

2. En los supuestos en que el espacio afectado figure en la confluencia de dos o más calles clasificadas en distinta categoría, se aplicará la tarifa correspondiente a la calle de categoría superior.

San Bartolomé, a cinco de noviembre de dos mil cuatro.

EL ALCALDE- PRESIDENTE, Miguel Martín Betancort.

5.276-E

ILUSTRE AYUNTAMIENTO DE SAN BARTOLOMÉ DE TIRAJANA

Concejalía de Nuevas Tecnologías

EDICTO

6.609

Habiendo transcurrido el período de exposición pública del Reglamento sobre seguridad de la información, para su entrada en vigor en el presente ejercicio, sin que se hayan presentado alegaciones o reclamaciones, y de conformidad con el artículo 49.c de la Ley 7/1985, de 2 de abril Reguladora de las Bases de Régimen Local, se entiende aprobada definitivamente el indicado reglamento, publicándose su texto íntegro, a los efectos de su entrada en vigor.

REGLAMENTO SOBRE SEGURIDAD DE LA INFORMACION

Introducción

La dependencia cada vez mayor de los servicios y sistemas de información hacen que las organizaciones sean cada vez más vulnerables a las amenazas de seguridad. La interconexión de redes públicas y privadas y la compartición de los recursos de información incrementan la dificultad de conseguir asegurar los controles de acceso a los mismos.

La información es un activo el cual, como cualquier otro activo de la organización, tiene un valor y consecuentemente necesita ser adecuadamente protegido. La información puede encontrarse en diferentes formatos. Puede ser impresa o escrita, almacenada electrónicamente, transmitida por correo o usando medios electrónicos. Cualquier forma en que la información se encuentre

o medio por el cual es compartido o almacenado sería siempre protegido apropiadamente.

Los componentes hardware y software representan una inversión monetaria que debe ser protegida.

El uso de las tecnologías de la información para un propósito para el cual no fueron dispuestos por nuestra organización representan una pérdida de valor y posiblemente una pérdida de reputación o la violación de la Ley.

La corporación del Ayuntamiento de San Bartolomé de Tirajana reconociendo el valor que tiene la información que usa para su gestión diaria a través de las tecnologías de la información y la dependencia cada vez mayor de los servicios y sistema de información para un adecuado servicio al ciudadano, reconoce su obligación de establecer unos criterios de seguridad para toda la tecnología de la información que se encuentra bajo su propiedad y control: datos, software, hardware, redes, telecomunicaciones y operaciones de procesamiento de información. Los empleados del Ayuntamiento de San Bartolomé de Tirajana comparten esta obligación al igual que cualquier otro usuario que use la infraestructura de las tecnologías de la información del Ayuntamiento.

TÍTULO I. OBJETIVOS Y ALCANCE

Artículo 1. El presente reglamento tiene por objeto establecer las medidas de protección y seguridad técnica a aplicar en el trabajo con las tecnologías informáticas, las que incluyen los medios técnicos y los programas, así como establecer las normas de disciplina informática.

Artículo 2. A los efectos de este reglamento se entenderá por Protección y Seguridad Técnica de los Sistemas Informáticos al conjunto de medidas administrativas, organizativas, físico-tecnológicas, técnicas, legales y formativas dirigidas a preservar la confidencialidad, integridad y disponibilidad de la información procesada por medios informáticos.

Artículo 3. Definición de términos

- Confidencialidad: Asegurar que la información es accesible solo a las personas autorizadas. Privacidad de la información del Ayuntamiento y personal.

- Integridad: Asegurar que la información y los métodos de procesamiento son precisos.

- Disponibilidad: Asegurar que los usuarios autorizados tienen acceso a la información cuando lo requieran. Completa funcionalidad de los sistemas y sus componentes.

Artículo 4. Se definen los siguientes dominios de seguridad para la gestión de la Seguridad de la Información del Ayuntamiento:

- Seguridad del PC: CPU, periféricos, sistema operativo, seguridad de los datos.

- Seguridad física: Lugares ocupados por tecnologías de la información por personal y equipos.

- Seguridad operacional: Control ambiental, equipos de suministro eléctrico, actividades de operación.

- Seguridad de procedimiento: Gestión, personal, compras

- Seguridad de comunicaciones: Equipos de comunicaciones, personal, medios de transmisión.

Artículo 5. Este Reglamento será de aplicación en todas las concejalías, departamentos y sus dependencias y otras entidades que dependan del Ayuntamiento. Siendo de obligado cumplimiento por todas las personas que participen en la elaboración, uso, aplicación, explotación y mantenimiento de las tecnologías informáticas.

TÍTULO II. FUNCIONES Y RESPONSABILIDADES

Artículo 6. La aprobación de este Reglamento y sus modificaciones corresponde al Pleno Municipal, conforme al procedimiento establecido en el artículo 49 de la Ley 7/1985, de 2n de Abril, reguladora de las Bases del Régimen Local.

Artículo 7. El coordinador de la Concejalía de Nuevas Tecnologías se encargará de valorar y elevar informe técnico sobre las modificaciones al presente reglamento.

Artículo 8. El servicio de Desarrollo Tecnológico será el encargado del mantenimiento e implementación de las políticas de seguridad establecidas.

Artículo 9. Cada miembro del personal del Ayuntamiento de San Bartolomé de Tirajana y entidades que dependan del ayuntamiento será responsable de cumplir los estándares de comportamiento sobre seguridad informática establecidos en este reglamento.

Artículo 10. La responsabilidad de la seguridad informática de cada sistema es la siguiente:

- Desarrollo Tecnológico será el responsable de todas las plataformas estratégicas de sistemas de información.

- Desarrollo Tecnológico será el responsable de los sistemas de comunicación estratégicos.

- Los departamentos serán responsables de las aplicaciones bajo su control de gestión.

- El personal del Ayuntamiento será responsable de los sistemas personales bajo su control.

Artículo 11. Todo el personal que use los recursos de sistemas de información y comunicaciones del ayuntamiento de San Bartolomé de Tirajana:

- Operará y se comportará bajo los requisitos que figuran en los anexos I, II y III de este reglamento.

- Es responsable del cuidado y uso adecuado de los recursos informáticos bajo su control.

Artículo 12. Los estándares, que son obligatorios, y las guías, que son sugerencias, se publicarán como Anexo a este reglamento para ayudar a los usuarios y responsables de sistemas a cumplir con sus responsabilidades de seguridad informática. Los estándares y guías, aunque sean anexos, son parte integral de la política de seguridad de este Ayuntamiento y por tanto la define en detalle.

