NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Índice

CONTROL DE REVISIONES

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	ELABORADO
1.0	Primera versión del documento	19/06/2020
2.0	Actualización del procedimiento	24/03/2022
3.0	Actualización del punto 9.1 de la normativa	12/12/2024

1 Objeto

La continua evolución tecnológica que se está experimentado en la administración pública y más en concreto en RADMAS TECHNOLOGIES, encaminándonos a una administración totalmente digital, con una gestión considerable de volúmenes de datos, herramientas específicas y gran variedad de dispositivos, conlleva que exista un sistema informático complejo donde la seguridad debe estar garantizada en todo momento. El usuario debe ser consciente de la importancia de dicha seguridad y disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos.

Por ello, con el fin de garantizar la correcta gestión del sistema, RADMAS TECHNOLOGIES acuerda aprobar las siguientes normas de utilización del Sistema Informático de la Institución para garantizar el buen uso de los medios técnicos puestos a disposición de los usuarios:

2 Alcance

Esta Normativa es de aplicación a todo el ámbito de actuación de RADMAS TECHNOLOGIES, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en RADMAS TECHNOLOGIES, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de RADMAS TECHNOLOGIES.

En el ámbito de la presente normativa, se entiende por usuario cualquier usuario perteneciente o ajeno a RADMAS TECHNOLOGIES, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con RADMAS TECHNOLOGIES y que utilice o posea acceso a los Sistemas de Información de RADMAS TECHNOLOGIES.

3 Vigencia

La presente Normativa de Seguridad de la Información de RADMAS TECHNOLOGIES ha sido aprobada por el Director General de RADMAS TECHNOLOGIES, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que RADMAS TECHNOLOGIES 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.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de RADMAS TECHNOLOGIES.

4 Revisión y evaluación

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

- Interpretar las dudas que puedan surgir en 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.
- Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación del Director General de RADMAS TECHNOLOGIES.
- 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.
- Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5 Utilización del equipamiento informático y de comunicaciones

RADMAS TECHNOLOGIES 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 RADMAS TECHNOLOGIES pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos RADMAS TECHNOLOGIES, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este apartado concierne específicamente a todos los equipos facilitados por RADMAS TECHNOLOGIES para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

5.1 Normas generales

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

- 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 de RADMAS TECHNOLOGIES. Cuando se precise instalar dispositivos no provistos por RADMAS TECHNOLOGIES deberá solicitarse autorización previa al Departamento Técnico.

- 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 del Departamento Técnico.

- Salvo autorización expresa del Departamento Técnico, los usuarios podrán modificar la configuración de los equipos.

- 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.

- Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad, que tomará las oportunas medidas correctoras.

- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.

- Los usuarios deberán notificar al Responsable de Seguridad de RADMAS TECHNOLOGIES, a la mayor brevedad posible, siempre en un plazo de tiempo no superior a una hora, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad de la información de RADMAS TECHNOLOGIES.

- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable de los equipos para reducir este riesgo.

- 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.

- El cese de actividad de cualquier usuario debe ser comunicado de forma inmediata al Departamento de Administración, con el objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por RADMAS TECHNOLOGIES estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

5.2 Usos específicamente prohibidos

Están terminantemente prohibidos los siguientes comportamientos:

- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por RADMAS TECHNOLOGIES, sin la previa autorización del Departamento Técnico.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por RADMAS TECHNOLOGIES.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización y solicitud expresa al Departamento de Administración.
- 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.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de RADMAS TECHNOLOGIES.
- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

5.3 Normas específicas para equipos portátiles y móviles

- Los equipos portátiles y móviles serán asignados por el Departamento de Administración a petición del Responsable de Área correspondiente.

- Existirá un inventario actualizado de los equipos portátiles y móviles. El Departamento de Administración será responsable de gestionar dicho inventario.

- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, quién deberá 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 Administración para la adopción de las medidas que correspondan y a efectos de baja en el inventario.

- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de RADMAS TECHNOLOGIES.

- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a RADMAS TECHNOLOGIES o no autorizadas para ello.

- Los usuarios de equipos portátiles deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por RADMAS TECHNOLOGIES, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.

- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).

- Los usuarios no realizarán cambios de configuración en los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al Departamento Técnico llevar a cabo estas modificaciones.

- Los equipos portátiles no deberán contener claves de acceso remoto a la organización.

5.4 Uso de memorias/lápices USB (pendrives)

- Con carácter general, el uso de memorias USB en RADMAS TECHNOLOGIES no está autorizado. En su caso, la autorización deberá proporcionarla el Departamento de Administración.

