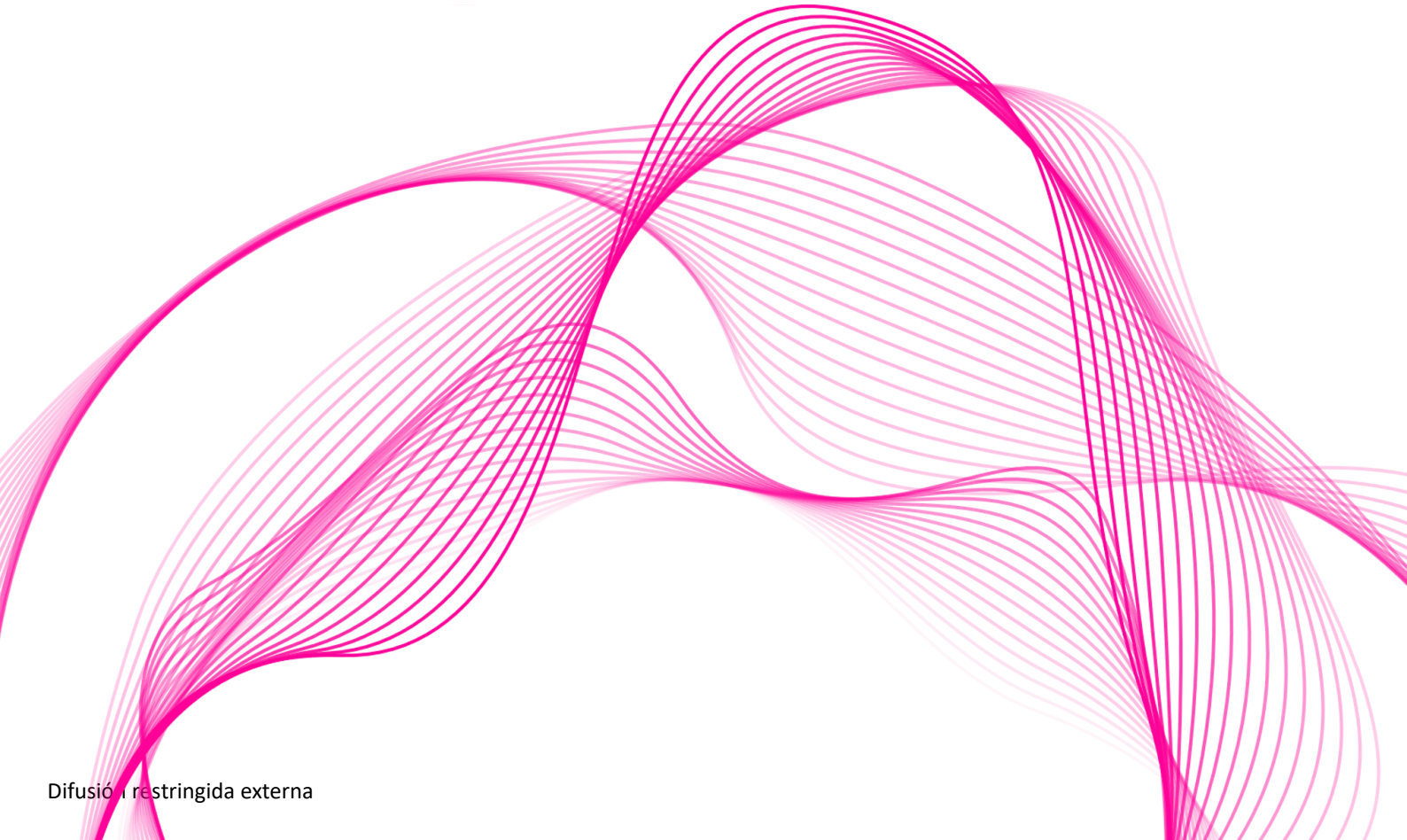
SGSI02 – Normativa de Seguridad

Normativa



Información del documento:

Título del documento	SGSI02 – Normativa de Seguridad
Tipo de documento	Normativa
Descripción	SGSI02 – Normativa de Seguridad
Nivel de seguridad	Interno

Registro de versiones		
Descripción	**Versión**	**Fecha**
Versión inicial del documento.	V1	09/12/2024

Índice

1. INTRODUCCIÓN

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS, en adelante), este documento contiene la Normativa de Seguridad de aplicación para aquellos sistemas de información gestionados por el AJUNTAMENT DE LA VILAJOIOSA o bajo su responsabilidad, señalando asimismo los compromisos que adquieren sus usuarios respecto a su seguridad y buen uso.