Artículo 13. El Reglamento de seguridad debe ser accesible en todo su contenido al personal del Ayuntamiento, por tanto es responsabilidad de cada jefe de departamento hacerla llegar a todo el personal bajo su responsabilidad para su conocimiento y aplicación y así mismo será publicado en la web del Ayuntamiento para su consulta.

Artículo 14: El Reglamento de seguridad es un documento “vivo” que será modificado cuando sea requerido por cambios en la tecnología, aplicaciones, procedimientos, imperativos legales y sociales, peligros percibidos, etc., ...

Los cambios que afecten al reglamento de seguridad en su aspectos fundamentales serán realizados mediante informe del Coordinador de Nuevas Tecnologías y aprobados por el Alcalde-Presidente o Concejal en quien delegue.

Los cambios menores al Reglamento de seguridad serán aprobados por el Coordinador de Nuevas Tecnologías.

Cualquier cambio a este documento será comunicado por el Coordinador de Nuevas Tecnologías y es responsabilidad de los jefes de departamento el comunicar los mismos a los empleados bajo su cargo.

TÍTULO III. GUÍAS SOBRE CONTRASEÑAS

Artículo 15. Gestión de las contraseñas:

- Las contraseñas deben ser memorizados – nunca escritas en ningún medio
- Las contraseñas son personales e intransferibles, por lo tanto nunca deben ser compartidas con otras personas
- Las contraseñas se cambiarán cada 4 meses o inmediatamente si la seguridad de los sistemas se ve comprometida.

Artículo 16. Las contraseñas serán puestas por los usuarios en el sistema, para ello una vez dado de alta el usuario el procedimiento le solicitará que la cambie de forma automática.

En caso de cualquier comunicación de algún tipo de contraseña este se hará por escrito al usuario previa identificación, nunca por teléfono o e-mail.

Artículo 17. Construcción de las contraseñas:

Se debe elegir una contraseña que sea difícil para otra persona adivinar o crackear.

Se deben seguir las siguientes normas para elegir un contraseña:

- Deben tener al menos 6 caracteres
- Nunca la contraseña debe ser un nombre o algo familiar, como la mascota, el hijo o cónyuge, ni fechas de nacimiento, etc. ya que son fáciles de adivinar.
- Nunca, bajo ninguna circunstancia, una contraseña puede ser la misma que el nombre de usuario o su nombre real.
- No use palabras que se asocien con Vd.

- No use una contraseña que sea una palabra de diccionario. Los programas básicos de crack contienen esas palabras.

- Mezcle en su contraseña números y letras. Añada un “%” o “\$” hacia la mitad de la contraseña.

- Elija algo que se pueda recordar, que pueda escribir rápida y concisamente e incluya caracteres distintos a las letras minúsculas.

TÍTULO IV. CÓDIGO DE PRÁCTICAS DEL PERSONAL DEL AYUNTAMIENTO

Artículo 18. El acceso a la red del Ayuntamiento es proporcionado por el Ayuntamiento de San Bartolomé de Tirajana para propósitos administrativos. La red del Ayuntamiento se considera un recurso valioso pero limitado que debe ser compartido por todos. Es obligación del personal del ayuntamiento usar las facilidades de dicha red de forma eficiente, ética, legal y responsable, de acuerdo con “Código de Prácticas para el uso de ordenadores y facilidades de red” y el código de conducta que se especifica en este título. Una conducta inadecuada puede dar lugar a que no se le conceda acceso a los recursos de dicha red o ser materia de otro tipo de sanciones disciplinarias según la gravedad del hecho.

Artículo 19. Gestión de cuentas:

- La cuenta de usuario se proporciona por el Ayuntamiento para uso exclusivo de dicho usuario.
- La contraseña y cuenta de usuario no se deben compartir con familia, amigos o cualquier otra persona.
- Cada 4 meses se cambiará la contraseña
- No se puede usar la cuenta de otra persona . Si de forma inadvertida se obtiene acceso a información no autorizada se tiene la obligación de ponerlo en conocimiento del servicio de Desarrollo Tecnológico.
- En ciertas circunstancias se puede compartir una cuenta con otros, dicha compartición debe ser autorizada por el Coordinador de Nuevas Tecnologías. En tal caso todos los que la compartan son responsables por igual del uso de la cuenta.
- No se debe intentar descubrir la contraseña de otro usuario o acceder a su cuenta con un nombre de usuario desautorizado.

Artículo 20. Conducta electrónica adecuada.

Los usuarios de Internet y la red del Ayuntamiento deben cumplir con la guía de buena conducta de red. La guía de buena conducta de red se basa en el uso de la buena educación y el sentido común.

- Limitar los correos electrónicos a una pantalla de texto siempre que sea posible.

- No enviar grandes ficheros adjuntos en los e-mails

- No usar lenguaje ofensivo

- Sea educado con el resto de usuarios de la red del Ayuntamiento e Internet.

Artículo 21. Actividades ilegales.

- Está prohibido la descarga, copia o instalación de software sin la licencia o permiso apropiado.

- Está prohibido cualquier intento de introducir virus o intentos de “pirateo informático”.

- Esta prohibido transmitir cualquier tipo de material que sea obsceno, ofensivo, calumnioso, que dañe los ficheros o programas de otros o que violen cualquier ley aplicable.

TÍTULO V. PRINCIPIOS DE PRIVACIDAD DE LOS DATOS

Artículo 22. El personal que use los recursos informáticos del Ayuntamiento de San Bartolomé de Tirajana está sujeto a la normativa actualmente vigente sobre protección de datos de carácter personal y es deber de cada responsable de departamento hacer las inscripciones ante la agencia de protección de datos de los ficheros de carácter personal que dicho departamento maneje.

Artículo 23. Los siguientes principios de privacidad serán de obligado cumplimiento para el personal que use los recursos informáticos del Ayuntamiento.

- Principio de limitación de recogida de datos: La recogida de datos de carácter personal será realizada con el conocimiento y consentimiento de la personas.

- Principio de calidad del dato: Los datos de carácter personal serán utilizados para los propósitos para los cuales serán solicitados. Serán precisos, completos y actualizados.

- Principio de especificación de propósito: Siempre se especificará el propósito para el cual se recogen los datos de carácter personal y el uso que se les va a dar.

- Principio de limitación de uso: Los datos personales no serán suministrados o usados para otros propósitos que los especificados, excepto que exista consentimiento de la persona o requerimientos legales.