- En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por RADMAS TECHNOLOGIES, que serán conformes a las normas de seguridad de la organización.

- Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. RADMAS TECHNOLOGIES podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de RADMAS TECHNOLOGIES unidades de almacenamiento en red, que podrán usarse para tal propósito.

- La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Departamento de Administración, de forma inmediata.

5.5 Grabación de CDs y DVDs

- Con carácter general, el uso de equipos grabadores de CDs y DVDs en RADMAS TECHNOLOGIES no está autorizado. En su caso, la autorización deberá proporcionarla el Departamento de Administración.

5.6 Impresoras en red y fotocopiadoras

- 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 RADMAS TECHNOLOGIES y, en su consecuencia, estén debidamente inventariados.

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

- 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 Responsable de Seguridad.

5.7 Digitalización de documentos

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

- 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 Responsable de Seguridad.

5.8 Protección de equipos y puestos de trabajo

- Los puestos de trabajo del personal deben ubicarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. No será de aplicación esta norma en el caso de equipos que estén destinados al uso público.

- Los puestos ubicados en zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

- Al finalizar la jornada de trabajo, los usuarios deben guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

- Cada vez que un usuario se ausente de su lugar de trabajo debe bloquear su puesto de usuario, de forma que se proteja el acceso a las aplicaciones y servicios. Adicionalmente, los puestos de trabajo se configurarán para bloquearse automáticamente tras un periodo de inactividad.

5.9 Telefonía Móvil

- El personal al servicio de RADMAS TECHNOLOGIES dispondrá de este tipo de recursos cuando la naturaleza de las funciones encomendadas lo justifique y previa autorización del Área de Administración.

- Justificada la necesidad de disponer de teléfono móvil, se clasificará a los usuarios según perfiles de uso.

- Existe un perfil de datos para aquellos usuarios que deban utilizar acceso a datos de Internet, que en todo caso tendrá habilitada tarifa plana.

- El servicio de datos internacional se encontrará desactivado; podrá ser autorizado puntualmente en casos debidamente motivados o bien se puede autorizar la utilización de bonos con importe limitado para su consumo en el extranjero.

- Se debe evitar perder de vista el dispositivo y, en caso de pérdida o robo, informar lo antes posible para proceder a su bloqueo.

- Los dispositivos deberán tener activado el bloqueo por PIN y, siempre que lo permitan, se activará la opción de bloqueo de terminal cada cierto tiempo y la solicitud de una contraseña para desbloquearlo.

- No se permite la modificación del hardware o software del dispositivo móvil sin previa autorización.

- Siempre que sea posible, no se almacenará la información sensible en los dispositivos móviles, asegurándose de limpiar los archivos temporales periódicamente.

- Se podrán utilizar programas de cifrado para proteger la información sensible.

- Solo se realizarán conexiones de dispositivos móviles a redes inalámbricas que ofrezcan confianza.

- El bluetooth se desconectará siempre que no se utilice. Estará configurado como oculto y con contraseña. No se permite la conexión a un dispositivo bluetooth de origen desconocido y se evitará realizar emparejamientos en lugares públicos.

- El usuario será responsable de realizar las copias de respaldo de la información almacenada en el dispositivo móvil.

5.10 Cuidado y protección de la documentación impresa

- 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, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

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

- Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.

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

5.11 Pizarras

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

5.12 Protección de la dignidad de las personas

- Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

6 Identificación y autenticación

- Los usuarios dispondrán de un código de usuario y una contraseña, para el acceso a los Sistemas de Información de RADMAS TECHNOLOGIES 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.

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

- Los usuarios 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 Responsable de Seguridad el correspondiente incidente de seguridad.

- Los usuarios deben utilizar contraseñas seguras de acuerdo a la política de calidad de contraseñas que RADMAS TECHNOLOGIES establezca. 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.).

- 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 Responsable de Seguridad, de forma inmediata.

7 Acceso de terceros a los edificios

Los terceros ajenos a RADMAS TECHNOLOGIES que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- El personal ajeno a RADMAS TECHNOLOGIES que temporalmente deba acceder a los Sistemas de Información de RADMAS TECHNOLOGIES, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de RADMAS TECHNOLOGIES (responsable).

- Cualquier incidente que surja antes o en el transcurso del acceso a RADMAS TECHNOLOGIES deberá ponerlo en conocimiento de su responsable.

