza

Octubre 2019

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	NR.07	DOCUMENTO:	NORMATIVA DE CONTROL DE ACCESO A SISTEMAS, REDES Y APLICACIONES

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 tiene por objeto regular el sistema de acceso y las medidas de seguridad mínima para la conexión a redes, sistemas y aplicaciones del Excmo. Ayuntamiento de Baeza (en adelante Ayuntamiento).

2) ALCANCE

El ámbito de aplicación de esta normativa se circunscribe a todos los usuarios de los sistemas, redes y aplicaciones del Ayuntamiento, ya sean personal interno o terceros que deban acceder a las mismas.

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

Será responsabilidad del Responsable del Sistema vigilar el cumplimiento de esta norma de seguridad y acceso, así como de determinar, previa consulta al responsable de la entidad y responsables de áreas o departamentos, de los perfiles de acceso de cada uno de los usuarios.

4) DESARROLLO NORMATIVO

4.1) NORMATIVA DE CONEXIÓN A TERMINALES REMOTOS Y EQUIPOS

El acceso a los sistemas operativos está monitorizado por herramientas de control y regulado por un sistema de permisos de acceso que debe pasar por un proceso de aprobación por parte del Responsable del Sistema.

Antes de validar el sistema se muestra un mensaje de advertencia general indicando que el acceso es solo para usuarios autorizados y cualquier intento no permitido será registrado e investigado.

Las credenciales únicas y personales, esto es, ID de usuario y contraseña que son insertadas para validar en el sistema operativo. Si los datos introducidos son incorrectos se solicitan de nuevo hasta un máximo de 5 intentos, si éstos se agotan, el id de usuario se bloquea durante 5 minutos. Se registra el suceso fallido, la hora, los datos del usuario y nivel de acceso.

Si los datos son correctos, se registra el suceso satisfactorio con el nombre de usuario, la fecha, la hora y nivel de acceso; finalmente, se permite el acceso al sistema.

Las contraseñas introducidas para validar en el sistema, no son visibles o mostradas en el momento de ser insertadas.

4.1.1) AISLAMIENTO DE SISTEMAS CRÍTICOS Y SENSIBLES

Para evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación, son utilizados distintos medios de seguridad para restringir el acceso a los sistemas de aplicación a usuarios no autorizados.

Los sistemas con servicios críticos y datos sensibles están disponibles en entornos de virtualización dedicados propios.

4.2) NORMATIVA DE IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS

- Los usuarios del sistema son responsables de sus credenciales de acceso (id de usuario, permisos, contraseñas…). Por lo tanto, bajo ningún concepto deben desvelar a terceros estos datos. Cualquier uso indebido causado por estas credenciales será responsabilidad del propietario de los mismos.
- A través de una política de dominio, el último usuario logado no se muestra al iniciar el sistema en la pantalla de login.

- Cada usuario del sistema que accede a la infraestructura tecnológica del Ayuntamiento cuenta con un ID de usuario único y personalizado, por lo cual no está permitido el uso de un mismo ID de usuario por varios usuarios del sistema. Cada usuario es responsable de su propio ID de usuario y su confidencialidad.
- Si por razones técnicas es necesario la existencia de IDs de usuarios genéricos estos deberán ser autorizados por el Responsable de Seguridad y la responsabilidad de este usuario genérico recaerá sobre el Responsable del Sistema correspondiente.
- Los accesos a los sistemas del Ayuntamiento son registrados con el nombre de usuario, fecha y hora.
- Los usuarios con acceso a cuentas privilegiadas deben utilizar sus cuentas personales para las tareas que no precisan de privilegios.

4.3) NORMATIVA DE USO DE LOS SERVICIOS DEL SISTEMA

El acceso a las utilidades del sistema en equipos servidores vía remota o en consola está limitado a los usuarios con permisos de acceso al sistema operativo. Por defecto en los servidores los usuarios no tienen privilegios para acceder al sistema operativo excepto usuarios privilegiados que lo necesiten para sus funciones, estos deben pertenecer al grupo local del servidor que permite conexiones remotas.

En los puestos clientes, existen una serie restricciones para evitar el uso indebido de las utilidades del sistema, dichas restricciones son las siguientes:

- El acceso a las herramientas administrativas está restringido por política de dominio para evitar el acceso a las configuraciones más básicas y sensibles del sistema. Esta restricción será aplicada a los usuarios que no necesitan estas herramientas para realizar sus funciones.
- Los usuarios que no tienen privilegios de instalación en sus propios equipos, si necesitaran realizar alguna gestión como instalaciones que precise de estos privilegios, deberán solicitarlo al Responsable del Sistema correspondiente y éste valorará si permite dicho privilegio. Una vez terminada la tarea, estos privilegios le serán revocados.
- El antivirus está protegido por contraseña para evitar que los servicios puedan ser detenidos y que la configuración sea modificada.
- El acceso remoto o por consola a servidores u otros equipos de la entidad está limitado a los grupos locales de control remoto de cada equipo.
- Está prohibida la instalación de cualquier software que no haya sido autorizado previamente.
- La grabación a CDs o DVDs está restringida en los equipos.
- Se prohíbe cualquier tipo de acción o comportamiento que vaya en contra de la seguridad física y/o lógica de los recursos asociados a la red organizativa y cualquier software o herramienta que puedan afectar a la estructura de red del Ayuntamiento.
- No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.
- Con respecto al CPD, al igual que los servidores internos, los usuarios que tienen acceso a estos sistemas no son administradores de los mismos, el control de acceso a aplicaciones fuera de las determinadas para sus funciones está restringido.

4.4) NORMATIVA DE DESCONEXIÓN AUTOMÁTICA DE TERMINALES

Para evitar el acceso no autorizado a un sistema desatendido debido a que el usuario propietario no se encuentra en su puesto de trabajo, se han establecido unas políticas de desconexión y bloqueos automáticos encaminados a proteger los sistemas desprotegidos y evitar así la interferencia, manipulación, robo o uso indebido de los sistemas a los cuales tiene acceso el usuario responsable. Las medidas establecen las siguientes recomendaciones y restricciones:

- El usuario es responsable de su ID de usuario y del uso o acciones que puedan realizarse con dicho ID. El usuario debe bloquear o desconectar sus sesiones de los distintos sistemas a los cuales accede cuando vaya a ausentarse de su puesto de trabajo.
- La política global del dominio establece una desconexión automática de las sesiones remotas que superen las 2 horas de inactividad en todos los sistemas. Seguidamente, se registran el ID de usuario junto con la hora y fecha de la desconexión.

4.5) DESCRIPCIÓN DE LA AUTENTICACIÓN DEL USUARIO PARA CONEXIONES VPN AL AYUNTAMIENTO

La conexión remota a la red del Ayuntamiento se realizará siempre a través de una red privada virtual (VPN) cifrada.

La conexión remota a la red del Ayuntamiento solo se podrá llevar a cabo con activos municipales.

La conexión VPN se realiza mediante el software GlobalProtect. La conexión es cifrada mediante IPSEC-ESP con el algoritmo AES-CBC-256 y SHA256.

La autentificación se llevará a cabo con certificado de empleado público que estará contenido en su tarjeta criptográfica.

Una vez autenticado, el usuario estará restringido por un perfil previamente configurado por el administrador del Sistema para garantizar el mínimo acceso necesario basado en los requerimientos de la petición de acceso. Estos perfiles garantizarán acceso a la máquina del usuario para que trabaje tal y como si estuviera en el Ayuntamiento.

5) RESPONSABLE DEL CUMPLIMIENTO

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

7) REGISTROS/ANEXOS