- Principio de transparencia: Habrá siempre una política de transparencia sobre desarrollos, prácticas y políticas con respecto a los datos personales. Esto quiere decir que será fácilmente accesible la información sobre la existencia y naturaleza de los ficheros de carácter personal y el propósito de su uso, así como la identidad del responsable de dichos ficheros.

- Principio de participación individual: Cualquier persona tendrá derecho a:

- a. Obtener datos sobre la información que el Ayuntamiento tenga sobre ella.

- b. Acceder a sus datos personales en tiempo y forma razonable y comprensible, previa identificación.

TÍTULO VI. PLATAFORMAS DE SISTEMA ESTRATÉGICO

Artículo 24. Se entenderá por sistema estratégico aquel que satisfaga alguno o varios de los siguientes criterios:

- Es crítico para el desarrollo de la misión del Ayuntamiento de San Bartolomé de Tirajana

- Afecta a gran parte del Ayuntamiento de San Bartolomé de Tirajana

- Ayuda a aumentar el servicio que presta el Ayuntamiento de San Bartolomé de Tirajana

- Es caro

Artículo 25. Gestión de los sistemas estratégicos.

La gestión de la plataforma estratégica y sus programas asociados será llevada a cabo por el servicio de Desarrollo Tecnológico.

Artículo 26. Seguridad Física.

Se cumplirán con los siguiente estándares de seguridad física en los sistemas estratégicos:

- Los locales donde se alojen dichos sistemas deben estar físicamente aislados de riesgos inaceptables como inundaciones, vibraciones, polvo, exceso de temperatura, etc., ...

- La humedad y la temperatura debe ser controlada dentro de unos límites aceptables

- La plataforma debe tener protección eléctrica vía UPS que proporciones lo siguiente:

- a. 15 minutos de operación en caso de fallo de suministro eléctrico

- b. Adecuada protección contra subidas inesperadas de tensión

- c. Apagado ordenado de equipos cuando sea necesario

- Habrá detectores de temperatura, humo, fuego y agua en las salas donde se alojan los sistemas estratégicos.

Artículo 27. Acceso Físico

Las puertas de acceso externo a los sistemas estratégicos permanecerán cerradas con medios electrónicos.

Sólo el personal de Nuevas Tecnologías (Servicio de Desarrollo Tecnológico y el Servicio de Innovación Tecnológica) está autorizado a estar en la sala que alberga los sistemas estratégicos. En caso de que otro personal necesite acceder a dicha sala, siempre estará acompañada e identificada por una persona del servicio de Desarrollo Tecnológico.

Artículo 28. Acceso de los usuarios

El alta de nuevos usuarios para acceder al sistema se gestionará como sigue:

- Se debe remitir una solicitud firmada por el responsable del departamento al cual pertenece la persona

- La solicitud debe recoger el nombre y apellidos de la persona, departamento, teléfono de contacto, D.N.I. y nivel de acceso permitido.

- La solicitud será remitida al coordinador de Nuevas Tecnologías quien tras validarla la remitirá al servicio de Desarrollo Tecnológico, quien la guardará de forma indefinida,

- La primera vez que el usuario haga login en el sistema se forzará el cambio de contraseña.

Los usuarios que dejen de ser personal del Ayuntamiento de San Bartolomé de Tirajana o no requieran acceso serán deshabilitados. Todos los ficheros que le pertenezcan serán puestos a disposición del jefe del departamento correspondiente. Los jefes de departamento están obligados a comunicar por escrito cualquier baja o cambio del nivel de acceso del personal de su departamento.

Artículo 29. Integridad de los datos

- Las copias de seguridad de todos los datos del sistema estratégico se harán todos los días laborables.

- El régimen de copias de seguridad debe satisfacer los siguientes requisitos

- a. Poder recuperar el trabajo con una semana de antelación

- b. Proporcionar al menos un nivel de copia de seguridad adicional a un tiempo anterior a esa semana, para cubrir en caso de fallo de la primera copia de seguridad.

- Se realizará una validación de la copia de seguridad al menos una vez cada seis meses.

Artículo 30. Validez de contraseñas

Será forzado por sistema operativo el cambio automático de contraseña. La vida de una contraseña será de 4 meses salvo circunstancias que aconsejen su cambio inmediato.

Artículo 31. Plan de recuperación de desastres

Habrà un plan de recuperación de desastres para cada sistema estratégico.

Artículo 32. Documentación

Los procedimientos que reflejan este reglamento deben ser documentados por el servicio de Desarrollo Tecnológico, en sus instrucciones de operación.

TÍTULO VII. COMUNICACIONES

Artículo 33. El acceso a la red se puede clasificar en cinco grandes áreas:

- Redes de área local
- Accesos externo vía módem
- Redes interedificios
- Redes de otros organismos (Policía nacional, ...)
- Redes de área extensa (Internet)

El Ayuntamiento toma distintas decisiones de control que afectan a la gestión de seguridad de estas áreas:

- Control total sobre las redes de área local, accesos externo vía módem y redes interedificios, ya que el servicio de Desarrollo Tecnológico debe planificar, instalar, gestionar y mantener estos sistemas.

- Control limitado sobre las redes de otros organismos, que son gestionadas por ellos mismos.

- Ningún control sobre Internet.

Artículo 34. Redes de área local. Seguridad física.

Los siguientes estándares de seguridad física sobre las redes de área local deben satisfacerse:

- Los locales que albergan el equipo de control de red deben estar libres de riesgos de inundación, vibración, polvo, temperatura, ...

- La distribución de cables dentro de techos, paredes o pisos deben estar dentro de conductos de protección.

- Temperatura y humedad deben ser controlados dentro de los límites definidos por los equipos.

- La electrónica de red debe ser alimentada vía una UPS que proporcione un mínimo de 10 minutos de corriente en caso de falta de suministro eléctrico y protección contra picos de corriente eléctrica.

Artículo 35. Redes de área local. Acceso físico

El acceso a áreas que alberguen electrónica de red será controlada por personal designado por el servicio de Desarrollo Tecnológico.

Las puertas a las áreas que albergan la electrónica de red permanecerán cerradas con una llave. De dicha llave existirán dos copias, cuya ubicación será determinada por el coordinador de Nuevas Tecnologías.

Sólo aquellos ordenadores pertenecientes al patrimonio del Ayuntamiento se les permite la conexión a la red del Ayuntamiento. El personal externo que desee acceder a la red debe tener autorización del Coordinados de Nuevas Tecnologías, previa consulta al departamento de desarrollo tecnológico y tras su puesta en conocimiento al Alcalde, que tendrá siempre la última palabra.