- Para los accesos de terceros a los sistemas de información de RADMAS TECHNOLOGIES, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en RADMAS TECHNOLOGIES. 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 puntualmente la presente Normativa General, así como el resto de normativa de seguridad de RADMAS TECHNOLOGIES.

- Para acceder a los edificios, instalaciones o dependencias de RADMAS TECHNOLOGIES deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse y solicitar la presencia de la persona responsable de RADMAS TECHNOLOGIES, que constituirá su enlace durante su estancia en él.

- Una vez en el interior de los edificios, dependencias o instalaciones de RADMAS TECHNOLOGIES, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común.

- Asimismo, deberán tener autorización del responsable cuando tengan necesidad de realizar desplazamientos entre distintos departamentos de RADMAS TECHNOLOGIES.

- Los terceros atenderán siempre a los requerimientos que le hiciere el personal de seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

8 Uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de RADMAS TECHNOLOGIES, 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.

Por ello, se dictan las siguientes normas de uso.

8.1 Normas generales

- 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.

- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por RADMAS TECHNOLOGIES.

- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.

- Se deberá notificar al Departamento de Informática cualquier tipo de anomalía detectada, así como un alto volumen de correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.

- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutar 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.

- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.

- Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

8.2 Usos especialmente prohibidos

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.

- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.

- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.

- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.

9 Acceso a internet y otras herramientas de colaboración

El acceso corporativo a Internet es un recurso centralizado que RADMAS TECHNOLOGIES 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.

RADMAS TECHNOLOGIES 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.

9.1 Normas generales

- Usar Internet para fines profesionales. Internet es una herramienta más de las utilizadas por los usuarios de RADMAS TECHNOLOGIES Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales (docencia, investigación, formación y uso administrativo). Si en algún caso fuese necesario realizar un uso personal (Por ejemplo, acceso a nóminas o gestión de vacaciones), se deberá utilizar un navegador web diferente al utilizado habitualmente para uso profesional, de forma que se separen las cookies almacenadas y se evite la contaminación entre uso personal y uso organizativo.

- No visitar páginas de contenido poco ético, ofensivo o ilegal. No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.

- No visitar páginas no fiables o sospechosas. Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas que se consideren sospechosas de contener código malicioso.

- Cuidar la información que se publica en Internet. No se debe proporcionar información sobre la organización en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin autorización cualquier tipo de información no pública sobre el funcionamiento interno de RADMAS TECHNOLOGIES, sus recursos, estructura, etc.

- Observar las restricciones legales que sean de aplicación. Antes de utilizar una información obtenida de Internet, los usuarios deberán comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.

- Realizar descargas sólo si se tiene autorización. Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque RADMAS TECHNOLOGIES decida no limitar técnicamente la capacidad para descargar archivos de audio o vídeo, los usuarios deberán tener en consideración que la

descarga de estos archivos puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, limitarán su descarga y reproducción al ámbito estrictamente profesional.

- No descargar código o programas no confiables. Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Conviene que tales actividades sean acometidas, de manera exclusiva, por el Servicio de Tecnologías de la Información y las Comunicaciones (STIC).

- Asegurar la autenticidad de la página visitada. Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad.

- Comprobar la seguridad de la conexión. En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar HTTP (examinando la barra de direcciones). También debería aparecer un icono representando un candado en la barra del navegador. A través de dicho candado se puede obtener información sobre el certificado digital de identidad del sitio web visitado.

- Cerrar las sesiones al terminar la conexión. Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información (siempre que se haya autenticado en la página web), ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otros usuarios tengan acceso a las cuentas de los usuarios que no hubieren cerrado correctamente las sesiones. La mayoría de los sitios web disponen de una opción de “desconexión”, “logout” o similar que conviene utilizar.

- Utilizar herramientas contra código dañino. El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes. Por tanto, es necesario disponer del adecuado abanico de herramientas que permitan una adecuada protección. El uso de un antivirus permanentemente actualizado es la primera medida de protección contra este tipo de ataques. Además de ello, es necesario configurar y usar adecuadamente cortafuegos, software específico contra programas espía (spyware), etc.

- Mantener actualizado el navegador y las herramientas de seguridad. Es imprescindible actualizar las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.) a las últimas versiones estables, siempre de conformidad con lo indicado y aprobado por el STIC. Puesto que el código dañino se genera incesantemente,

es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar sobre cualquier problema que se detecte en este proceso.

- Utilizar los niveles de seguridad del navegador. Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.

- Desactivar las cookies. Las cookies son pequeños programas fragmentos de texto que emplean los servidores Web para almacenar y recuperar información acerca de sus visitantes (Por ejemplo, quién, cuándo y desde dónde se ha conectado un usuario). Estos programas fragmentos de texto se almacenan en el ordenador del usuario al visitar una página Web, pudiendo ser desactivados usando las herramientas disponibles en el navegador.

- Eliminar la información privada. Los navegadores Web almacenan información privada durante su utilización, tal como el historial de navegación, cookies aceptadas, contraseñas, etc., información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.

- No instalar complementos desconocidos. Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (plug-in, add-on, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.

- Limitar y vigilar la ejecución de Applets y Scripts. Los scripts son un conjunto de instrucciones que permiten la automatización de tareas. Los applets son pequeñas aplicaciones (componentes de aplicaciones) que se ejecutan en el contexto del navegador Web. A pesar de que, en general, resultan útiles, pueden ser usados para ejecutar código malicioso y, por tanto, es recomendable limitar su ejecución.

9.2 Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

- La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.

- 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.).

10 Normativa en materia de uso de redes sociales

Los siguientes epígrafes recogen el conjunto de medidas que deben tenerse en cuenta cuando se use o se pretendan usar las Redes Sociales como herramienta de comunicación y difusión de las funciones competencialmente de RADMAS TECHNOLOGIES.

10.1 Autorización previa

Con carácter general, y salvo las excepciones que pudieran autorizarse en RADMAS TECHNOLOGIES, y que, en todo caso, deberán estar recogidas en la Política de Seguridad institucional, ninguna persona que preste sus servicios en RADMAS TECHNOLOGIES podrá darse de alta en ninguna red social, en nombre o en representación de RADMAS TECHNOLOGIES, salvo autorización expresa de Gerencia con el conocimiento del Responsable de Seguridad.

Por tanto, salvo en el supuesto señalado, la presencia en las redes sociales de un empleado público de RADMAS TECHNOLOGIES será siempre a título personal.

10.2 Medidas comportamentales

Una vez autorizado a darse de alta en una red social en representación de RADMAS TECHNOLOGIES, el empleado público usuario de la red social de que se trate debe observar las siguientes normas de comportamiento:

- Recordar en todo momento que las redes sociales constituyen un foro público. Por tanto, por el hecho de agregar cualquier dato, comentario o información, el usuario está asumiendo que éste puede ser visto por los restantes usuarios de tal red social, por RADMAS TECHNOLOGIES y, en general, por cualquier persona.

- Si el usuario está usando el perfil de la red social en representación de RADMAS TECHNOLOGIES, conviene mostrar abiertamente tal representación, a menos que existan circunstancias excepcionales que no lo aconsejen, tales como una amenaza potencial a la seguridad personal. En cualquier caso, nunca deben proporcionarse detalles personales tales como la dirección o los números de teléfono personales.

- Es siempre recomendable hablar en primera persona, tratando de aportar valor en los comentarios vertidos, facilitando informaciones y perspectivas contrastadas y que no se encuentren tipificadas como información clasificada o cuya revelación pudiera ocasionar un perjuicio a RADMAS TECHNOLOGIES o, en general, a cualquier persona o entidad, pública o privada. El usuario debe recordar que será siempre responsable de sus aportaciones y de las eventuales consecuencias en su reputación y, por ende, en la de RADMAS TECHNOLOGIES en el que presta sus servicios. En caso de dudas, lo mejor es abstenerse de hacer una contribución.

- Las redes sociales deben constituir un foro de intercambio de opiniones o para el debate constructivo, pero no es el ámbito apropiado para crear polémica, descalificar a otras personas o a terceros, ni para presentar quejas y reclamaciones que deben canalizarse a través de las vías específicas que la Administración Pública y al propio RADMAS TECHNOLOGIES tiene establecidas para esa finalidad.

- El usuario debe tratar con respeto a los otros usuarios, usando un lenguaje apropiado y correcto y actuando siempre como si estuviera en presencia de la(s) otra(s) persona(s).

- Salvo autorización, el usuario no debe publicar material publicitario ni comunicacional de RADMAS TECHNOLOGIES, ni debe hacer uso de su perfil en la red social para lucrarse o hacer negocio, ni para comparar las funciones, competencias o, en general, desenvolvimiento de RADMAS TECHNOLOGIES con otras entidades.

