MADRID
desarrollo urbano
área delegada de vivienda

emvs
Empresa Municipal de la Vivienda y Suelo

Empresa Municipal de la Vivienda y Suelo de Madrid S.A.

CÓDIGO DE NORMAS Y BUENAS PRÁCTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

INFORMACIÓN RELEVANTE DEL DOCUMENTO	
Título de la Norma	Código de Normas y Buenas Prácticas para la Seguridad de la Información y Protección de Datos
Responsable principal de su vigilancia	Consejo de Administración
Órgano que lo promueve y autor	Dirección de Transparencia, Cumplimiento y Protección de Datos
Órgano de aprobación	Consejo de Administración
Fecha de aplicación	27 enero 2023
Publicada y accesible	Portal de Transparencia e Intranet

Fecha	Versión	órgano	Observaciones
Octubre 2022	1.0	DTCPD	Elaboración del documento
27 enero 2023	1	Consejo Administración	Aprobación

CONTENIDO

1. INTRODUCCIÓN

El presente Código de Normas y Buenas Prácticas forma parte de la Política de Seguridad de la Información y de la Protección de Datos, como instrumento para salvaguardar a la EMVS de posibles riesgos relacionados con la Confidencialidad, Accesibilidad, Disponibilidad, Integridad de la Información y los Datos Personales.

La Dirección de la Empresa tendrá potestad disciplinaria para imponer sanciones en respuesta a su incumplimiento, tipificado en su Régimen Disciplinario con faltas leves, graves y muy graves, en función de su naturaleza, consecuencias, reincidencia y nivel de responsabilidad del trabajador.

2. DEBER DE CONFIDENCIALIDAD Y OBLIGACIÓN DE SECRETO

NORMAS

1. Deber del profesional de no difundir la información confidencial de la que tenga conocimiento en el ejercicio de su profesión.
2. El tratamiento de la información se limitará exclusivamente al desempeño profesional y solo podrá compartirse con quienes necesiten conocerla dentro del marco de los intereses de la empresa.
3. No podrá facilitarse o difundirse aquella información que no sea de carácter público, ni tampoco usarse con fines propios, sin el permiso de la Dirección.
4. Empleados, directivos y consejeros de la EMVS deberán respetar en todo momento la confidencialidad de la información, incluyendo know-how, propiedad intelectual e industrial y otros activos intangibles propiedad de los terceros con los que la EMVS se relaciona.
5. Toda la documentación relativa a datos personales de la plantilla o de nuestros usuarios será tratada de modo reservado de acuerdo con la normativa de Protección de Datos, para asegurar su confidencialidad y se utilizará exclusivamente para la finalidad para la que hayan sido facilitados y de acuerdo con las funciones que se tengan asignadas.
6. Estos principios mantienen su vigencia, incluso después del cese del vínculo laboral con la EMVS.
7. Obligación de firma de una cláusula de confidencialidad en el ámbito laboral, donde se indiquen las condiciones de uso adecuado de la información.
8. Para proteger la información se pretende garantizar el acceso sólo a las personas autorizadas y para ello será de obligado cumplimiento no compartir las claves de acceso del equipo, salvo autorización expresa y en casos muy excepcionales.

BUENAS PRÁCTICAS

- Clasificar la información en función del nivel de confidencialidad para adoptar unas u otras medidas de seguridad.

- Usar claves de usuario y contraseñas en los documentos sensibles.
- Después de imprimir documentos de carácter CONFIDENCIAL, comprobar que no queda nada en la impresora.
- Evitar reutilizar el papel que contenga información CONFIDENCIAL, procediendo a su destrucción cuando ésta ya no sea necesaria.
- Eliminar la información antes de desechar o reutilizar un soporte para evitar la recuperación de información no autorizada
- No dejar mensajes con información sensible en contestadores automáticos.
- Si se han de mantener conversaciones confidenciales, evitar hacerlo en lugares públicos o usando canales de información inseguros.
- Bloquear el acceso al equipo informático, al abandonar el puesto de trabajo.
- Cerrar la sesión en los sistemas corporativos, cuando no se esté utilizando el ordenador o cuando se permita el uso del mismo a otra persona.