Artículo 36. Redes de área local. Interfaz vía módem.

Está prohibido conectar módem capaz de recibir llamadas entrantes a la red del Ayuntamiento sin el expreso permiso del departamento de Sistemas de Desarrollo Tecnológico que estudiará cada caso en particular.

Artículo 37. Red interedificios.

La red interedificios será un sistema operado y gestionado por el servicio de Desarrollo Tecnológico quien establecerá las políticas para la gestión y operación de dicha red.

Artículo 38. Redes de otros organismos y redes de área extensa.

La protección de entrada ilegal desde redes de otros organismos y redes de área extensa se proporciona generalmente a través de firewalls, como norma general está prohibido cualquier tráfico entrante de estas redes de área extensa.

El riesgo de transmitir información sobre una Wan debe ser valorado por el departamento de Sistemas de Desarrollo Tecnológico teniendo en cuenta para ello la naturaleza de la información a ser enviada sobre la Wan y garantizando la aprobación sobre seguridad de nuevas aplicaciones que incluya transmisión de información sobre la Wan.

TÍTULO IX. CONTROL DE CAMBIO DE SOFTWARE

Artículo 39. Definición

El cambio de software cubre el control de todos los aspectos de los sistemas de software estratégicos incluyendo los sistemas operativos, los sistemas de

bases de datos, utilidades de sistemas operativos, aplicaciones desarrolladas por el Ayuntamiento y terceros, junto con cualquier procedimiento y documentación para el soporte y ejecutarlos.

Artículo 40. Obligaciones generales

Cuando sean requeridos cambios al software es obligado que dichos cambios sean:

- Apropiadamente autorizados y aprobados
- Hechos mediante consulta al servicio de Desarrollo Tecnológico
- Probados
- Documentados
- Implantados en un tiempo apropiado

Cualquier cambio debe ser transferido al entorno de producción cuando se aprueba por el responsable del servicio de Desarrollo Tecnológico correspondiente.

La gestión de seguridad del software requiere definir los procedimientos para gestionar el control de cambios en sistemas y aplicaciones.

Todo el software operacional relacionado con sistemas estratégicos deben ser sometidos a los procedimientos de Gestión de Configuración que se definan.

Artículo 41. Responsabilidades de control de cambios

Personal específico tendrá la responsabilidad para implementar cambios mediante la supervisión de las pruebas en el entorno establecido para ello y sujeto a las aprobaciones apropiadas para moverla al entorno de producción. Todos los elementos del sistema estarán sujetos a Procedimientos de Control de cambio de software.

Habrà una separación de responsabilidades en la transferencia de software desde el entorno de prueba al de producción.

Artículo 42. Entorno de control de cambios

Se mantendrá tres entornos separados para cada sistema estratégico:

- Desarrollo

- Prueba

- Producción

La migración entre entornos será realizado después de obtener las firmas apropiadas como se especifica en el Procedimiento de control de cambio de software.

El nuevo software y los cambios al software existente se preparará en el entorno de desarrollo por el personal del departamento de programación del servicio de Desarrollo Tecnológico. Las aplicaciones serán diseñadas y codificadas de acuerdo a la metodología de desarrollo del Ayuntamiento.

Una vez valorada como satisfactorio, el software nuevo o modificado será transferido al entorno de prueba para las pruebas de aceptación de acuerdo a un procedimiento de pruebas acordado. Los cambios al software no están permitidos en el entorno de prueba.

Una vez completadas con éxitos las pruebas y aprobadas por el departamento de Sistemas, el software nuevo o modificado se transferirá al entorno de producción para su implementación bajo el control del servicio de Desarrollo Tecnológico. Se establecerá un plan de contingencia para la restauración a la versión anterior en el caso que la implementación no tenga éxito.

Artículo 43. Documentación

- Procedimiento de Control de Cambio.

El procedimiento de control de cambios se reflejará la documentación necesaria para este procedimiento

- Petición de cambio de software.

Ningún cambio de software será realizado sin una Petición de Cambio de Software debidamente autorizada por el responsable del servicio que lo realiza. La petición de servicio es la documentación principal que se completará por el proceso de gestión de cambio de software.

- Documentación técnica, operaciones y usuario final

La documentación apropiada, con respecto a cada cambio de software, debe ser cumplimentada con suficiente detalle y aceptada antes de que el cambio se implemente en el entorno de producción.

TÍTULO X. CONDICIONES DE USO DE INTERNET

Artículo 44. Alcance

Los nuevos recursos, servicios y la interconectividad disponible vía Internet introduce nuevas oportunidades y riesgos. En respuesta a los riesgos, este título describe la política oficial de seguridad con respecto a Internet. Se aplica a cualquier persona o entidad que usa Internet mediante algún ordenador o recurso del Ayuntamiento de San Bartolomé de Tirajana.

Artículo 45. Transmisión de información. Descargas.

Todo el software descargado desde Internet debe ser comprobado mediante software de detección de virus antes de ser instalado. Si el suministrador de dicho software no es de confianza, dicho software será probado sobre máquinas aisladas que no sean de producción.

Artículo 46. Transmisión de información. Información sospechosa

Toda la información obtenida de Internet será considerada sospechosa hasta ser confirmada por otras fuentes de información. No existen procesos de control de calidad de la información sobre Internet y mucha cantidad de la información proporcionada está desfasada o es imprecisa.

Artículo 47. Transmisión de información. Contactos

A los contactos realizados a través de Internet no se le confiarían información del Ayuntamiento a menos que ciertos pasos previos y razonables hayan sido realizados para asegurar la legitimidad de dichos contactos. Esto se aplica al suministro de cualquier información interna del Ayuntamiento.

Artículo 48. Transmisión de información. Seguridad de la información

La intervención de las conexiones y los mensajes es un hecho que ocurre frecuentemente en Internet, por ello la información propiedad del Ayuntamiento no debe ser enviada a través de internet a menos que previamente haya sido encriptada por métodos aprobados. Las contraseñas y otros parámetros que se pueden usar para obtener acceso a los servicios, redes y sistemas del Ayuntamiento no deben ser enviados a través de internet sin encriptación previa.

Artículo 49. Seguridad del software

Cualquier tipo de información interna, software o documentación del Ayuntamiento no debe ser transferida a ningún tercero sin autorización expresa del Alcalde-Presidente.