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros del AJUNTAMENT DE LA VILAJOIOSA que se encuentren afectados por el alcance del ENS para el desempeño de su trabajo, y en su caso el personal externo vinculado a prestaciones de servicios.

Por ello, cada uno de ellos debe cumplir los requerimientos de la Normativa de Seguridad de la Información y su documentación asociada. Quienes deliberadamente o por negligencia incumplan la Normativa de Seguridad podrían estar sujetos a responsabilidad.

La presente Normativa ha sido aprobada por el Comité de Seguridad del AJUNTAMENT DE LA VILAJOIOSA, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que el AJUNTAMENT DE LA VILAJOIOSA pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes. La Normativa de Seguridad será mantenida, actualizada y adecuada a los fines de AJUNTAMENT DE LA VILAJOIOSA, alineándose con el contexto de gestión de riesgos estratégica de la entidad.

Este documento se considera de uso interno para el AJUNTAMENT DE LA VILAJOIOSA y, por consiguiente, no podrá ser divulgado salvo autorización del Comité de Seguridad.

2. OBJETIVO

El buen funcionamiento del AJUNTAMENT DE LA VILAJOIOSA depende en gran medida de los Sistemas de Información1 y de la Información que en ellos se almacena. La utilización de recursos tecnológicos para el tratamiento de la información es esencial y cumple con una doble finalidad para la organización:

- Facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión, y
- Proporcionar información completa, homogénea, actualizada y fiable.

Por ello, la utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier entidad pública. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño

[1] Siguiendo la definición dada por el ENS, en el ámbito de esta Normativa General se entiende por Sistema de Información todo conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

de su actividad profesional, razón por la cual compete a AJUNTAMENT DE LA VILAJOIOSA determinar las normas, condiciones y responsabilidades bajo las cuales deben utilizarse.

La Normativa de Seguridad tiene como misión establecer objetivos del AJUNTAMENT DE LA VILAJOIOSA, así como proteger los activos de información y alcanzar la mayor eficacia y seguridad en su uso. Estos objetivos incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento con la finalidad de proteger la información del AJUNTAMENT DE LA VILAJOIOSA. El objetivo principal del desarrollo de esta Normativa de Seguridad por parte del Comité de Seguridad es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiere para el desempeño del trabajo, así como evitar pérdidas de información y accesos no autorizados a la misma.

Para lograr los objetivos en materia de seguridad resulta necesario definir obligaciones integradas por un conjunto de acciones positivas (deber de hacer algo) u omisivas (deber de abstenerse de hacer). Estas obligaciones derivan directamente de la naturaleza de las tecnologías de la información que constituyen nuestra herramienta natural de trabajo y no son otra cosa que la actualización del deber de secreto y de preservar la información administrativa que incumbe a todo empleado público.

La seguridad es un instrumento al servicio de la organización y de todos los usuarios, capaz de proporcionar confianza en los sistemas, preservar el ejercicio de las funciones y responsabilidades propias de cada usuario y garantizar la calidad y veracidad de la información objeto de tratamiento.

La seguridad se articula en torno a cinco grandes objetivos-principios:

- Confidencialidad: La información perteneciente al AJUNTAMENT DE LA VILAJOIOSA debe ser conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.
- Integridad: La información del AJUNTAMENT DE LA VILAJOIOSA debe de ser completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- Autenticidad: La información del AJUNTAMENT DE LA VILAJOIOSA es generada por un autor identificado que es imposible de suplantar, lo que incluye el no repudio de la información introducida pues se garantiza que el emisor de la información es quien dice ser.
- Disponibilidad: La información del AJUNTAMENT DE LA VILAJOIOSA está accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad.
- Trazabilidad: Supone que las actuaciones de usuarios autorizados e identificados se pueden rastrear a posteriori para definir quién ha accedido o modificado una cierta información, de modo que puedan ser imputadas exclusivamente a su autor.