Con el objetivo de facilitar la consecución del principio de Confidencialidad se hace especial hincapié en los siguientes aspectos:

2.1. CONTROL DE ACCESO A DATOS

NORMAS

a) Limitar el acceso a los recursos de tratamiento de información y a la información en sí misma a los profesionales de la empresa que necesiten conocerla para el desempeño de su actividad principal.

b) Mantener la confidencialidad de la información.

c) Evitar guardar la información secreta en lugar no seguro.

d) No compartir claves de acceso. Cada trabajador debe acceder con sus propias credenciales de acceso personales.

e) Respetar las reglas de acceso para los diferentes roles de usuarios, con el fin de salvaguardar la confidencialidad e integridad de los datos, salvo autorización expresa y en casos muy excepcionales.

BUENAS PRÁCTICAS

- La principal barrera de seguridad en el acceso a datos es la concienciación de la necesidad de una contraseña robusta y eficaz.
- Utilizar contraseñas de 8 caracteres o más, fáciles de recordar y que mezclen mayúsculas, minúsculas, números y signos alfanuméricos.
- Si se sospecha que la contraseña ha sido comprometida, habría que cambiarla lo antes posible.
- No seleccionar "Recordar Contraseña".
- Utilizar doble factor de autenticación siempre que esté disponible.
- Utilizar una contraseña diferente para cada servicio, tanto corporativo como personal. (Usar herramientas comerciales de almacenamiento de contraseñas siempre que se necesite recordar muchas contraseñas diferentes).
- En lo relativo al uso de la información de la empresa: "todo está prohibido a no ser que se permita expresamente".

2.2. PUESTO DE TRABAJO DESPEJADO Y PANTALLA LIMPIA

NORMAS

a) Es crucial proteger la información confidencial.

b) Evitar que la información en cualquier formato, recaiga en manos no autorizadas, lo que podría dañar la imagen y reputación de la empresa.

c) Mantener bajo llave la documentación en papel con información sensible y los dispositivos móviles.

BUENAS PRÁCTICAS

- Todos los escritorios o mesas de trabajo deben permanecer limpios de documentos en papel y dispositivos de almacenamiento digitales, siempre que no estén bajo custodia durante el horario normal de trabajo y especialmente fuera del mismo.
- Ser cauto con los documentos en impresoras y faxes, o el desecho físico de documentación. Impedir el acceso no autorizado de terceros a la información.

- Al ausentarse del puesto de trabajo, aunque sea de forma efímera, no se dejará a la vista ningún documento que contenga información.
- No esperar al bloqueo automático de pantalla, bloquear al ausentarse.
- Mantener el puesto de trabajo libre de elementos que puedan derramarse y provocar daños en la documentación y en los equipos.
- Utilización de la destructora de documentos para eliminar la información impresa sensible. No es suficiente con romper y tirar las hojas a la papelera.
- Limpiar las pizarras y borrar la información de los equipos de presentación después de su uso.
- Revisar el contenido del papel previamente impreso cuando se vaya a reutilizar y evitarlo cuando contenga información confidencial.
- Al terminar la jornada laboral se debe cerrar con llave cajoneras y despachos/oficinas y asegurar que los equipos informáticos, así como cualquier otro equipamiento que esté bajo su responsabilidad, están debidamente apagados.

3. USO RESPONSABLE DE LOS RECURSOS

NORMAS

1. Uso responsable de los recursos que la empresa pone a disposición de su plantilla, directivos, consejeros y terceros autorizados.
2. Adoptar las medidas necesarias para evitar la pérdida, robo o daño de los activos de la empresa.
3. Devolver los dispositivos de la Empresa cuando no sea necesario para el desarrollo de la actividad profesional y, en todo caso, al cesar la relación laboral o profesional con la EMVS.
4. Destinar los activos de la empresa únicamente para el fin para el que le han sido entregados y abstenerse de darles cualquier otro uso. No permitir el uso de los recursos de la empresa a terceros no autorizados.
5. La empresa podrá supervisar y monitorizar los recursos suministrados para ratificar el uso responsable que la plantilla, directivos y consejeros están realizando de los mismos.
6. Queda prohibido el uso de las comunicaciones telefónicas de la empresa cuando se haga un uso de ellas destinado a los aspectos especificados a continuación:

- Beneficio personal.
- Negocios personales.
- Actividades políticas personales.
- Comportamiento antisocial o inmoral.
- Actividades que violen la legislación local, autonómica, nacional o internacional.
- Actividades recreativas.
- Divulgación no autorizada de información confidencial de la empresa.
- Actividades incompatibles con los valores propios de la Institución.

7. Queda prohibido y no se tolerará el uso de las comunicaciones telefónicas de la empresa para transmitir o distribuir material inapropiado u ofensivo, o como ofensas por motivo de raza, religión, o género.
8. Los usuarios/as de las comunicaciones telefónicas de la organización no deberán hacerse pasar por otro usuario o entidad en el transcurso de ninguna comunicación.

BUENAS PRÁCTICAS

- Evitar exposiciones a campos electromagnéticos intensos, daños físicos por descuidos, evitar comer, beber y fumar cerca de ellos. Protegerlos contra fallos de alimentación u otros fallos en las instalaciones de suministro.
- El acceso y los privilegios asociados a dicho acceso deben limitarse a lo necesario para llevar a cabo las labores correspondientes a sus tareas propias.

3.1. CORREO ELECTRÓNICO

NORMAS

Es una herramienta que aporta grandes beneficios, disponibilidad, accesibilidad, rapidez y posibilita el envío de documentos. Permite agilizar gran parte de las tareas del día a día, pero a su vez, es una de las fuentes más comunes de ciberataques e introducción de malware en cualquier empresa.

Los usuarios son responsables de las actividades realizadas con su cuenta/buzón de correo electrónico proporcionado por la empresa y deben cumplir lo siguiente:

1. La cuenta de correo electrónico que EMVS pone a disposición de su plantilla únicamente podrá ser utilizada para finalidades directamente relacionadas con el desarrollo de las funciones que les corresponden, quedando prohibido el uso de dicha cuenta para fines particulares o ajenos al objeto de su prestación laboral. La empresa podrá revisar, en caso de necesidad, los correos electrónicos, previa comunicación y autorización del trabajador y en todo caso respetando su derecho a la intimidad y la privacidad.

2. La cuenta de correo electrónico de la plantilla es un instrumento de trabajo propiedad de la EMVS y no un medio idóneo para las comunicaciones personales.
3. Por motivos de seguridad, el correo electrónico no podrá ser utilizado, de manera intencionada, para enviar ni para contestar mensajes o cadenas de mensajes susceptibles de provocar congestiones en los sistemas de EMVS o que puedan introducir malware o implicar cualesquiera riesgos o problemas en los sistemas informáticos.
4. El correo electrónico no podrá ser utilizado con fines comerciales ni lucrativos en beneficio del empleado.
5. Se cuidará en todo momento el lenguaje utilizado en sus comunicaciones, debiendo tener presente que en cada una de ellas compromete la imagen y el nombre de EMVS.
6. No utilizar la dirección de correo electrónico corporativo con fines publicitarios o para asuntos personales. Disponer de una dirección de correo alternativo donde recibir correo no deseado.
7. Queda expresamente prohibido el uso del correo electrónico corporativo para la difusión de mensajes racistas, violentos, xenófobos u ofensivos de cualquier forma.
8. Queda expresamente prohibido el uso del correo electrónico corporativo que impliquen un daño en la imagen corporativa de la compañía.
9. Queda expresamente prohibido el uso de direcciones de correo personales para el envío de información sensible.
10. Está prohibida la instalación y ejecución de software no autorizado que no sea indispensable para el correcto desempeño de las tareas asignadas en la organización, sin previa autorización.
11. Está prohibido ejecutar de forma malintencionada ningún fichero descargado desde Internet o recibido por correo electrónico u otros medios no confiables.

BUENAS PRÁCTICAS

- Antes de enviar un mensaje, revisar la dirección del destinatario.
- Para ausencias del puesto de trabajo por vacaciones, bajas, excedencias, mocosos y/o cualquier otra causa, deberá notificarse a la dirección del departamento a los fines de que su

correo electrónico sea eventualmente redireccionado a una cuenta del departamento con el fin de atender las gestiones de trabajo que al mismo se correspondan.

- Tanto el personal como en su caso el administrador de los correos, activará como acuse de recibo para los remitentes de los mensajes una comunicación en la que se indique que el destinatario del correo se encuentra ausente y en su lugar el mensaje de correo electrónico será abierto y contestado por personal de la entidad.
- Precaución con los enlaces. Evitar hacer clic en hipervínculos o enlaces de procedencia dudosa.
- Cuidar la redacción, la estructura y las faltas de ortografía del texto a enviar.
- Evitar publicar direcciones de correo de EMVS. Un mensaje dirigido a un grupo de personas fuera de la organización debería hacer uso el campo Con Copia Oculta (CCO).
- Evitar el reenvío de mensajes en cadena.
- En caso de tener que enviar información sensible por correo electrónico, ésta debe ser cifrada con contraseña
- Si sospechamos que se ha producido cualquier violación de la seguridad corporativa o que existe cualquier tipo de amenaza a través del servicio de correo electrónico, debe notificarse al departamento de Seguridad de forma inmediata a través del procedimiento de notificación de brechas de seguridad establecido FormularioSolicitudIncidencias - Nuevo formulario (emv.es)
- Aplicar la regla “desconfianza por defecto”. Ante una sospecha, contactar por cualesquiera medios alternativos con el remitente. Si persiste la duda, informar al administrador de seguridad de EMVS.
- Redactar mensajes desde cero, sin reutilizar mensajes previamente enviados.
- Desconfiar de correos con patrones fuera de lo común: mal estructurados, mal redactados o con faltas de ortografía. Ante este tipo de mensajes, desconfiar incluso si incluyen información personal y contactar con el administrador de seguridad de EMVS.
- No confiar únicamente en el nombre del remitente. Comprobar que el propio domino de correo de origen es de confianza.
- Asegurarse de la extensión del fichero adjunto que desea descargar del correo electrónico. No abrir ficheros ejecutables con extensiones del tipo .EXE, .COM, .BAT, etc. Se debe desconfiar de los adjuntos que incluyen múltiples espacios justo antes de la verdadera extensión.

- En general, desconfiar de ficheros adjuntos no esperados. Uno de los recursos más utilizados para engañar al usuario es asignar al fichero adjunto esperado un icono representativo de determinado software conocido o incluir datos personales en el texto del mensaje.
- No habilitar las macros independientemente de lo que solicite el documento (de hecho, ese puede considerarse un indicador de sospecha).
- Evitar utilizar cuentas de correo online gratuitas para el envío y recepción de información corporativa de EMVS.
- No incluir en el texto del mensaje datos personales, datos protegidos, datos bancarios ni claves. Transmitir esa información por otros medios más seguros.
- No utilizar Outlook para configurar otras conexiones de correo electrónico (Gmail, etc.) diferentes a la conexión a los servidores de correo de EMVS.
- No utilizar almacenamiento en la nube tipo Dropbox, WeTransfer, OneDrive, etc para enviar información. Para enviar ficheros de gran tamaño, solicitar al departamento de informática la transmisión a través de la aplicación ALMACEN de AAPP.

3.2. DISPOSITIVOS MÓVILES

NORMAS

1. La utilización de dispositivos móviles (portátiles, unidades (USB), teléfonos móviles, y tablets) se restringirá al ámbito laboral y profesional.
2. La empresa facilitará los dispositivos con el objetivo de mantener la productividad y eficiencia, para ello se impone la necesidad de sincronizar los archivos y producir copias de seguridad que permitan su uso seguro.
3. Realizar copias de seguridad periódicas, preferiblemente automáticas, de todos los contenidos del dispositivo que se desea proteger y consérvelas a través de la herramienta de backup del fabricante del dispositivo.
4. Utilizar una red privada virtual VPN para proteger todo el tráfico de datos desde el dispositivo hasta la infraestructura de EMVS.

5. Mantenerse alerta frente a ataques a dispositivos, en especial los del tipo SMS (SMiShing), ignorando los que o invitan a hacer un clic en un enlace, o informan de un premio obtenido, o solicitan introducir credenciales bancarias.
6. Tener instalado y actualizado un antivirus gratuito especialmente en dispositivos Android

BUENAS PRÁCTICAS

- Proteger el dispositivo mediante un código de acceso de 6 a 8 dígitos, asociado a la pantalla de bloqueo. No utilizar códigos de acceso de 4 dígitos, ni números iguales, consecutivos o combinaciones fácilmente deducibles.

- Minimizar la funcionalidad disponible en la pantalla de bloqueo si no se introduce el código de acceso.

- Deshabilitar todos los servicios y funcionalidades del dispositivo que no se vayan a utilizar de forma permanente.
- Restringir al máximo los servicios de geolocalización por parte de las apps instaladas en el dispositivo.
- Disminuir el consumo de datos limitando la funcionalidad de las apps cuando ésta no sea absolutamente necesaria.
- Separar todo lo posible las comunicaciones personales de las profesionales.
- Utilizar en lo posible el desbloqueo con huella dactilar o reconocimiento facial.
- Debido a que muchos dispositivos añaden las coordenadas GPS en la información de las imágenes tomadas, limitar la compartición de las imágenes en la red o utilizar aplicaciones que eliminen dicha información.
- Familiarizarse con las capacidades de gestión remota del dispositivo y comprobar el correcto funcionamiento de este servicio y de toda su funcionalidad. Complementariamente, la funcionalidad “Buscar mi iPhone” (en iPad/iPhone) y “Device Manager” (en Android) deberían estar habilitadas y correctamente configuradas.
- Con el objetivo de mejorar la protección frente a un acceso físico no autorizado al dispositivo, reducir el impacto frente a la pérdida o robo, mejorar la confidencialidad y seguridad del almacenamiento y proteger las comunicaciones con otros equipos y servicios se recomienda:

- Configurar el bloqueo automático del dispositivo de forma inmediata si no hay actividad por parte del usuario.
- Activar el acceso mediante PIN a las conexiones Bluetooth y configurar el dispositivo en modo oculto. No aceptar conexiones de dispositivos desconocidos.
- No conectar el dispositivo ni aceptar ninguna relación de confianza por USB sin constancia de que sea un ordenador de confianza.
- Mantener el sistema operativo actualizado y disponer de la última actualización de todas las apps corporativas instaladas en el dispositivo.
- Hacer uso de las capacidades de cifrado para proteger las unidades internas y externas de almacenamiento. No guardar ninguna información sensible en unidades extraíbles.
- Tener cuidado con las solicitudes de permisos de las aplicaciones que se ejecuten en el teléfono.
- Descargar aplicaciones únicamente desde las tiendas oficiales. Evitar las descargas de software de sitios poco fiables. Solicitar al responsable las aplicaciones necesarias.

3.3. NAVEGACION SEGURA

NORMAS

Las pautas de actuación para prevenir las posibles incidencias respecto a la confidencialidad, disponibilidad, trazabilidad, autenticidad e integridad de la información serán:

1. Se debe descargar programas exclusivamente desde sitios oficiales. Queda prohibido cualquier tipo de piratería o uso de descargas peer-to-peer.

BUENAS PRÁCTICAS

- Acceder únicamente a sitios web de confianza.
- Mantener actualizado el navegador a la última versión disponible del fabricante.
- Hacer uso de los niveles de seguridad del navegador.
- Configurar el navegador para bloquear ventanas emergentes.

- Borrar las “cookies”, los ficheros temporales y el historial cuando utilice equipos ajenos para no dejar rastro de la navegación.
- Desactivar la posibilidad “script” en navegadores web como Firefox (NoScript) o Chrome (NotScript), para prevenir la ejecución de los mismos por parte de dominios desconocidos.
- Usar HTTPS (SSL/TLS) frente a HTTP incluso para aquellos servicios que no manejen información sensible. Funcionalidades como HSTS y extensiones como HTTPS Everywhere servirán de gran ayuda para garantizar la seguridad durante la navegación web.
- Se recomienda utiliza un usuario sin permisos de administración para navegar por internet al objeto de impedir la instalación de programas y cambios en los valores del sistema.

4. ARCHIVO DE DATOS

NORMAS

Garantizar la accesibilidad a la información de la Empresa.

1. Se deben archivar los datos en lugares (físicos y lógicos) con acceso restringido (contraseña o llave) a las personas no autorizadas.

2. Solo deben de tener acceso a los datos personales las personas estén autorizados para la realización de su trabajo y siempre respetando los fines del tratamiento.

3. No se deben sacar de la EMVS datos personales en ningún formato, salvo autorización de la Dirección. En el caso de ser necesario, y previa autorización, hay que extremar la seguridad y su custodia. Los datos deben volver a la EMVS lo antes posible.

4. Los datos personales se conservarán hasta que concluya la finalidad del tratamiento y, en todo caso, hasta que haya prescrito los plazos para interponer cualquier acción civil, penal o administrativa relacionada con el tratamiento.

5. Existe un Registro de Actividades de Tratamiento, en el que se establecen los plazos previstos para la supresión de las diferentes categorías de datos. Todas las Direcciones y Departamentos de la Empresa deberán cumplir los plazos marcados y proceder periódicamente a la revisión de expedientes (tanto digitales como en papel), para la eliminación o bloqueo de los datos personales que ya no sean necesarios para la finalidad para la que fueron recabados.

6. Sin perjuicio de lo anterior y según indica el Art 89 del RGPD existen Garantías y Excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Se regirán por su propia ley y lo indicado en el Reglamento.

7. Si se trabaja con ficheros de datos almacenados en su disco duro, éstos deben subirse a la Intranet de EMVS a la mayor brevedad posible. Queda prohibido trabajar indefinidamente con ficheros o datos corporativos en discos duros de portátiles, PCs o

llaves USB. Los ficheros corporativos, especialmente con datos sensibles, deben almacenarse en la intranet para su correcta protección.

8. Será necesaria la autorización de la Dirección correspondiente en caso de necesidad de intercambiar datos personales con terceros con dispositivos portátiles.

BUENAS PRÁCTICAS

- Tratar los documentos respetando el procedimiento establecido por el Área de Archivo.
- No utilizar el escritorio ni el disco duro del ordenador para guardar documentos de trabajo. Archivarlos siempre en la intranet corporativa.
- Realizar copias de seguridad para evitar pérdidas de información.
- Almacenamiento Local: Con el fin de garantizar el almacenamiento de la información en los sistemas, se aconseja no usar dispositivos de almacenamiento local, entre otras, por las siguientes razones:
    - Por su mayor vulnerabilidad a ataques o pérdida de datos
    - Por el carácter limitado de su ciclo de vida
    - Porque no se realizan copias de seguridad
    - Porque recuperar datos resulta imposible
- Por todo ello, se recomienda guardar los datos en la arquitectura dispuesta por la EMVS (de red o proveedores externos), ya que, además de garantizar la disponibilidad de la información ubicada en estos sistemas de almacenamiento, se aplican políticas de copia de seguridad programadas, lo que posibilita su recuperación en caso de pérdida de los datos o fallo del sistema.
- Almacenamiento portátil: Se debe tener especial precaución con el almacenamiento en dispositivos portátiles (discos duros portátiles, memorias flash, cds, dvds...etc), dado que su movilidad y conectividad aumentan la vulnerabilidad de la información que contienen (entre otros, facilitan la salida de datos de la organización; debido a su tamaño se pueden extraviar con facilidad y son potencial fuente de divulgación de virus).
- No se debe dejar nunca desatendido este tipo de dispositivos, no se debe almacenar en ellos datos de accesos y se debe cifrar la información cuando ésta sea confidencial o relativa a datos de carácter personal.
- Recomendable emplear métodos de autenticación siempre que sea posible.

5. TELETRABAJO

NORMAS

EMVS ha instaurado la posibilidad del teletrabajo, como una forma de trabajo a distancia en la cual el trabajador desempeña su actividad sin necesidad de presentarse físicamente en la empresa o lugar de trabajo específico. No obstante, han de seguirse unas pautas de actuación con objeto de prevenir las posibles incidencias en lo que a la confidencialidad, disponibilidad, trazabilidad, autenticidad e integridad de la información que contienen se refiere.

Según el Centro Criptológico Nacional, el teletrabajo obliga a extremar las precauciones para evitar incidentes de seguridad. Las amenazas de seguridad informática se multiplican por diez durante una sesión de teletrabajo, por ello es necesario cumplir las siguientes pautas:

1. Utilizar ordenadores propios, de confianza o corporativos para iniciar una sesión de teletrabajo.
2. Usar aplicaciones aprobadas por EMVS durante una sesión de teletrabajo, que en su caso son Teams para reuniones virtuales, FlexIP como teléfono software y OWA/Outlook for Mobile como cliente de correo electrónico.
3. A través de la aplicación correspondiente, y mientras dure la conexión al servicio de acceso remoto, se utilizarán indicadores de productividad vinculados al identificador de la personal usaría autentificada. En todo caso se respetará el derecho a la intimidad, privacidad e inviolabilidad de las comunicaciones del personal vinculado al identificador de la persona usuaria autentificada para su posible análisis en caso de necesidad. En todo caso se respetará el derecho a la intimidad, privacidad e inviolabilidad de las comunicaciones del personal.
4. En caso de que se produzca un mal funcionamiento en el equipo informático o en las aplicaciones instaladas en él, así como en el servidor o plataformas que permitan el teletrabajo, deberá comunicarse sin dilación al departamento de informática.
5. El servicio informático de la EMVS podrá revisar las condiciones del equipo empleado, previa comunicación, y siempre que con carácter previo el/la trabajador/a hubiese autorizado expresamente el acceso a sus equipos informáticos.

BUENAS PRÁCTICAS:

- Utilizar preferiblemente una conexión cableada a su router WIFI frente a una conexión inalámbrica.
- Teclear la dirección de acceso al teletrabajo, https://portal.emvs.es, o bien seleccionarla de la lista de Favoritos, evitando la búsqueda en Google con objeto de evitar ataques de phishing.
- No seleccionar "Recordar Contraseña".
- Utilizar conexiones 4G/5G si la sesión de teletrabajo debe realizarse desde dependencias ajenas a EMVS, especialmente en hoteles, aeropuertos, oficinas, etc. y siempre que disponga de gigabytes suficientes.
- Disponer de un sistema antivirus actualizado en el PC antes de iniciar una sesión de teletrabajo.
- Evitar que personal ajeno a EMVS pueda espiar y obtener información de la conexión o de la información que se transmite desde lugares públicos.
- Evitar la transmisión de videos durante una sesión de teletrabajo.
- Evitar almacenar información de EMVS en el equipo que inicia la sesión de teletrabajo.

6. INCIDENCIAS DE SEGURIDAD DE LA INFORMACIÓN

NORMAS

1- Evitar o minimizar los riesgos de destrucción, pérdida, alteración, comunicación o acceso no autorizado en información de la empresa y notificación de incidencias.

2. Comunicación inmediata a través de la herramienta de incidencias informáticas mediante el PROCEDIMIENTO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD en caso de:

a) Pérdida, robo, o localización insegura, de documentación o correspondencia confidencial.

b) Envío por error de datos personales, tanto de forma electrónica como en papel.

c) Accesos, modificación o eliminación de datos no autorizada.

d) Sospecha de malware, phishing o cualquier incidencia informática.

e) Eliminación incorrecta de datos personales en papel o en soportes electrónicos obsoletos.

7. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EJERCICIO DE DERECHOS

NORMAS

Respecto a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales se procederá conforme a lo establecido en PROCEDIMIENTO PARA LA ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.