Los intercambios de software y/o datos entre el Ayuntamiento y terceras partes a través de Internet no se pueden realizar a menos que exista un acuerdo escrito que esté firmado por ambas partes. Tal acuerdo debe especificar los términos del intercambio, así como las formas en que el software y/o datos serán manejados y protegidos.

El Ayuntamiento apoya decididamente un estricto cumplimiento de los acuerdos de licencia de los vendedores de software. El cumplimiento de estos acuerdos está sujeto a auditorías realizadas por dichos vendedores. El uso de los recursos de red o de ordenadores del Ayuntamiento para la copia de software de forma no acorde a la licencia del vendedor está estrictamente prohibida.

Artículo 50. Seguridad Personal. Privacidad

El personal que usa Internet tendrá en cuenta que sus comunicaciones no son automáticamente protegidas de ser vistas por terceras partes. A menos que la encriptación se use, el personal del Ayuntamiento no enviará información considerada privada a través de Internet.

De igual modo, y para evitar posibles manipulaciones de la información por personas ajenas al Ayuntamiento, los equipos informáticos se bloquearán automáticamente cada 30 minutos.

Artículo 51. Seguridad Personal. Representaciones públicas

El personal del Ayuntamiento puede indicar su pertenencia al mismo a través de Internet. Este hecho puede ser realizado explícitamente o puede ser realizado implícitamente a través por ejemplo de la dirección de correo electrónico. En cualquier caso, cuando el personal proporcione su pertenencia, deben indicar claramente que las opiniones que expresen son personales y no necesariamente la opinión del Ayuntamiento de San Bartolomé de Tirajana. Todas las representaciones externas del Ayuntamiento deben ser autorizadas por el Alcalde-Presidente. Cuando se incluya la pertenencia al Ayuntamiento a través de un mensaje de Internet

o adjuntos a los mismos, está prohibido cualquier tipo de ataque escrito, palabras injuriosas o malsonantes.

El personal no debe enviar a través de internet cualquier tipo de información que puede afectar de manera negativa la imagen pública del Ayuntamiento o sus relaciones externas.

Se debe tener cuidado para estructurar de forma adecuada comentarios y cualquier opinión que se envíe o publique a través de Internet. Si un trabajador está trabajando en colaboración con terceros, organismos o instituciones, toda la información de ese proyecto debe ser clarificada y validada con el Alcalde-Presidente antes de ser colocada de forma pública en Internet.

Artículo 52. Control de acceso

Todos los usuarios que deseen establecer una conexión con los ordenadores del Ayuntamiento vía Internet deben autenticarse en un firewall con el fin de obtener acceso a la red interna del mismo.

Queda prohibido que el personal del Ayuntamiento pueda establecer conexiones vía módem, de Internet u otras conexiones externas que pudieran permitir a personal que no sea del Ayuntamiento obtener acceso a sistemas y/o información del Ayuntamiento y sus redes.

Salvo autorización expresa del Alcalde-Presidente queda prohibido que los usuarios utilicen conexiones existentes o nuevas a Internet.

Artículo 53. Informe de problemas de seguridad

Todo el personal del Ayuntamiento tiene el deber de informar al servicio de Desarrollo Tecnológico en los siguientes casos:

- Información sensible al Ayuntamiento que ha sido perdida, revelada a terceras partes no autorizada o se sospecha de ello.

- Uso desautorizado de sistemas de información o sospechas de haberse hecho.

- Contraseñas u otros sistemas de control de acceso han sido perdidos, robados o revelados o se sospecha de ello.

- La existencia de una forma de actuar poco usual de los sistemas, tal como ficheros perdidos, frecuentes roturas del sistema, mensajes de pérdida de rutas, ...

Los usuarios de los sistemas de información del Ayuntamiento tienen prohibido probar los mecanismos de seguridad del Ayuntamiento. Si los usuarios prueban los mecanismos de seguridad, las alarmas de los sistemas se activarán y recursos del Ayuntamiento se activarán innecesariamente para seguir dicha actividad por ello se iniciará un procedimiento disciplinario.

Los ficheros que contengan herramientas de hacking u otro material sospechoso se pueden tomar como primera evidencia de una actividad desautorizada de hacking y puede exponer al usuario a procedimientos disciplinarios.

Artículo 54. Sanciones

La violación de estas políticas de seguridad pueden ocasionar la aplicación de medidas disciplinarias, recogidas en la normativa que sobre el personal funcionario y laboral está vigente a tales efectos.

TÍTULO XI. CONDICIONES DE USO DEL CORREO ELECTRÓNICO

Artículo 55. El correo electrónico proporcionado por el Ayuntamiento de San Bartolomé de Tirajana se usará con propósitos administrativos. El uso de dichos correos se registrará por la normativa de seguridad del Ayuntamiento y las leyes vigentes a nivel autonómico y estatal.

Artículo 56. Uso y responsabilidad de los usuarios

El correo electrónico puede ser informal como una llamada telefónica o formal como un informe del Ayuntamiento, por estas razones, los usuarios son responsables del contenido, distribución y gestión de los mensajes que ellos envían. Esta responsabilidad implica los siguientes puntos:

- No contener información que sea dañina para el Ayuntamiento o los miembros del mismo.

- Ser corteses y educados

- Ser consistentes con las políticas del Ayuntamiento

- Proteger los derechos de privacidad y confidencialidad
- No contener material obsceno, ofensivo ni calumnioso
- No usarse para propósitos contrarios con los intereses del Ayuntamiento
- Contener una firma precisa, apropiada e informativa
- No sobrecargar el sistema de correos innecesario o frívolos (es decir el spam y el correo basura no está permitido)
- No puede ser usado para propósitos comerciales a menos que sea autorizado por el Alcalde-Presidente.

Los correos electrónicos que contengan una aprobación formal, una autorización o delegación deben ser impresos y archivados apropiadamente como evidencia.

Artículo 57. Confidencialidad y seguridad

- El correo electrónico es no seguro implícitamente
- Se recomienda que el material personal no se almacene o envíe a través de los equipos del Ayuntamiento.
- Los usuarios deben asegurar la integridad de sus contraseñas y seguir la política del Ayuntamiento sobre seguridad de los mismos.
- El material confidencial de especial sensibilidad no se enviará por correo electrónico a menos que se encripte.
- Los mensajes de correo electrónico pueden ser falsificados del mismo modo que un fax, por lo tanto si un mensaje es sospechoso, los usuarios verificarían su autenticidad vía teléfono o fax.

Artículo 58. Los usuarios serán responsables de cualquier pérdida o daño que se de en los sistemas del Ayuntamiento por el uso inadecuado del correo electrónico.