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las

misiones encomendadas al AJUNTAMENT DE LA VILAJOIOSA, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Estas dimensiones de la seguridad alcanzan no sólo al personal del AJUNTAMENT DE LA VILAJOIOSA sino también a los usuarios integrados en las organizaciones externas que se relacionan con la misma o prestan en ella sus servicios.

3. ÁMBITO DE APLICACIÓN

Esta normativa es de aplicación y obligado cumplimiento para todo el personal del AJUNTAMENT DE LA VILAJOIOSA que desempeñe sus funciones en los sistemas de información bajo el alcance del ENS. Se entiende por usuario de los Sistemas de Información:

1. Cualquier empleado perteneciente al ayuntamiento.
2. El personal de prestadores de servicios, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el AJUNTAMENT DE LA VILAJOIOSA cuando utilice o posea acceso a sus Sistemas de Información.

Sus contenidos se basan en las directrices de carácter más general definidas en la Política de Seguridad de la Información del AJUNTAMENT DE LA VILAJOIOSA

Bajo el alcance del ENS se entienden incluidos tanto los recursos informáticos como la información que puede ser tratada o extraída por ellos y cualquier soporte que la contenga.

4. APROBACIÓN Y VIGENCIA

Esta normativa se difundirá a todo el personal mediante su publicación y entrará en vigor transcurrido un mes natural desde la fecha de aprobación por el Comité de Seguridad del AJUNTAMENT DE LA VILAJOIOSA.

La Normativa de Seguridad será mantenida, actualizada y adecuada a los fines de la empresa. Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación.

5. REVISIÓN Y EVALUACIÓN

La gestión de esta Normativa General corresponde al Comité de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Verificar su efectividad.
- Proponer su revisión.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo

aconsejen), el Comité de Seguridad revisará la presente Normativa General. La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, etc.

El Responsable de Seguridad de la Información, es la persona encargada de la difusión de la versión aprobada de este documento.

6. ENTORNO DE GESTIÓN DE LA SEGURIDAD

El AJUNTAMENT DE LA VILAJOIOSA dispone de un Sistema de Gestión de Seguridad de la Información integrado con el cumplimiento de las obligaciones del Esquema Nacional de Seguridad. Todas las políticas y procedimientos a los que se hace referencia en este documento y en el Sistema han sido revisados, aprobados e impulsados por el Comité de Seguridad del AJUNTAMENT DE LA VILAJOIOSA.

El conjunto de obligaciones que derivan de esta Normativa se definen en directa relación con los activos protegidos y la sensibilidad de la información objeto de protección.

Los Activos de Información

Esta normativa afecta a todos los Activos de Información del AJUNTAMENT DE LA VILAJOIOSA implicados en el alcance del ENS, tanto a ordenadores personales o servidores, redes, aplicaciones, sistemas operativos y procesos del AJUNTAMENT DE LA VILAJOIOSA que pertenecen o son administrados por el AJUNTAMENT DE LA VILAJOIOSA.

Clasificación de la información conforme a su sensibilidad

La información del AJUNTAMENT DE LA VILAJOIOSA está clasificada en 2 categorías dependiendo de su grado de confidencialidad. Todo empleado debe ser consciente de esta clasificación:

Difusión que puede realizarse de la misma:

- Uso Oficial: Documento de difusión parcialmente controlada no apto para su difusión pública. Su uso se restringe únicamente al personal interno del organismo y entidades y colaboradores.
- Público: información de difusión no controlada para el público general. Apto para difusión entre todo tipo de organismos y entidades

Corresponde al Comité de Seguridad la clasificación del conjunto del Sistema de información. Como principio general la información se clasifica como Uso Oficial. En aquellos supuestos en los que resulte necesaria la reclasificación de alguna información o documento con motivo del desempeño de las funciones propias del servicio ésta será decidida por el correspondiente Jefe de Servicio teniendo en cuenta las directrices fijadas por el Comité de Seguridad.

El procedimiento de seguridad a aplicar a la información se puede consultar el procedimiento PR22-Calificación de la información.

7. NORMAS DE SEGURIDAD

El AJUNTAMENT DE LA VILAJOIOSA facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la entidad pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales.

A continuación, se detallan las Normas de Seguridad que todos los usuarios deben conocer y aplicar en su caso.

7.1 Normas Generales

1. Los equipos informáticos (PCs, dispositivos móviles, portátiles…), serán asignados por el departamento de informática.

2. Existirá un inventario actualizado de los equipos informáticos. El departamento de informática será la unidad encargada de gestionar dicho inventario.

3. A cada nuevo usuario que se incorpore a la organización y así lo precise, se le facilitará un ordenador personal debidamente configurado y con acceso a los servicios y aplicaciones necesarias para el desempeño de sus competencias profesionales.

4. Los ordenadores personales deberán utilizarse únicamente para fines institucionales y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

5. Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información. Cuando se precise instalar dispositivos no provistos por la entidad, se deberá solicitarse autorización previa.

6. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.

7. Por normal general, los usuarios no tendrán privilegio de administración sobre los equipos.

8. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.

9. Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente norma, lo escalará y se tomaran las oportunas medidas correctoras y dará traslado de la incidencia.

10. Cada equipo deberá estar asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su correcto uso.

11. Dentro de las medidas de austeridad y reducción del gasto, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios.
    - Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
    - Imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando, siempre que sea posible, la impresión en color.

12. El usuario debe ser consciente de las amenazas provocadas por malware. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.

13. El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.

14. El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al departamento de informática al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por el AJUNTAMENT DE LA VILAJOIOSA estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente cuando finalice su vinculación con dicho puesto o función.

7.2 Normas específicas para el almacenamiento de información

15. Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. La entidad pondrá a disposición de los usuarios el espacio en red necesarios para el desempeño de su trabajo.

16. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa.

17. Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria, siendo obligación del usuario la limpieza y optimización del espacio del disco asignado.

7.3 Normas específicas para equipos portátiles y móviles

18. Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. se deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.

19. Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales y autorizados, especialmente cuando se usen fuera de las instalaciones del AJUNTAMENT DE LA VILAJOIOSA.

20. Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la entidad o no autorizadas para ello.

21. En caso de pérdida o sustracción del dispositivo el usuario tendrá la obligación de notificarlo lo antes posible al departamento de informática del Ayuntamiento.

7.4 Normas específicas para para memorias USB

22. El uso de memorias USB está prohibido en el Ayuntamiento. En el caso de que sea necesario su uso deberá solicitarse al departamento de informática.

23. Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento.

24. La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento el departamento de Informática de forma inmediata.

25. Siempre que el contenido esté clasificado como confidencial o existan datos sensibles, las memorias USB deberán ir cifradas.

7.5 Copias de Seguridad

26. Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en una unidad de red compartida, evitando los duplicados y documentos innecesarios.

27. De forma periódica, se realizarán copias de seguridad incrementales de las unidades de red compartidas donde se almacene la información del usuario.

28. La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse al departamento de informática.

7.6 Borrado y eliminación de soportes informáticos

29. Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

    - Asegurarse del contenido de cualquier soporte antes de su eliminación.
    - Cuando contenga información sensible, confidencial o protegida, el soporte deberá destruirse según los procedimientos establecidos por el AJUNTAMENT DE LA VILAJOIOSA.

7.7 Impresoras en red, fotocopiadoras y faxes

30. Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la entidad y, en su consecuencia, estén debidamente inventariados.

31. Cuando se imprima documentación o se envíe un fax, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

32. Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del departamento de informática.

7.8 Digitalización de documentos

33. Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarlos, especialmente si contienen información sensible, confidencial o protegida.

34. Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su

propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del departamento de informática.

7.9 Cuidado y protección de la documentación impresa

35. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, utilizando la opción de impresión con código seguro, y debiendo ser recogida rápidamente de las impresoras para ser custodiada en armarios bajo llave.

36. Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las maquinas destructoras, de forma que no sea recuperable la información que pudieran contener.

37. Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

7.10 Pizarras y flipcharts

38. Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiaran adecuadamente las pizarras y flipcharts de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

7.11 Protección de la propiedad intelectual

39. Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA sin la correspondiente licencia de uso.

40. Los programas informáticos propiedad están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, está estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del departamento de informática.

41. Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

7.12 Instalación de software

42. Únicamente el departamento de informática podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

43. No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.

44. Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de la entidad de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

45. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el departamento de informática, especialmente aquellas relacionadas con la seguridad.

7.13 Acceso a los sistemas de información y a los datos tratados

46. Los datos gestionados por el AJUNTAMENT DE LA VILAJOIOSA y tratados por cualquier Sistema de Información deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

47. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar en caso de mala utilización.

48. Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

49. Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar los salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad de 15 minutos.

50. La baja de los usuarios será comunicada por Gerencia, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

7.14 Identificación y autenticación

51. Los usuarios dispondrán de un código de usuario (user-id) y una contraseña (password), para el acceso a los Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

52. Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

53. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

54. Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar la correspondiente incidencia de seguridad.

55. El usuario deberá utilizar contraseñas robustas siguiendo las indicaciones siguientes:

    - La contraseña no deberá contener el nombre de la cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
    - Deberá tener una longitud mínima de ocho (8) caracteres.
    - Deberá incluir caracteres de tres de las siguientes categorías:
        1. Mayúsculas (de la A a la Z)
        2. Minúsculas (de la a a la z)
        - Dígitos de base 10 (del 0 al 9)
        3. Caracteres no alfanuméricos (por ejemplo, !, $, #, %)

56. Si, en un momento dado, un usuario recibiera una llamada telefónica solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho al departamento de informática, de forma inmediata.

57. El acceso remoto a los sistemas de información deberá realizarse a través de red privada virtual (VPN) haciendo uso de doble factor de autenticación.

58. Para el acceso a las aplicaciones se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es», o bien se emplearán certificados cualificados como mecanismo de autenticación que estará protegido por un segundo factor del tipo PIN.

7.15 Protección de datos de carácter personal y deber de secreto

59. La información contenida en las bases de datos que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Tratamientos de datos de carácter personal gestionados por la entidad han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

60. Todo usuario que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con el AJUNTAMENT DE LA VILAJOIOSA, de conformidad con el documento "Contrato de Confidencialidad".

7.16 Tratamiento de la información

61. Toda la información contenida en los Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a su personal.

62. Cualquier tratamiento en los Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

63. Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia del AJUNTAMENT DE LA VILAJOIOSA en servidores externos (en la nube) a la entidad salvo autorización expresa del responsable, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre el AJUNTAMENT DE LA VILAJOIOSA y la empresa responsable de la prestación del servicio, incluyendo el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

64. La transmisión de información se realizará siempre que sea posible por la aplicación Almacén. En el caso de que no sea posible se contactará con el Responsable de Seguridad para buscar una alternativa segura.

65. La salida de datos sensibles, confidenciales o protegidos, requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

7.17 Uso del correo electrónico corporativo

66. El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios del AJUNTAMENT DE LA VILAJOIOSA, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

67. No se permite el uso de cuentas de correo que no sean las corporativas.

68. Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

69. Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización.

70. El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal.

71. Se deberá notificar al departamento de informática cualquier tipo de anomalía detectada en el uso del correo electrónico.

72. Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al departamento de informática.

73. No está permitido el acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio, sin la debida autorización.

74. No se debe responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.

75. Se recomienda asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

76. Es recomendable evitar, en la medida de lo posible, el uso ineficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de los mismos), envíos innecesarios, etc.

77. No se permite el envío de contraseñas en plano a través del correo electrónico.

7.18 Acceso a internet y otras herramientas de colaboración

78. El acceso corporativo a Internet es un recurso centralizado que el AJUNTAMENT DE LA VILAJOIOSA pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

79. El AJUNTAMENT DE LA VILAJOIOSA velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

80. Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos.

81. Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por el AJUNTAMENT DE LA VILAJOIOSA en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del departamento de informática.

82. Se debe de evitar la descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

83. No está autorizada la descarga de programas informáticos sin la autorización previa del departamento de informática. En todo caso debe asegurarse que el sitio Web visitado es confiable.

7.19 Utilización de las Redes Sociales

84. No compartir contenidos sensibles sobre la vida personal o la de otros en redes sociales: documentos identificativos, números de teléfono, direcciones postales, localizaciones exactas, identificadores de vehículos, etc. Cuanto más contenidos de este tipo se compartan, más probabilidades hay de ser víctima de un robo de identidad, de ciberacoso u otra conducta ilícita que utilice esa propia información para perjudicar al usuario.

85. Un sitio permanente encabezado por fotografías, datos personales e información sobre estudios, profesión, gustos, intereses, amigos y familia proporciona mucha más información de la persona que su DNI o Pasaporte.
Además, quedaría a la vista de todo el mundo. Es clave, prestar atención a cómo uno define su perfil en redes sociales, ya que será la carta de presentación de su identidad en el ciberespacio.

86. En el ciberespacio aplica el principio de “prevención ante lo desconocido”. No hacer clic en contenidos sobre los que no se tenga claro su origen o propósito y aumentar la cautela ante mensajes de identidades desconocidas.
En definitiva, huir de la tentación de todo aquello que cuanto más desconocido, más atractivo parece.

87. Proteger el acceso a los perfiles en redes sociales con contraseñas fuertes utilizando dos factores de autenticación donde sea viable.

88. Controlar la geolocalización de perfiles y contenidos en redes sociales. Desactivar la geolocalización por defecto en el menú de configuración de los perfiles y hacer un uso inteligente de la misma, pensando en cada caso si interesa que los demás tengan un mapa de tu vida o de parte de ella.

89. Comprobar la configuración de privacidad tanto en el perfil como en los contenidos que se comparten.

90. No difundir información privada sobre otras personas sin su consentimiento y no etiquetar por su nombre a otras personas que no tienen perfil en redes sociales sin solicitar previamente su permiso para hacerlo.

91. Cuidar y proteger las relaciones en el ciberespacio. Mantener en privado la lista de contactos y analizar en detenimiento las solicitudes de amistad de desconocidos.

92. Adoptar la consciencia de que la primera línea de defensa para la protección en el ciberespacio es uno mismo. De esta manera, la ayuda que instituciones y organizaciones de ciberseguridad presten será mucho más eficiente y uno mismo será de ayuda inapreciable para mantener unas redes sociales seguras.

7.20 Incidencias de seguridad

93. Los usuarios deberán notificar al departamento de informática, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

94. Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA o su imagen, deberá informar inmediatamente al departamento de informática, que lo registrará debidamente y elevará, en su caso.

95. Deberá notificarse al departamento de informática cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

7.21 Compromisos de los usuarios

96. Es responsabilidad directa del usuario:
    a) Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad que elabore el departamento de informática, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.
    b) En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa establezca al respecto.

7.22 Control de actuaciones sobre las bases de datos

97. El AJUNTAMENT DE LA VILAJOIOSA podrán habilitar Sistemas de Información cuyo acceso y/o modificación de la información contenida quedarán registrados en una Base de Datos, lo que permitirá su ulterior auditoría.

98. Se prohíbe realizar cualquier tipo de actualización en Bases de Datos corporativas, masiva o puntual, desde fuera de las aplicaciones del AJUNTAMENT DE LA VILAJOIOSA sin la autorización previa del departamento de informática.

7.23 Monitorización y aplicación de esta normativa

99. El AJUNTAMENT DE LA VILAJOIOSA, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente puede:

    a) Revisar periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
    b) Monitorizar los accesos a la información contenida en sus sistemas.
    c) Auditara la seguridad de las credenciales y aplicaciones.
    d)Monitorizar los servicios de internet, correo electrónico y otras herramientas de colaboración.

100. El AJUNTAMENT DE LA VILAJOIOSA llevará a cabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios

101. Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente, previo aviso del usuario. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El departamento de informática, con la colaboración de las restantes unidades del AJUNTAMENT DE LA VILAJOIOSA, velarán por el cumplimiento de la presente Normativa General.

102. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

7.24 Modelo de aceptación y compromiso de cumplimiento

103. Todos los usuarios de los recursos informáticos y/o Sistemas de Información del AJUNTAMENT DE LA VILAJOIOSA tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa, debiendo suscribirla.
104. Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

7.25 Publicación en web.

105. La publicación de contenidos en la web del AJUNTAMENT DE LA VILAJOIOSA se limitará a los documentos o informaciones con clasificación pública.

