REGLAMENTO GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN

1.- INFORMACIÓN DEL DOCUMENTO
2.- ÁMBITO DE APLICACIÓN
2.1 Ámbito funcional
2.2 Ámbito personal
2.3 Ámbito temporal
2.4 Ámbito material
3.- OBJETIVO
4.- REVISIÓN Y EVALUACIÓN
5.- NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES
5.1 Normas Generales
5.2 Normas específicas para equipos portátiles y móviles
5.3 Instalación de software
6.- NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE LA INFORMACIÓN Y COPIAS DE SEGURIDAD
7.- NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES
7.1 Normas para el borrado y eliminación de soportes informáticos
8.- NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS
8.1 Impresoras en red, fotocopiadoras y faxes
8.2 Cuidado y protección de la documentación con datos sensibles
9.- PROTECCIÓN DE LA PROPIEDAD INTELECTUAL
10.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS
10.1 Acceso a una cuenta de usuario en su ausencia o baja
10.2 Identificación y Autenticación
11.- PUESTOS DESPEJADOS Y PANTALLAS LIMPIAS
12.- CERTIFICADOS ELECTRÓNICOS
13.- CONFIDENCIALIDAD DE LA INFORMACIÓN
14.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO
15.- SALIDA DE INFORMACIÓN
16.- USO DEL CORREO ELECTRÓNICO CORPORATIVO.
17.- ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN
18.- INCIDENCIAS DE SEGURIDAD
19.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS DE LA ADMINISTRACIÓN
20.- ACCESOS DEL PERSONAL DEL SERVICIO SOPORTE
21.- MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA
22.- INCUMPLIMIENTO DE LA NORMATIVA

2.- ÁMBITO DE APLICACIÓN

2.1.- Ámbito funcional

La presente Política, establece la regulación del uso de los recursos y sistemas de información para la Diputación Provincial de Ávila, Fundación Cultural Santa Teresa y el Organismo Autónomo de Recaudación, así como cualquier otro organismo

autónomo que se constituya con posterioridad durante su vigencia, en adelante "Administración".

2.2.- Ámbito personal

Con carácter general, el presente Reglamento afecta a todo el personal dependiente de las entidades señaladas en el ámbito funcional, independientemente de su vinculación funcionarial o laboral y de su carácter permanente o duración determinada.

Así mismo, se entenderán incluidos en el ámbito de aplicación de esta Norma, los siguientes colectivos:

a) El personal eventual o de confianza y cargos electos.
b) El personal vinculado, por una relación laboral especial de alta dirección.
c) El personal contratado por la Administración dentro de planes y programas públicos de empleo sujetos a un convenio colectivo específico.
d) Personal becado.
e) Personal colaborador.
f) Personal de terceros, empresas proveedoras y/o colaboradoras.

En adelante, se expresará con el concepto "usuario/personal", al conjunto de actores incluidos en el ámbito personal de la presente Política.

Por tanto, las partes reconocen que tienen conocimiento y asumen los compromisos, normas y reglamentos para el uso de los medios tecnológicos, recogidas en la presente Norma (incluidas las complementarias que la desarrollan), tomando todas las medidas que correspondan para su estricto cumplimiento.

2.3.- Ámbito temporal

El presente Reglamento General de Utilización de los Recursos y Sistemas de Información, ha sido aprobada por el Pleno de la Diputación Provincial de Ávila, previamente dictaminado por la Comisión Informativa de Seguimiento de la Política de Transparencia y Buen Gobierno, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Administración 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.

Este Reglamento es efectivo desde la fecha de su aprobación, y hasta que sea reemplazado por una nueva Normativa. Sin perjuicio de la posibilidad de revisión durante su vigencia.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este Reglamento General.

Será el Comité de Seguridad de la Información de la Diputación Provincial de Ávila (hay que crearlo) el órgano encargado de la custodia y divulgación de la versión aprobada de este documento.

2.4.- Ámbito material

Este Reglamento será de aplicación a todos los sistemas de información de la Administración que, siguiendo la definición dada en el Esquema Nacional de Seguridad, se entiende a los efectos de este Reglamento como el 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.