Artículo 59. El Ayuntamiento no tiene responsabilidad y no proporciona garantías contra mensajes, datos y ficheros no entregados o perdidos a través del correo electrónico. El Ayuntamiento no acepta ninguna responsabilidad por pérdidas que sean consecuencia de un uso inadecuado o cualquier otra circunstancia.

TÍTULO XII. CONDICIONES DE USO DE LOS ORDENADORES Y LAS REDES

Artículo 60. Los ordenadores y redes del Ayuntamiento se proporcionan para uso estricto en labores administrativas que den apoyo a la misión y razón de ser del Ayuntamiento. El Ayuntamiento se reserva el derecho a limitar, restringir o extender el acceso a los mismos.

Artículo 61. Todo el personal que use ordenadores y redes del Ayuntamiento será responsable de su uso apropiado tal como se especifica en el “Código de prácticas de uso de los ordenadores y redes” que figuran en el anexo de este reglamento y seguirán las condiciones y normas de uso que publicará el Administrador del sistema.

Artículo 62. Los ordenadores y redes del Ayuntamiento no serán usados para actividades no relacionadas con el mismo sin una autorización escrita del Alcalde-Presidente. En caso de disputa de cómo el trabajo se lleva a cabo sobre los ordenadores y redes del Ayuntamiento la decisión sobre la misma la tomará el Coordinador de Nuevas Tecnologías o quien delegue y será definitiva.

Artículo 63. Los usuarios no grabarán o procesarán información que sepan infringen las leyes de protección de datos o de copyright.

Artículo 64. El Ayuntamiento se esforzará en proteger la confidencialidad de la información y el material usado por los usuarios y formará a todo el personal para proteger la confidencialidad de la información y material, y será responsabilidad del usuario un mal uso del mismo.

Artículo 65. El Ayuntamiento se esforzará para salvaguardar la posibilidad de pérdida de información dentro de las redes y ordenadores del mismo pero no será responsable ante el usuario de tal pérdida. El usuario debe tomar las medidas para salvaguardar la información ante cualquier pérdida de la misma solicitando en caso necesario la colaboración del personal de la Concejalía de Nuevas Tecnologías.

Artículo 66. El uso de ordenadores y redes del Ayuntamiento se permite bajo la condición de que no se infrinja ninguna ley o derechos de copyright del software que se usa. Los usuarios responderán personalmente ante cualquier acción o demanda en

contra del Ayuntamiento por el uso de material en sus ordenadores que no respete las leyes o derechos de copyright vigentes.

Artículo 67. La información de los usuarios de ordenadores y redes del Ayuntamiento en el momento en que cesan de sus funciones en el mismo (es decir no es personal de este Ayuntamiento) puede ser borrada de los mismo sin serles notificado. Los usuarios deben borrar su información o disponer los medios adecuados para su retención antes de abandonar el Ayuntamiento.

Artículo 68. El Ayuntamiento se reserva el derecho de limitar permanentemente o restringir a cualquier usuario el uso de los ordenadores o redes del Ayuntamiento sin notificar al usuario con el fin de proteger la integridad de los ordenadores y redes contra uso desautorizado o inadecuado.

Artículo 69. El Ayuntamiento por medio de personal autorizado se reserva el derecho de comprobar periódicamente y monitorizar los ordenadores y redes, reservándose cualquier otro derecho necesario para protegerlos.

Artículo 70. El Ayuntamiento se reserva el derecho a llevar acabo acciones de emergencia para salvaguardar la integridad y seguridad de los ordenadores personales y redes. Estas acciones incluyen pero no están solo limitadas a: finalización de un programa, tarea o sesión o la alteración temporal de cuentas de usuario y contraseñas. El hecho de tomar acciones de emergencia no eximen el derecho del Ayuntamiento a tomar otro tipo de acciones que se encuentren en este reglamento.

Artículo 71. Los usuarios de los ordenadores personales y redes están sujetos a las leyes vigentes y los reglamentos y normas del Ayuntamiento. El Ayuntamiento de San Bartolomé de Tirajana no tiene ninguna responsabilidad y/o garantiza la información y material que reside en sistemas fuera del Ayuntamiento o en redes de acceso público, excepto donde tal responsabilidad esté formalmente expresada.

Artículo 72. El Coordinador de Nuevas Tecnologías deberá velar por el cumplimiento interno del presente Reglamento. De esta manera y ante cualquier incumplimiento del mismo, pondrá tal situación en conocimiento del Concejal/a responsable de Nuevas Tecnologías y del Alcalde-Presidente del Municipio, para que se inicien las acciones correspondientes y prescritas en la normativa sobre régimen disciplinario

tanto del personal funcionario como del laboral en lo que a infracciones en esta materia se refiere.

ANEXO I

Código de práctica para el uso de ordenadores y facilidades de red

Introducción

Los estándares para el uso de los ordenadores y facilidades de red del Ayuntamiento se derivan directamente de aplicar el sentido común al uso de cualquier recurso compartido. Este código de prácticas se basa en el principio de mutuo respeto y cooperación. Su propósito es especificar las responsabilidades de los usuarios y promover el uso apropiado de las tecnologías de la información y comunicaciones para la protección de todos los miembros que pertenecen al Ayuntamiento.

Uso apropiado y razonable

El uso razonable y apropiado de los ordenadores y facilidades de red del Ayuntamiento de San Bartolomé de Tirajana se define como el uso dado a los mismos para cumplir con los objetivos administrativos y de servicio al ciudadano del Ayuntamiento. Todos los usos fuera de esos objetivos se consideran inapropiados.

Responsabilidades

Los usuarios de los ordenadores y facilidades de red del Ayuntamiento aceptan las siguientes responsabilidades:

1. Seguridad:

- Salvaguardar sus datos, información personal, contraseñas y códigos de autorización y datos confidenciales.
- Elegir sus contraseñas sabiamente y cambiarlos periódicamente.

- Seguir las políticas y procedimientos de seguridad establecidos para el control de accesos y el uso de los datos administrativos.

2. Confidencialidad

- Respetar la privacidad de los otros usuarios; por ejemplo no buscar información, hacer copias o modificar

ficheros o contraseñas intencionadamente perteneciente a otros usuarios del Ayuntamiento.

- No representar a otros, a menos que se autorice explícitamente a hacerlo por dichos usuarios.

- No divulgar datos personales sensibles a los cuales tienen acceso.