106. Se retirará de estos documentos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente.

107. La información publicada debe garantizar los principios de autenticidad e integridad.

108. Los gestores y editores de páginas web asegurarán la disponibilidad de la información durante el periodo previsto de vigencia de la misma procediendo a su retirada cuando se produzca el vencimiento.

7.26 Directrices de puesto de trabajo despejado

109. La documentación que no se está utilizando en un momento determinado debe estar guardada correctamente, especialmente cuando dejamos nuestro puesto de trabajo y al finalizar la jornada.

110. La información se destruirá de manera segura, haciendo uso de las destructoras de papel.

111. No se conservarán contraseñas en lugares visibles alrededor del puesto de trabajo (apuntadas en post-it o similares).

112. El puesto de trabajo estará limpio y ordenado.

113. El usuario bloqueará el ordenador cuando este quede desatendido.

7.27 Navegación WEB

114. Se cuenta con filtros de acceso que bloquean el acceso a páginas web con contenidos inadecuados.

115. Utilizar siempre un navegador actualizado. Los principales navegadores de hoy en día se actualizan automáticamente bien de forma transparente al usuario o mediante notificaciones que deberán ser aprobadas.

116. Se recomienda hacer uso de HTTPS frente a HTTP incluso para aquellos servicios que no manejen información sensible. Algunas funcionalidades como HSTS y extensiones como HTTPS Everywhere servirán de gran ayuda para garantizar el uso preferente de HTTPS sobre HTTP durante la navegación web.

117. Se recomienda no almacenar contraseñas de forma predeterminada por medio del navegador y utilizar herramientas más seguras para dicha gestión (por ejemplo, gestores de contraseñas que implementen un sistema de cifrado robusto). En el caso de que se decida utilizar el navegador es importante hacer uso de una llave maestra que cifre el repositorio de credenciales

118. Es importante verificar que los certificados remitidos por servicios HTTPS que manejen información sensible (por ejemplo, servicios de correo, banca electrónica, etc.) han sido remitidos por una CA de confianza. Cualquier error o alerta generada por el navegador como consecuencia de la validación del certificado (por ejemplo, certificados autofirmados) deberá revisarse cuidadosamente.

7.28 Acceso remoto y teletrabajo

119. De forma general, el usuario que realice sus labores en modo teletrabajo fuera de las instalaciones del Ayuntamiento se compromete a adoptar las medidas de seguridad oportunas para garantizar que el acceso a la información sensible se realiza de manera responsable y con la misma política de seguridad de la organización. Para ello, se podrán utilizar los dispositivos móviles (portátiles, smartphones) proporcionados por la empresa o, en su defecto, equipos no corporativos, siempre y cuando se garantice el cumplimiento de las medidas de seguridad establecidas en este documento.

120. En la medida de lo posible, se evitará el teletrabajo realizado desde instalaciones o recursos compartidos o públicos. Especialmente en lo que a conectividad se refiere, se primará siempre el uso de conexiones propias y confiables (red doméstica o telefonía móvil) sobre cualquier otra opción compartida.

121. Para cuando no podamos acceder a una conexión confiable o sea necesario acceder a la red corporativa de forma remota, se dispone de la conexión segura mediante VPN desde la que se podrá acceder con garantías al resto de recursos.

122. En este tipo de conexiones, el usuario dispondrá de los mismos permisos y accesos que desde su puesto de trabajo local. Además, se establece la desconexión automática de sesiones después de un período de una hora de inactividad.

123. En caso de ser necesario el acceso remoto por parte de terceros (clientes, proveedores), se les proporcionaran las credenciales oportunas con una fecha de caducidad que obligue a la desactivación inmediata después del uso requerido y se asegurará que sólo puedan acceder a los recursos necesarios.

8. INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de los sistemas de información están obligados a cumplir la presente Normativa de Seguridad. Su incumplimiento genera responsabilidad que se sustanciará conforme al procedimiento establecido al efecto en cada caso.

9. REFERENCIAS

- SGSI01-PoliticaDeSeguridad