Los datos del Diputación Provincial de Ávila que son considerados categorías especiales de datos o datos confidenciales, y los cuales se hará referencia en la presente Normativa, son los siguientes:

Categorías especiales de datos establecidos en el artículo 9 del RGPD (origen étnico o racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos, datos biométricos, salud, vida sexual, orientación sexual) o artículo 10 del RGPD (condenas e infracciones penales).

Documentos en fase de desarrollo, que sirvan de soporte para la elaboración de los acuerdos institucionales.

3.- OBJETIVO

La Administración consciente de que la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, se compromete a la protección de sus propiedades más significativas como parte de una estrategia orientada a la gestión y tratamiento de los riesgos y a la consolidación de una cultura de seguridad.

Los sistemas de información son elementos básicos para el desarrollo, gestión y tratamiento de la información propiedad de la Administración. Estos medios se ponen a disposición del personal/usuarios como instrumentos de trabajo para el desempeño de su actividad profesional. Motivo por el cual, éstos utilizarán estos recursos de manera responsable, mediante el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de la información, los sistemas de información y los recursos tecnológicos proporcionados por la Administración.

Los derechos de acceso a la información y a los recursos de los Sistemas de información que la tratan se otorgarán siempre en base a los principios de “mínimo privilegio posible y
necesidad de conocer”.

4.- REVISIÓN Y EVALUACIÓN

La gestión de las normas incluidas en esta Normativa corresponde al Comité de Cumplimiento Normativo de Transparencia y Seguridad de la Diputación Provincial de Ávila la cual es competente para:

Interpretar las dudas que puedan surgir de su aplicación.

Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.

Verificar su efectividad.

Con periodicidad anual el Comité de Cumplimiento Normativo de Transparencia y Seguridad revisará la presente Normativa que se someterá, en caso de que existan modificaciones a la aprobación por el Pleno de la Corporación. Los puntos mínimos a considerar en las revisiones serán los siguientes:

Identificación de acciones de mejora en la gestión de la seguridad de la información.

Adaptación a los posibles cambios normativos, de infraestructuras tecnológicas, organizativas, etc.

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, organización general, etc.

5.- NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

La Diputación Provincial de Ávila pondrá a disposición del personal/usuario, que así lo precisen, los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de las funciones profesionales que tenga atribuidas. Mediante estos equipos los usuarios tendrán acceso a los Sistemas de Información de la Administración, motivo por lo que es necesario adoptar una serie de precauciones y medidas para su adecuada utilización.

Las normas que se indican en este apartado serán de aplicación a todos los equipos facilitados y configurados por la Administración para su utilización por parte de los usuarios, entendiendo por equipos los siguientes: terminales, ordenadores personales de sobremesa, portátiles, teléfonos móviles, smartphones, tabletas o similar y cualquier otro dispositivo con capacidad de acceso a los Sistemas de Información de la organización.

5.1.- Normas Generales

El Departamento de Informática, proporcionará a los usuarios el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones. Respecto a los cuales se observarán las siguientes normas generales:

Los equipos deberán de utilizarse únicamente para fines institucionales y como herramienta para el desempeño de las tareas encomendadas.

Salvo autorización expresa del Departamento de Informática, los usuarios no tendrán privilegios de administrador sobre los equipos.

Únicamente el personal autorizado por el Departamento de Informática, podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos.

Cuando sea necesario instalar equipos que no hayan sido provistos por la Administración deberá de solicitarse autorización previa al Departamento de Informática.

Los usuarios deberán notificar al Departamento de Informática, a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Del mismo modo deberá de comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro del mismo.

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

El usuario debe ser consciente de que “el eslabón más débil en la cadena de seguridad es el propio usuario”. Muchos virus y troyanos requieren la participación de los usuarios para propagarse.

5.2.- Normas específicas para equipos portátiles y móviles

El Departamento de Informática será el encargado de la distribución de los equipos portátiles, siendo Presidencia la encargada de la asignación de los dispositivos móviles. Al igual que el resto de los equipos, estarán debidamente configurados con acceso a los servicios y aplicaciones necesarios para el desempeño de sus funciones. Respecto a los cuales les serán de aplicación además de las normas generales, las siguientes:

Los equipos móviles estarán, en todo momento, bajo la custodia del usuario que los utilice. Siendo éste el responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.

La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del
Departamento de Informática para la adopción de las medidas que correspondan.

Al igual que el resto del equipamiento proporcionado por la Diputación Provincial de Ávila, deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de la Institución.

Cuando se trata de datos sensibles, los ordenadores portátiles afectados deberán tener cifrado el disco duro y disponer de software que garantice un arranque seguro. Desde el Departamento de Informática implementarán los mecanismos necesarios en cada caso.

Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al Departamento de Informática, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

El uso de dispositivos móviles propios, denominado BYOD (Bring Your Own Device), para el acceso a información institucional, no está permitido. En caso de ser necesario su uso, deberá solicitarse al Departamento de Informática y deberá contar con la autorización expresa del Comité de Seguridad de la Información de la Diputación Provincial de Ávila.

5.3.- Instalación de software

Como norma general, únicamente el personal del Departamento de Informática podrá instalar software en los equipos de los usuarios, salvo que se disponga de autorización expresa. En cuyo caso se deberán de tener en cuenta las siguientes indicaciones:

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.

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

En aquellos casos, en las que los usuarios dispongan de cuentas con privilegios de administrador local (en su propia máquina), no está permitido eliminar o deshabilitar las aplicaciones informáticas instaladas por el Departamento de Informática,
especialmente aquellas relacionadas con la seguridad.

6.- NORMAS ESPECÍFICAS PARA EL ALMACENAMIENTO DE LA INFORMACIÓN Y COPIAS DE SEGURIDAD

Para garantizar la disponibilidad de la información, frente a la materialización de un incidente de seguridad, el Departamento de Informática realiza, de forma periódica, copias de seguridad de las unidades de red compartidas de la Diputación Provincial de Ávila y resto de aplicativos corporativos. Por este motivo, los usuarios deberán almacenar en estas unidades de red, los datos generados en el desempeño de sus competencias profesionales.

Las unidades de red centralizadas, que la Diputación Provincial de Ávila, pone a disposición de los usuarios. En ninguna de estas unidades de red está permitido almacenar información privada, de ninguna naturaleza.

El almacenamiento de información, fuera de estas unidades de red centralizadas, como por ejemplo en los discos duros, escritorio, carpeta “Mis Documentos”, discos duros externos, deberá estar previamente autorizado por el Departamento de Informática, desde la que le darán las indicaciones necesarias para proceder a la realización de copias de seguridad de esta información.

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 solicitar la recuperación al Departamento de Informática, a través del sistema de gestión de incidencias
previa autorización del Responsable del Servicio/Área a la que pertenece.

7.- NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

Como norma general, en la Diputación Provincial de Ávila, el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros, etc.) no está permitido, salvo autorización expresa del Responsable del Servicio/Área/Departamento del usuario y deberá solicitarse al Departamento de Informática.

En el caso de que a un usuario se le autorice el uso de este tipo de soportes, para trasladar información de titularidad de la Administración, estos soportes deberán cumplir las normas de seguridad establecidas y serán utilizados, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento.

Se deberá almacenar este tipo de dispositivos en lugares seguros, al objeto de prevenir robos o accesos de terceros no autorizados. La pérdida o sustracción de

estos dispositivos, con indicación de su contenido, deberá ponerse en conocimiento del Departamento de Informática de forma inmediata.

7.1.- Normas para el borrado y eliminación de soportes informáticos

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información clasificada como sensible o especialmente protegida, deberán ser eliminados de forma segura para evitar accesos a dicha información. En este sentido, el usuario deberá tener en cuenta las siguientes indicaciones:

Asegurarse que el contenido del soporte puede ser eliminado.

Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por el Departamento de Informática previa petición del Responsable del Servicio/Área/Departamento del usuario.

Cuando contenga información sensible, o protegida, el soporte deberá destruirse según los procedimientos establecidos por el Departamento de Informática.

8.- NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS

8.1.- Impresoras en red, fotocopiadoras y faxes

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 Servicio/Área/Departamento del usuario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la Diputación Provincial de Ávila. Para estos tratamientos de documentos, el usuario debe observar las siguientes indicaciones:

Cuando se impriman documentos, éstos deberán permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

En la realización de copias de documentos y/o escaneo, no debe olvidarse retirar los originales.

Cuando se tenga el conocimiento de que se va a recibir un fax, debe procurar qué estos documentos sean retirados inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no dispone de la autorización precisa.

En caso de encontrase documentación catalogada como sensible “olvidada” en una fotocopiadora/impresora/escáner/fax, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, lo pondrá inmediatamente en conocimiento del Responsable de su Servicio/Área/Departamento, si esta información está catalogada como sensible o especialmente protegida, deberá abrirse el correspondiente incidente de seguridad.

8.2.- Cuidado y protección de la documentación con datos sensibles

La documentación que contenga información catalogada como sensible o protegida, deberá ser protegida, de forma que sólo tenga acceso a ella el personal autorizado, a tal efecto se tendrán en cuenta las siguientes medidas:

Cuando no vaya a ser utilizada deberá estar almacenada en armarios bajo llave.

No podrá ser publicada en tablones o similares.

Cuando los documentos no sean necesarios, deberán ser eliminado o desechados utilizando para ello las destructoras o contenedores de papel según sea el caso.

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

9.- PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de
Información de la Diputación Provincial de Ávila sin la correspondiente licencia de uso.

Los programas informáticos propiedad de la Administración o licenciados a la misma 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.

Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad
Intelectual, sin la debida autorización del Departamento de Informática.

10.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS

El Departamento de Recursos Humanos, mensualmente trasladará al Departamento de Informática, las altas para que se proceda a otorgar el acceso al Portal del Empleado y a los Usuarios Configuradores de la Administración Electrónica para las altas que en el Programa se produzcan. La autorización de acceso al sistema de información (dominio, correo, aplicaciones, carpetas, etc.), así como los permisos en la aplicación serán solicitados por el Responsable del Servicio/Área/Departamento a la que pertenece el usuario. En esta autorización de acceso, el Responsable también establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas. De igual modo, se actuará para la solicitud de cambios en los privilegios de acceso.

Las bajas de usuarios en los sistemas, será comunicada por Servicio de Recursos Humanos al Departamento de Informática y a los Usuarios Configuradores de la Administración Electrónica con la mayor celeridad posible, con una periodicidad máxima de un mes, para proceder a la modificación/eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo, a la mayor brevedad posible. Así mismo, se procederá al bloqueo de acceso a la información contenida en la carpeta de usuario y a su buzón correo electrónico, trascurridos seis meses se procederá al borrado definitivo de su contenido.

Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por el Departamento de Informática en caso de mala utilización. 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.

10.1- Acceso a una cuenta de usuario en su ausencia o baja

Cuando sea necesario acceder a la carpeta personal y/o cuenta de correo corporativa de un usuario, ésta se deberá realizar contando con la autorización expresa de la persona titular de las mismas y solo podrá ser realizado por el Responsable del Servicio/Área del usuario o por la persona en que éste delegue. En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.) este acceso podrá ser realizado, siempre y cuando haya sido autorizado por parte del Responsable del Servicio/Área del usuario y en su defecto por la Secretaría General de la Corporación. En todos los casos, deberá estar debidamente motivado.

10.2- Identificación y Autenticación

Los usuarios dispondrán de un código de usuario y una contraseña para el acceso a los Sistemas de Información de la Diputación Provincial de Ávila y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. Respecto a los cuales deberá de observar las siguientes medidas:

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.

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. De igual modo, no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

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

Los usuarios deben utilizar contraseñas seguras: Las contraseñas han de tener una longitud mínima de 10 caracteres incluyendo letras mayúsculas y minúsculas, caracteres especiales (del tipo @, #, +, etc.) y dígitos numéricos. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables al usuario (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

Las contraseñas deberán cambiarse periódicamente, al menos cada 3 meses. En aquellos sistemas, en los que sea posible, el cambio se solicitará de forma automática. En los que no sea posible, será responsabilidad del usuario su cambio.

11.- PUESTOS DESPEJADOS Y PANTALLAS LIMPIAS

Cuando un usuario deje de atender su equipo durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Por razones de seguridad, el equipo de un usuario se bloqueará automáticamente tras un periodo de inactividad de 10 minutos.

Todo el personal al finalizar la jornada laboral debe de mantener la mesa despejada, libre de documentos, soportes, etc.

12.- CERTIFICADOS ELECTRÓNICOS

El personal que dispongan de certificados electrónicos asociados a tarjetas smartcard y/o instalados en el navegador de Internet, serán responsable de la custodia de los mismos. Por tanto, deberán asegurarse que la seguridad de su contraseña no se ha visto comprometida. De producirse esa sospecha deberá de proceder inmediatamente al cambio de la contraseña y dar traslado este hecho a través del sistema de gestión de incidencias.

El Departamento de Informática proporcionará a los usuarios una copia de seguridad del certificado, en soporte extraíble, siendo también responsabilidad del usuario la custodia de este soporte.

13.- CONFIDENCIALIDAD DE LA INFORMACIÓN

La información contenida en los Sistemas de Información de la Diputación Provincial de Ávila es propiedad de dicho organismo, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia Institución. Además deberá de tener en cuenta las siguientes premisas:

Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por la Administración (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

Los usuarios sólo podrán acceder a aquella información para la que la Administración le haya otorgado las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.

Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de “mínimo privilegio posible y necesidad de conocer”.

14.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

Toda la información contenida en los Sistemas de Información de la Diputación Provincial de Ávila o que circule por sus redes de comunicación deberá ser utilizada únicamente para el cumplimiento de las funciones encomendadas por la Diputación a su personal. La información que comprenda datos de carácter personal quedará regulada por la normativa Europea de protección de datos - Reglamento (UE) 2016/679 – Reglamento General de Protección de Datos (RGPD) y demás normativa complementaria.

Las Políticas, procedimientos e instrucciones en materia de protección de datos establecidas en la Diputación serán de obligado cumplimiento por parte de todos los usuarios que realicen tratamientos de datos personales.

Todo usuario de la Diputación Provincial de Ávila o de terceras organizaciones 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 Diputación Provincial de Ávila.

Queda prohibido, asimismo, transmitir o alojar información que contenga categorías especiales de datos del Diputación Provincial de Ávila, en servidores externos al mismo, salvo autorización expresa del Delegado de Protección de Datos (DPD).

La contratación de servicios externos con acceso a datos personales, requiere la formalización de un contrato de encargo de tratamiento con la empresa prestadora del servicio y/o acuerdos de confidencialidad, así como el establecimiento de acuerdos de nivel del servicio. Igualmente, en algunos casos además, podría implicar el alojamiento de datos fuera del
territorio español, por lo que será necesario analizar la inexistencia de trabas legales.

15.- SALIDA DE INFORMACIÓN

La salida de información de la Diputación Provincial de Ávila (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado previamente por el Responsable Servicio/Área a la que pertenezca el usuario, autorización que contemplará igualmente a la información que sale.

La salida de información con datos sensibles, incluido el correo electrónico, requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Solicitar al Departamento de Informática las instrucciones necesarias para la implementación de estas medidas de seguridad.

Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la legislación vigente en materia de protección de datos.

16.- USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la Diputación Provincial de Ávila, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. 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.

Todos los correos salientes deberán incluir el modelo de firma establecida en la Administración.

El acceso a cuentas de correo gratuitas (Gmail, Yahoo!, Hotmail, etc.) desde los equipos (fijos o móviles) puestos a disposición del personal por parte de la Administración, supone una amenaza a la seguridad, por lo que su uso deberá ser limitado y deberán de aplicarse las mismas normas que para el correo corporativo. No está autorizado el reenvío del correo profesional a este tipo de cuentas.

Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades. Motivo por el cual se establecen las siguientes directrices con el objetivo reducir el riesgo en el uso del correo electrónico:

Utilizar el correo electrónico exclusivamente para propósitos profesionales. Gran parte de los mensajes de correo electrónico no deseados que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo. Utilizar el correo electrónico únicamente para fines profesionales reduce la posibilidad de ataque.

No se debe ceder el uso de la cuenta de correo a terceras personas. Esto provocaría una suplantación de identidad y el acceso a información confidencial.

Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y cuando el fin último sea el cumplimiento de las funciones encomendadas.

Revisar la barra de direcciones antes de enviar un mensaje. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo Con Copia (CC). Además deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.

No se deben enviar o reenviar correos de forma masiva. Si previa autorización se envía por necesidad un correo a un conjunto de destinatarios, conviene usar una lista de distribución o, en su defecto, colocar la lista de direcciones en el campo de Copia
Oculta (CCO), evitando su visibilidad a todos los receptores del mensaje.

No enviar mensajes en cadena. Las alarmas de virus y las cadenas de mensajes son, en muchas ocasiones, correos simulados, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus, se debe proceder a su borrado inmediatamente.

No responder a mensajes de Spam. La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la Corporación. En cualquier caso, nunca debe responderse a los mismos.

No está autorizado el envío de correos que contengan en el cuerpo o en los adjuntos información con datos sensibles. En caso de que sea necesario el envío de esta información deberá ponerse en contacto con el Departamento de Informática, la cual le proporcionará mecanismos alternativos para su realización. En todo caso, esta salida de información deberá estar autorizada por el Responsable del Área/Servicio a la que pertenece el usuario.

Asegurar la identidad del remitente antes de abrir un mensaje. Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información sensible, confidencial o protegida a petición de un correo del que no se puede asegurar la identidad del remitente debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

No abrir correos basura ni correos sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra spam, no debe abrirse, debiendo reportarse el correspondiente incidente de seguridad. Es conveniente borrar los correos sospechosos o, al menos, situarlos (sin abrir) en una zona de cuarentena.

No ejecutar archivos adjuntos, ni “pinchar” en enlaces sospechosos. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

Informar de correos con virus, sin reenviarlos. Si el personal detectara que un correo contiene un virus o, en general, código malicioso, hay que notificar el incidente de seguridad al Departamento de Informática, a través del gestor de incidencias y no reenviarlo, para evitar su posible propagación.

No utilizar el correo electrónico como espacio de almacenamiento. La capacidad de espacio en los servidores de correo de la Corporación es limitada. Cuando una cuenta se satura puede ser que se restrinjan por parte del servidor los privilegios de envío y/o recepción de mensajes o que se realice un borrado, más o menos selectivo, de los mensajes almacenados. Por todo ello, se recomienda conservar únicamente los mensajes imprescindibles y revisar periódicamente aquellos que hubieren quedado obsoletos.

En relación con el acceso remoto (vía web) al correo electrónico, deben adoptarse las siguientes cautelas:

Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.

Desactivar la interpretación de contenidos remotos a la hora de leer mensajes de correo vía webmail.

Desactivar las características de recordar contraseñas para el navegador.

Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.

Salvo autorización expresa, está prohibida la instalación de “complementos” para el navegador.

16.1.1.- Prevención contra el SPAM

El término spam se define como el envío de correos no solicitados, de forma masiva, a direcciones de correo electrónico, constituyendo uno de los problemas de seguridad más habituales con los que se enfrentan las organizaciones. Tales mensajes pueden contener código dañino que de penetrar en los sistemas de información pueden propagarse a través de las redes de comunicación.

La Administración ha implementado medidas técnicas de prevención y eliminación de spam. No obstante es necesario que los usuarios observen las siguientes pautas:

Con carácter general, sólo se proporcionará la dirección de correo electrónico profesional de la Administración a personas de confianza y del entorno profesional.

Se debe evitar introducir la dirección de correo de la Administración en foros de noticias o listas de correo a través de Internet, salvo en los casos necesarios y con proveedores de confianza. Muchos ataques de spam se sirven de estas direcciones, introducidas en sitios no seguros.

Con carácter general, si no se conoce el remitente de un correo, y/o el asunto del mismo es extraño, se recomienda borrar el mensaje (o situarlo en cuarentena hasta disponer de más datos), especialmente si contiene ficheros adjuntos.

La Corporación dispone de sistemas antispam para la detección y borrado de mensajes identificados como spam. Sin embargo, es posible que dichos sistemas no puedan eliminar la totalidad de estos mensajes. Por este motivo, si recibe un mensaje de spam, deberá:

Si lo reconociera como tal por la dirección o el asunto que contiene, lo borrará inmediatamente (sin abrirlo).

No responderá nunca.

No accederá a los enlaces o anexos que pudieran contener.

17.- ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

El acceso corporativo a Internet es un recurso centralizado que la Diputación Provincial de Ávila 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. La Administración 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. Respecto al acceso a Internet se observarán las siguientes normas generales:

El acceso a Internet (incluido redes sociales) deberá ser autorizado por el Responsable del Servicio/Área a la que pertenece el usuario, siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante.

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. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por el Departamento de Informática, en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización de dicho Servicio.

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.

Se consideran usos prohibidos las siguientes actuaciones:

La descarga regular de archivos muy voluminosos, especialmente en horarios coincidentes con el horario laboral, salvo autorización expresa.

La descarga de programas informáticos sin la autorización previa del Departamento de Informática o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.

El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizada por el Departamento de Informática.

18.- INCIDENCIAS DE SEGURIDAD

Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Diputación Provincial de Ávila o su imagen, deberá informar inmediatamente al Departamento de Informática, a través del sistema de gestión de incidencias, que lo registrará debidamente y elevará, en su caso.

19.- ACCESO A LOS SISTEMAS DE INFORMACIÓN Y PERMANENCIA DE TERCEROS EN LOS EDIFICIOS, INSTALACIONES Y DEPENDENCIAS DE LA ADMINISTRACIÓN

El personal ajeno a la Institución que temporalmente deba acceder a los Sistemas de Información de la Diputación Provincial de Ávila, deberá hacerlo siempre bajo la supervisión de algún miembro de la misma y previa autorización Responsable del Servicio/Área afectado y deberán de observar las siguientes normas:

Para los accesos de terceros a los sistemas de información de la Administración, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.

Tales personas, en lo que les sea de aplicación, deberán cumplir la presente
Normativa, así como el resto de normativa de seguridad de la Administración.

Cualquier incidencia que pudiera afectar y/o comprometer la seguridad de los sistemas de información de la Administración, durante el acceso de terceros deberá de ponerse en conocimiento del Departamento de Informática, a la mayor brevedad posible.

Una vez en el interior de los edificios, dependencias o instalaciones de la Administración, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común (aseos, comedor, zona de máquinas de cafetería, etc.).

20.- ACCESOS DEL PERSONAL DEL SERVICIO SOPORTE

El personal que realice labores de asistencia y/o soporte a las personas usuarias del sistema de información, se obliga a actuar con absoluta diligencia, teniendo el deber y la obligación de guardar confidencialidad respecto a la información a la que tengan acceso para el cumplimiento de sus actividades, quedando estrictamente prohibido comunicarla o facilitarla, directa o indirectamente a ningún tercero. Siendo algunas de sus actividades, entre otras, las siguientes:

Acceso (remoto y/o presencial) a los equipos y sistemas de información para llevar a cabo tareas de mantenimiento.

Acceso (remoto y/o presencial) a los equipos, sistemas de información y documentos electrónicos por motivos de seguridad.

Configurar los accesos de los usuarios a los sistemas de información que requieren para el cumplimiento de sus tareas, así como a los equipos informáticos.

Acceso a los equipos, redes o sistemas de información por incidencias en la Seguridad de la Información.

En estas asistencias, como norma general, las personas usuarias de los equipos estarán presentes, en todo momento, durante la realización de estas acciones.

21.- MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

La Diputación Provincial de Ávila, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.

Monitorizará los accesos a la información contenida en sus sistemas.

Auditará la seguridad de las credenciales y aplicaciones.

Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Información de protección de datos:

Responsable del tratamiento: Diputación Provincial de Ávila. | Finalidad del tratamiento: Garantizar el cumplimiento de lo establecido en la presente normativa, gestión de los sistemas de información de la Diputación y velar por el cumplimiento de las políticas y normas que les afectan. | Legitimación: Relación contractual de carácter laboral/funcionarial, para el tratamiento de datos personales de la persona empleada y relación contractual de carácter mercantil en el caso de personal externo.
| Plazos de conservación: Los previstos por la legislación aplicable según la tipología de los datos tratados respecto a la prescripción de responsabilidades. | Destinatarios: No se cederán datos a terceros, salvo obligación legal. | Derechos: Acceder, rectificar y suprimir los datos, así como otros derechos, ante el responsable del tratamiento Diputación Provincial de Ávila - Plaza Corral de las Campanas, s/n - 05001 – ÁVILA (Ávila), indicando en el asunto: Ref. Protección de Datos o a través de la Sede Electrónica.

La Diputación Provincial de Ávila llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la

información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegitimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

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. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El Departamento de Informática en colaboración de las restantes Unidades Administrativas de la Administración, velará por el cumplimiento de la presente Normativa e informará al Comité de Comité de Cumplimiento Normativo de Transparencia y Seguridad sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

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.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

22.- INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de los Sistemas de Información de la Diputación Provincial de Ávila están obligados a cumplir lo prescrito en la presente Normativa General de Utilización de los Recursos y Sistemas de Información.

En el supuesto de que un usuario no observe alguna de los preceptos señalados el presente Reglamento, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.”