3. Respetar los derechos de otros usuarios, por ejemplo, de acuerdo a las políticas del Ayuntamiento contra cualquier discriminación racial, sexual o de otro tipo. El Ayuntamiento rechaza de forma explícita cualquier discriminación de tipo racial, étnica, sexual y religiosa.

4. Respetar la protección legal dada por el copyright y la licencia de programas y datos; por ejemplo, no hacer copias de programas licenciados para evitar el pago de licencias adicionales o compartir programas con otros usuarios.

5. Respetar el uso de los recursos; por ejemplo, usar el nombre de usuario y contraseñas, datos y procesos asignados para el propósito que se le haya especificado, y no acceder a nombre de usuario y contraseñas, datos y procesos a menos que explícitamente sea autorizado por el responsable del departamento correspondiente.

6. Respetar el uso de sistemas para el intercambio electrónico de datos (como el correo electrónico); por ejemplo, no enviar correo basura, que intimide u ofenda a otros usuarios, spam, leer el correo electrónico de otros usuarios sin su permiso.

7. Respetar la integridad de los ordenadores y facilidades de red; por ejemplo, no desarrollar o usar programas, transacciones, datos o procesos que de forma intencionada dañen a otros usuarios o se infiltren en sus sistemas o dañen o alteren el software o datos de un sistema. Las alteraciones a cualquier componente de sistema de un ordenador serán hecho sólo bajo instrucciones específicas del personal del servicio de Desarrollo Tecnológico.

8. Adherirse a todas las políticas y procedimientos generales del Ayuntamiento incluyendo, pero no limitándose, a las políticas sobre el uso adecuado de los recursos de información, los ordenadores y las facilidades de red; la compra, uso y disposición de los ordenadores propiedad del Ayuntamiento; uso de los equipos de telecomunicaciones; uso legal del software y uso legal de los datos administrativos.

9. Informar sobre cualquier circunstancia en la cual el reglamento de seguridad del Ayuntamiento o cualquiera de sus estándares y códigos de prácticas hayan sido o estén siendo violadas. En general, los informes sobre violaciones se enviarán directamente al Coordinador de Nuevas Tecnologías.

ANEXO II

Código de práctica para actividades específicas

Actividad Ilegal

En general, es un uso inapropiado almacenar y/o dar acceso a información de los ordenadores y facilidades de red que no estén explícitamente autorizados por el responsable del departamento correspondiente.

Material prohibido

Los ordenadores y facilidades de red del Ayuntamiento no deben ser usados para la transmisión, obtención, demostración o anuncio de material prohibido. El material prohibido se define como el siguiente:

- Pornografía

- Cualquier material (películas, canciones...) que promuevan el crimen o la violencia, o incite o instruya en tema de violencia y crimen.

- Cualquier material (películas, canciones...) que describan o desarrollen materias que causen ofensa, como por ejemplo:

- a. El uso de la violencia o coerción para incitar a una persona a participar en determinadas conductas sexuales

- b. Actos de tortura o de extrema violencia o crueldad.

Se advierte a los usuarios que estarán sujetos a fuertes sanciones disciplinarias si desarrollan tales actividades.

Software y hardware restringido

Los usuarios no dejarán instalar a personas no autorizadas por el servicio de Desarrollo Tecnológico programas, hardware u otra información sobre sus ordenadores.

La conexión física a los ordenadores o a la red para monitorizar dispositivos se considera un uso inapropiado.

Incluye pero no está limitado a la conexión de cualquier dispositivo electrónico al ordenador o a la red con el propósito de monitorizar datos, paquetes, señales u otra información. La autorización para el uso de tal hardware para propósitos de diagnóstico debe obtenerse del servicio de Desarrollo Tecnológico.

Copias y Copyrights

1. El software que reside en los ordenadores y en la red es propiedad del Ayuntamiento o terceros y está protegido por el copyright y otras leyes de propiedad intelectual, junto con licencias y otros acuerdos contractuales. Los usuarios deben respetar los términos y condiciones de uso del software y de redistribución de licencias. Dichas restricciones implica la prohibición de copias y/o instalación de programas o datos para su uso en los ordenadores o en la red del Ayuntamiento sin la licencia correspondiente o para su distribución fuera del Ayuntamiento.

2. Está prohibido el uso de los ordenadores o facilidades de red del Ayuntamiento para reproducir total o parcialmente cualquier trabajo que tenga copyright sin la autorización expresa del autor de dicho trabajo.

Ofensas

La política del Ayuntamiento prohíbe las ofensas discriminatorias o sexuales. Los ordenadores y las redes del Ayuntamiento no serán usadas para difamar, calumniar o acosar a cualquier persona, dichas actitudes se considerarán faltas disciplinarias muy graves. Los siguientes son ejemplo de ofensas en entornos informáticos:

- Usar el ordenador intencionadamente para fastidiar, acosar, aterrorizar, intimidar, amenazar, ofender o molestar a otras personas usando lenguaje, imágenes o cualquier otro material considerado obsceno o que trate de herir al receptor.

- Usar intencionadamente el ordenador para contactar con otra persona repetidamente con el fin de fastidiar, acosar, o molestar sin existir propósito de legítima comunicación y donde el receptor ha expresado el deseo para que la comunicación cese

- Usar de forma intencionada el ordenador para interrumpir o dañar las tareas administrativas de otra persona.

- Usar intencionadamente el ordenador para invadir la privacidad de otro o amenazar con hacerlo.

La muestra de material ofensivo viola la política de ofensas del Ayuntamiento. Hay material en Internet y en otras ubicaciones que se consideran ofensivos. Un ejemplo son las imágenes sexualmente explícitas. El Ayuntamiento hará todo lo posible por limitar el acceso a dicho material en los ordenadores y facilidades de red por él suministradas, en cualquier caso considera la muestra de dicho material en sus ordenadores, servicios de red o lugares públicos que es inapropiado y se considera falta disciplinaria grave.

Desaprovechamiento de recursos

1. Se considera falta grave el realizar deliberadamente cualquier acto que perjudique la operación de cualquier parte del ordenador y facilidad de red o denegar el acceso por usuarios legítimos a cualquier parte de los mismos. Esto incluye pero no se limita a desaprovechamiento de recursos, manipulación de componentes o reducir la operativa de las facilidades suministradas.

2. Se considera falta grave el desaprovechamiento de forma voluntaria de los recursos de red y los ordenadores. Esto incluye pero se limita generar de forma voluntaria grandes volúmenes de salida impresa innecesaria o uso de disco innecesariamente, creación de múltiples trabajos y procesos innecesarios de forma voluntaria o generar gran tráfico de red de forma voluntaria. En particular, el uso de forma voluntaria de los ordenadores y las facilidades de red para el establecimiento de frívola e innecesaria cadenas de comunicación es una pérdida de recursos considerada inapropiada.