- Los contenidos publicados en las redes sociales pueden estar sujetos a Derechos de Propiedad Intelectual, por lo que la publicación de cualquier contenido requiere tener la certidumbre de que se encuentra libre de estas cargas.

- La contribución del usuario en la red social debe presentar datos reales, concretos y argumentación consistente. Se permiten citas o la reproducción de pequeños fragmentos de textos, libros u obras de terceros en general, siempre y cuando se indique la fuente y el nombre del autor. Si el usuario realiza una contribución propia (texto, fotografías, gráficos, vídeos o audios) debe saber que otorga a RADMAS TECHNOLOGIES autorización para reproducirla en cualquier medio físico o virtual donde se indicará el nombre del empleado público como autor, todo ello sin perjuicio de que otros usuarios también podrían guardarlos o reproducirlos.

- El logotipo de RADMAS TECHNOLOGIES y, en general, cualquier otro logotipo o distintivo gráfico de RADMAS TECHNOLOGIES o de cualquier entidad del Sector Público constituyen marcas registradas. También son titularidad de RADMAS TECHNOLOGIES los contenidos colgados en su portal o sede electrónica y, por tanto, RADMAS TECHNOLOGIES se reserva todos los derechos de propiedad intelectual e industrial asociados a los mismos. El usuario debe comprometerse a respetarlos y a no utilizarlos sin la debida autorización, cualquiera que sea el medio.

- La descarga de contenidos, su copia o impresión requerirá autorización del superior del empleado (Jefe de Área, Servicio o Departamento).

- En ningún caso deberá usarse la red social para el intercambio de credenciales o contraseñas, de cualquier sistema y para cualquier finalidad.

- La información contenida en el perfil de la red social no deberá considerarse nunca como información oficial en relación con las funciones y competencias de RADMAS TECHNOLOGIES, en los términos que puedan estar reservados a las funciones de la sede electrónica de RADMAS TECHNOLOGIES, según dispone el art. 38 de la Ley 40/2015.

- El perfil de la red social de que se trate puede contener manifestaciones sobre previsiones o estimaciones que incluyen comentarios sobre el desarrollo de las funciones de RADMAS TECHNOLOGIES basadas en juicios actuales, pudiendo suceder que determinados riesgos, incertidumbres y otros factores relevantes, desconocidos o imprevisibles ocasionen que los resultados difieran materialmente de lo esperado. El usuario debe recordar que las declaraciones relativas a los resultados, funciones, competencias, etc., no pretenden dar a entender que el desempeño de RADMAS TECHNOLOGIES será necesariamente el previsto. Nada en el perfil debe ser tomado como una previsión de resultados.

- RADMAS TECHNOLOGIES velará en todo momento por preservar el buen uso del perfil y, por ello, RADMAS TECHNOLOGIES, como administrador, se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que:

    - Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales a RADMAS TECHNOLOGIES, sus empleados, colaboradores o terceros.

    - Incorpore datos de terceros sin su autorización.

    - Contenga cualquier tipo de recomendación relativa a las funciones y competencias de RADMAS TECHNOLOGIES privilegiada o material publicitario o de comunicación, personal o en beneficio de terceros, sean personas físicas o jurídicas.

    - Sea redundante.

    - No esté relacionada con la finalidad perseguida por RADMAS TECHNOLOGIES al darse de alta en la red social de que se trate.

10.3 Uso de medios sociales con fines exclusivamente personales

En ocasiones, el uso personal o profesional de una red social puede llegar a confundirse. Por tanto, se debe ser consciente de las responsabilidades cuando se mezclan la vida personal y la laboral en estos medios.

Las personas que trabajan para RADMAS TECHNOLOGIES deben usar su buen juicio y asumir la responsabilidad personal y profesional de los contenidos que publican a través de los medios sociales.

Es frecuente que se admita el uso de una cuenta personal para comentar sobre asuntos no relacionados con el trabajo, aunque no debiera permitirse, de manera general, que el uso de tales cuentas se lleve a cabo en horario laboral ni, por motivos de seguridad, usando los medios electrónicos de RADMAS TECHNOLOGIES.

En cualquier caso, el uso de plataformas de redes sociales nunca debe interferir con las funciones principales, con la excepción de aquellos puestos de trabajo que incluyan entre sus tareas precisamente el uso de estas herramientas sociales.

Debemos recordar que el uso de una cuenta privada no exime de cumplir los códigos de buena conducta generalmente admitidos y los específicamente contemplados en la Política de Seguridad de la Información de RADMAS TECHNOLOGIES.

Por todo ello, no deben publicarse opiniones personales a través de cuentas oficiales y tampoco promover las cuentas personales a través de cuentas oficiales.

No debe comentarse en redes sociales aquello que no debe ser de dominio público, aunque exista una única persona a la que se desee dejar al margen. Las redes sociales pueden actuar de amplificador y comprometer a sus usuarios.

Aquellas personas que tienen responsabilidades de gobierno, en virtud de su posición, deben tener en cuenta si los comentarios personales que publican, incluso en lugares claramente personales, pueden ser mal interpretados como declaraciones realizadas por RADMAS TECHNOLOGIES.

10.4 Medidas de seguridad de la información

En primer lugar, es preciso identificar claramente los canales oficiales de RADMAS TECHNOLOGIES que ya pudieran existir y, en la medida de lo posible, diferenciar los canales verdaderos e impulsar la vigilancia y el cierre de canales falsos.

10.5 Medidas de seguridad tecnológica

Las cuentas en redes sociales de RADMAS TECHNOLOGIES se crearán desde correos electrónicos corporativos, delegándose la gestión de las mismas en las unidades organizativas designadas para cada una de ellas.

El Responsable de Seguridad de RADMAS TECHNOLOGIES extenderá sus competencias a los perfiles de redes sociales que pudieran crearse.

La custodia de las contraseñas de los perfiles de las redes o de sus administradores que así lo requieran, estará centralizada y será responsabilidad de la unidad organizativa de la entidad de que se trate.

Cualquier instalación de aplicaciones de terceros que tenga algún tipo de permisos sobre cuentas de las redes sociales deberá ser previamente autorizada por el Responsable de Seguridad de RADMAS TECHNOLOGIES, para verificar que esta aplicación no pone en riesgo ni los datos ni la seguridad de la cuenta.

La modificación de cualquiera de las opciones de privacidad o publicación de comentarios deberá autorizarse previamente por RADMAS TECHNOLOGIES, contando con la opinión del Responsable de Seguridad.

Como norma general, las contraseñas de las plataformas de gestión deberán ser robustas.

Siempre que sea posible, es conveniente mantener las cuentas desde una herramienta de gestión que pueda otorgar permisos diferentes de publicación y que su acceso no se realice a través de la propia contraseña de la red social de que se trate. El responsable de cada cuenta definirá quiénes son las personas que la gestionarán, velando y haciendo respetar la confidencialidad de las contraseñas de acceso.

Siempre que sea posible, el acceso a las cuentas se realizará desde sistemas corporativos. En caso de necesitar publicar contenidos desde un dispositivo móvil, se hará desde una aplicación diferente a la que se utiliza de modo personal.

11 Incidentes 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 RADMAS TECHNOLOGIES o su imagen, deberá informar inmediatamente al Departamento de Informática, que lo registrará debidamente en la herramienta corporativa Jira.

- Ante un incidente de pérdida o robo de un dispositivo móvil, el usuario responsable de dicho dispositivo deberá notificarlo de manera inmediata al Departamento de Administración bien por vía telefónica (91 777 36 33 / 669 22 66 78) o por correo electrónico (dpto.administracion@radmas.com).

12 Compromiso de los usuarios

Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad fijadas por RADMAS TECHNOLOGIES, 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.

- 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 de RADMAS TECHNOLOGIES establezca al respecto.

- Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de RADMAS TECHNOLOGIES para desarrollar actividades que persigan o tengan como consecuencia:

    - El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.

    - La degradación de los servicios.

    - La destrucción o modificación no autorizada de la información, de manera premeditada.

    - La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.

    - El deterioro intencionado del trabajo de otras personas.

- El uso de los sistemas de información para fines ajenos a los de RADMAS TECHNOLOGIES, salvo aquellas excepciones que contempla la presente Normativa.

- Dañar intencionadamente los recursos informáticos de RADMAS TECHNOLOGIES o de otras instituciones.

- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

13 Monitorización y aplicación de esta normativa

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

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

b) Monitorizará los accesos a la información contenida en sus sistemas.

c) Auditará la seguridad de las credenciales y aplicaciones.

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

RADMAS TECHNOLOGIES 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 ilegítimo 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 Responsable de Seguridad, con la colaboración de las restantes unidades de RADMAS TECHNOLOGIES, velará por el cumplimiento de la presente Normativa General e informará al Comité de 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.

14 Incumplimiento de la normativa

Todos los usuarios de RADMAS TECHNOLOGIES están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa, 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.