3. El uso de los ordenadores y facilidades de red del Ayuntamiento para el uso de juegos de ordenador está prohibido y se considera falta grave.

Conexión a la red de datos del Ayuntamiento

Para mantener la integridad de los ordenadores y las facilidades de red del Ayuntamiento, las conexiones a la red del Ayuntamiento se hará por personal especializado bajo la dirección del personal del servicio de Desarrollo Tecnológico.

Uso de los Sistemas personales

Los usuarios son responsables de la seguridad e integridad de la información almacenados en sus sistemas personales. Esta responsabilidad incluye realizar copias de seguridad de sus discos regularmente, controlar el acceso físico y de red a la máquina y tener actualizado e instalado un antivirus. Los usuarios evitarán mantener almacenados contraseñas u otra información que se pueda usar para obtener acceso a otros recursos de red, tampoco almacenarán las contraseñas del ayuntamiento o cualquier otro dato confidencial en sus ordenadores personales, portátiles o diskettes, CD o DVD de su propiedad.

Uso de servicios externos

Será responsabilidad del usuario adherirse y respetar las políticas establecidas de los servicios externos contratados por el Ayuntamiento.

Listados e impresiones

Los usuarios son responsables de la seguridad y privacidad de los listados e impresiones de la información del Ayuntamiento.

ANEXO III

Guías de seguridad de los ordenadores personales

Definición

Se definirán como ordenadores personales aquellas estaciones de trabajo personales, que aunque unidas posiblemente a otros ordenadores mediante una red de área local, funcionan como unidades autónomas. Como ordenadores personales se incluirán los ordenadores compatible-IBM, Macintosh y estaciones de trabajo Unix.

Obligaciones generales

Los usuarios de ordenadores personales están sujetos a las condiciones de uso y al código de práctica especificados en este reglamento.

Seguridad Hardware

1. Cierre las oficinas. Las llaves de las oficinas serán registradas y controladas.

2. Asegurar los ordenadores personales en zonas accesibles al público. Los equipos localizados en zonas accesibles al público u oficinas que no pueden ser cerradas serán sujetos mediante un cable para bloquear sistemas o colocados en una unidad que bloquee el acceso al ordenador

3. Asegure los discos duros. Los discos duros externos serán asegurados contra acceso y robos.

4. Etiquetar los ordenadores personales claramente

5. Colocar los ordenadores personales fuera de zonas peligrosas

6. Almacenar los medios de copia de seguridad en armarios ignífugos.

7. Inventariar todos los ordenadores del Ayuntamiento

Seguridad de acceso

Use contraseña que asegure que sólo usuarios autorizados puedan acceder al sistema, Cuando el ordenador personal se localice en un espacio abierto o sea difícil asegurarlo físicamente se debe extremar los mecanismos y procedimientos de protección mediante las siguientes recomendaciones:

- Longitud de la contraseña de 8 caracteres

- Evitar palabras que se encuentren en el diccionario e incluir al menos un carácter numérico

- Elegir contraseñas que no sean fácilmente adivinables por alguien relacionado con el usuario (no usar nombres propios de hijos, mascotas,...)

- No anotar las contraseñas en ningún lugar

- Cambiar las contraseñas periódicamente

- No incluir contraseñas en correos electrónicos

Disponibilidad de Software y Datos

- Haga copia de seguridad de registros y programas importantes de forma planificada

- Compruebe la integridad del software y los datos

- Informe de los problemas de software inmediatamente

Información confidencial

- Encripte la información sensible y confidencial cuando sea necesario

- Controle las impresoras usada para producir información confidencial y sensible

- Sobrescriba ficheros sensibles sobre disquetes, Cd Rom, Dvds. o discos duros.

Software

El software está protegido por las leyes de copyright y de propiedad intelectual. Las copias de software es una violación de la política de seguridad del Ayuntamiento. Cualquier usuario estará de acuerdo con los requisitos de licencia del software que usa y será responsable del software ilegal que haya en su máquina instalado ante posible auditorias de sus sistemas.

Virus

Los Virus son programas que se autopropagan e infectan a otros programas. Los Virus pueden destruir datos y programas, así como usar la memoria y el procesador del ordenador. Ante el temor de un virus en el sistema informático se informará al servicio de Desarrollo Tecnológico tan pronto como sea posible.

Para reducir el riesgo de virus siga las siguientes normas:

- Compruebe todo el software antes de instalarlo.
- Use antivirus para detectar y borrar virus
- Aislé inmediatamente cualquier sistema contaminado

Ordenadores de red

Los ordenadores de red requieren medidas de seguridad más exigentes que los ordenadores aislados porque son puntos de acceso a la red de ordenadores.

Mientras el servicio de Desarrollo Tecnológico tengan la responsabilidad de instalar y mantener los procedimientos de seguridad en la red, cada usuario es responsable de trabajar sobre su ordenador con una conducta ética con los otros usuarios en dicho entorno compartido.

Se tendrán en cuenta las siguientes consideraciones y procedimientos en un entorno de red:

- Comprobar todos los ficheros descargados de Internet. Evite descargar ficheros shareware

- Compruebe todo el software antes de instalarlo para asegurarse que no contiene ningún virus que pudiera tener consecuencias para otros ordenadores personales y servidores de la red del Ayuntamiento.

- Elija contraseñas con gran cuidado para prevenir el uso desautorizado de ficheros sobre las redes o los ordenadores personales.

- Siempre haga copia de seguridad de sus ficheros importantes

- Use, cuando sea necesario, servicios de autenticación y encriptación para enviar información confidencial sobre la red del Ayuntamiento.

- Nunca almacene contraseñas del Ayuntamiento o cualquier dato o información confidencial en el portátil u ordenador propio en casa o sobre diskettes, Cd- Roms o Dvds.

El presente reglamento entrará en vigor a los quince días hábiles de su publicación en el Boletín Oficial de la Provincia.

San Bartolomé de Tirajana, a once de abril de dos mil cinco.

EL ALCALDE-PRESIDENTE, Marco Aurelio Pérez Sánchez.

5.345

ANUNCIO

6.610

Se hace saber a las personas o entidades que a continuación se relacionan que por esta Alcaldía se ha dictado resolución de expedientes sancionadores, por infracciones en materia de Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, en virtud de denuncias formuladas por agentes de la autoridad: