Objeto

EMASESA establece unas **normas de uso** para sus recursos informáticos y de telecomunicaciones (ordenadores, aplicaciones, dispositivos móviles, Internet, etc.), así como en el acceso y utilización de datos e información de la organización, con independencia del tipo de soporte utilizado (informático, papel o cualquier otro). **Estas normas se establecen para proteger a la compañía y sus partes interesadas** (usuarios, accionistas, personas de la organización, colaboradores, proveedores y sociedad en general) de los riesgos que podrían ocasionar un uso inadecuado, accidental o malintencionado, de la información y de los sistemas electrónicos que la recogen, procesan, almacenan y trasmiten. Entre otros objetivos, se persigue:

- **Salvaguardar la información** que EMASESA genera en la ejecución de sus funciones, y aquella que le es entregada en custodia por cualquiera de sus partes interesadas.
- **Garantizar el uso responsable y la disponibilidad de los recursos tecnológicos** de la compañía (redes de telecomunicaciones, sistemas de información, equipos ofimáticos, etc.).
- **Asegurar el cumplimiento de las obligaciones legales**, regulatorias o contractuales vigentes en materia de protección de datos, seguridad de la información y ciberseguridad.
- **Proteger el prestigio y el buen nombre de EMASESA y sus empleados**.

EMASESA
metropolitana

NURTI

Normas de Uso de los Recursos Tecnológicos y de Información*

*Este documento es un extracto del documento completa "Normas de Uso de los Recursos Tecnológicos y de Información" (GE.010.04) disponible en la intranet corporativa de EMASESA.

Propiedad de los activos de información

EMASESA facilita a los usuarios los recursos necesarios (información, servicios, aplicaciones, ordenador fijo o portátil, red de comunicaciones, teléfono móvil, tabletas, memorias USB, etc.) para la realización de las tareas relacionadas con su puesto de trabajo o actividad prestada en la compañía.

Dichos recursos son propiedad de EMASESA y, con carácter general, deben utilizarse para fines profesionales.

No obstante, EMASESA tolera un cierto uso personal de internet, del correo electrónico, de las llamadas mediante telefonía fija o móvil, y de las aplicaciones móviles de mensajería instantánea autorizadas en la compañía, siempre y cuando éste se realice de buena fe y de forma comedida, no sea excesivo ni en el tiempo dedicado ni en el consumo de recursos (coste económico, ancho de banda, etc.), se atenga a lo dispuesto en ésta norma, y no suponga alteración alguna de as medidas y directrices de seguridad establecidas por la compañía.

Esta prestación no supone en modo alguno un derecho para el usuario ni una obligación para EMASESA, teniendo ésta última la potestad exclusiva de determinar cuándo se produce un incumplimiento de cualquiera de los preceptos antedichos. Para ello, el usuario es conocedor de que se adoptan medidas de supervisión y control. El usuario es el único responsable de los daños, de cualquier índole (materiales, económicos, legales, etc.), accidentales o voluntarios, que pudieran producirse como consecuencia del uso personal de estos recursos, ya sea sobre sus propios intereses o los de EMASESA.

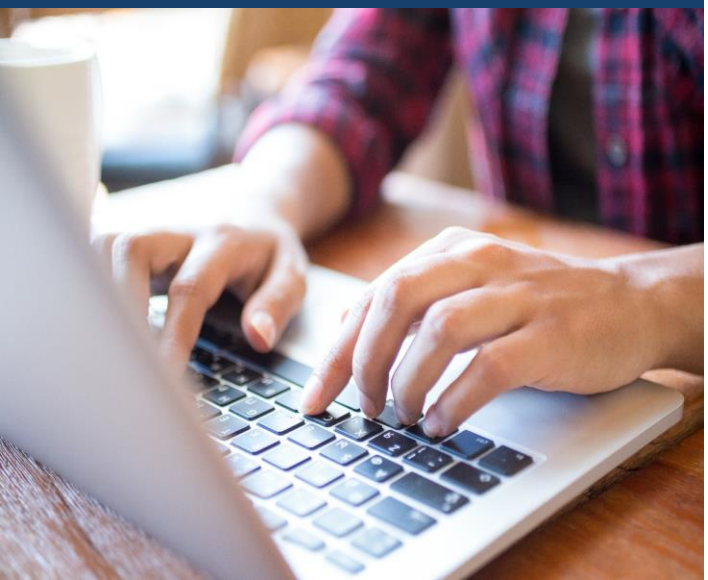
La información de trabajo alojada en los sistemas de almacenamiento de EMASESA y en su equipamiento informático de cualquier índole (teléfono móvil, tableta, memoria USB, etc.), así como aquella que se envía a través de su red de telecomunicaciones, es propiedad de EMASESA.

Queda prohibido cualquier uso comercial y/o privado, contrario a estas normas, de los recursos informáticos, telemáticos y de información de EMASESA.

Uso de ordenadores

No está permitido:

- Alterar la configuración física de los equipos ni conectar otros dispositivos a iniciativa del usuario, así como variar su ubicación, a excepción de los ordenadores portátiles autorizados.
- Alterar la configuración software de los equipos, desinstalar o instalar programas o cualquier otro tipo de software distinto a la configuración lógica predefinida, tarea que queda reservada al personal del área TIC.
- Conectar ordenadores no autorizados (fijos o portátiles) a la red corporativa.



- Se evitará especialmente almacenar archivos y documentos de trabajo en el ordenador asignado, dado que de estos equipos no se realizan copias de seguridad. En su lugar se utilizarán los sistemas de información corporativos (AquaWS, SAP, etc.) o, en su defecto, se guardarán los archivos en las unidades de red disponibles a estos efectos (carpetas compartidas).
- No está permitida la creación de carpetas compartidas, ni el cifrado de información, en los ordenadores de trabajo asignados, salvo autorización expresa.
- Está prohibido utilizar, copiar o transmitir información propiedad de EMASESA para uso privado o cualquier otro fin distinto del servicio al que está destinada.

En ningún caso se podrá acceder a los recursos informáticos y telemáticos con las siguientes finalidades:

- Difundir contenidos contrarios a los principios y valores de EMASESA.
- Usar la red u ordenadores de EMASESA para conseguir acceso no autorizado a cualquier ordenador o recurso de la compañía.
- Incurrir en actividades ilícitas o ilegales de cualquier tipo y, particularmente difundir contenidos o propaganda de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo o atentatorio contra los derechos humanos, o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.

- Introducir o difundir en la red o en los sistemas informáticos, de forma voluntaria, virus informáticos o cualquier otro mecanismo o artefacto físico o lógico susceptible de dañar los sistemas físicos y/o lógicos de EMASESA, de sus proveedores o de terceras partes.
- Realizar, con conocimiento de causa, cualquier acto que interfiera en el correcto funcionamiento de los ordenadores, terminales, periféricos, red de comunicaciones, o cualquier otro componente de los Sistemas de Información de EMASESA.
- Ejecutar cualquier tipo de acción que trate de descubrir información distinta de la del propio usuario.
- Intentar evitar los mecanismos de protección de los datos o los sistemas de seguridad.
- Violar la privacidad de los datos y el trabajo de otros usuarios.

Uso de aplicaciones

- No se instalarán, ejecutarán o descargarán aplicaciones o programas informáticos en el ordenador de trabajo. Se incluyen las aplicaciones conocidas como portables o de cualquier otro tipo, aunque no requieran instalación. Cualquier aplicación que se requiera para la actividad laboral, deberá ser solicitada siguiendo el procedimiento establecido, para su aprobación e instalación por el personal del Área TIC.
- No se introducirán de forma voluntaria programas que causen, o sean susceptibles de causar, cualquier tipo de alteración en los sistemas informáticos y telemáticos de EMASESA o de terceros.

- No se borrará o eliminará ninguno de los programas instalados por el personal de Área TIC.
- No se desactivarán los programas antivirus y/o sus actualizaciones, ni ninguna otra aplicación de seguridad.
- No se realizarán copias ilegales de los programas utilizados por EMASESA.

Uso de ficheros informáticos

- No está permitido el uso, almacenamiento, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o documento sin licencia y/o protegida por la propiedad intelectual o industrial.
- No está permitida la apropiación de archivos o ficheros titularidad de EMASESA para uso particular y/o de terceros no autorizados.
- No se permite la copia, total o parcial, de ficheros que contengan datos de carácter personal u otro tipo de información sensible de EMASESA en el ordenador de trabajo, memorias USB o cualquier otro tipo de soporte de información, incluidos servicios de almacenamiento, transferencia o manipulación de documentos en la nube (internet), que no haya sido debidamente autorizado en razón del puesto ocupado por el usuario.

Uso de contraseñas

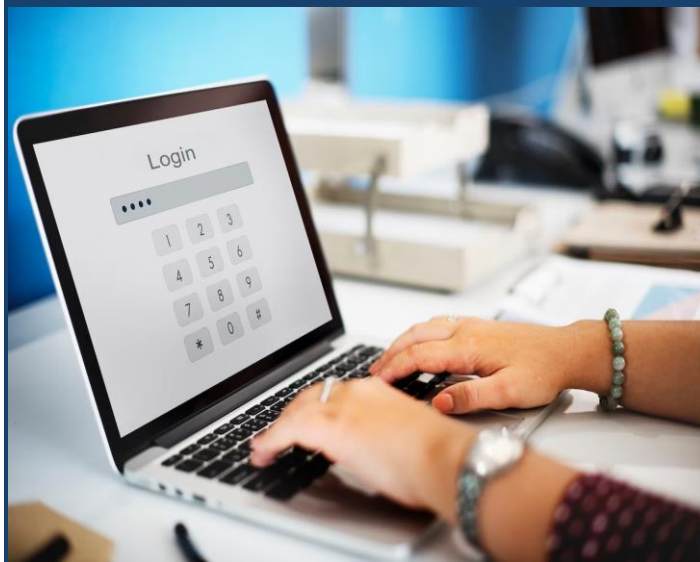
- Las contraseñas de acceso al equipo, sistemas de información y/o a la red son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida.

No está permitido:

- Obtener la contraseña de acceso de una cuenta de otro usuario.
- Usar identificadores y contraseñas de otros usuarios para acceder al sistema y a la red corporativa, salvo que por circunstancias excepcionales (vacaciones, ausencias, bajas, investigación de incidentes, etc.) así se determine, y previo conocimiento y autorización por parte del Responsable de Seguridad de la Información.
- Intentar modificar o acceder al registro de accesos de los equipos informáticos y sistemas de información.
- Intentar evitar las medidas de autenticación establecidas en los equipos informáticos y sistemas de información.

- En caso de que fuera necesario acceder al sistema en ausencia de un compañero, se solicitará autorización al Responsable de Seguridad de la Información para que se habilite un acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al Responsable de Seguridad de la Información para la revocación del acceso.
- Las contraseñas no deben anotarse, deben recordarse, o bien archivarse mediante un gestor de claves. Además, deben cumplir los requisitos establecidos en la normativa interna de EMASESA. En particular, deberán ser suficientemente complejas y modificarse periódicamente.
- Cuando se considere que la identificación de acceso ha podido verse comprometida se deberá comunicar al CAU con la mayor diligencia.

- Al abandonar temporalmente el puesto de trabajo, deben bloquearse las sesiones manualmente. Al finalizar la jornada laboral se deben apagar los equipos, salvo que el equipo tenga que permanecer encendido por causa justificada (por ejemplo, equipos de para mantenimiento remoto utilizados por personal de TIC). Todas las aplicaciones y sistemas que requieran de acceso mediante usuario y contraseña, contarán con un mecanismo para cierre automático de la sesión del usuario tras un período de inactividad.



Uso de la red corporativa

La red corporativa es un recurso compartido y limitado. Sirve para el acceso de los usuarios a los sistemas de información (AquaWS, SAP, etc.) y demás aplicaciones informáticas corporativas, y también para la comunicación de datos entre sistemas, internos o externos.

Para garantizar la integridad y el buen funcionamiento de la red, los usuarios deben cumplir las siguientes directrices de seguridad:

- Está prohibido realizar cualquier tipo de acción intencionada que degrade la calidad de servicio y el buen funcionamiento de la red de telecomunicaciones de EMASESA, así como aquellas que pongan en peligro el trabajo de otros usuarios, o permitan acceder a su información sin autorización específica.

- La utilización de Internet está destinada, prioritariamente, a la obtención de información relacionada con el trabajo desempeñado en EMASESA en virtud del puesto ocupado, en el caso de personal interno, o de la actividad asignada, en el caso de terceros, en los términos que se recogen en el apartado "Propiedad de los activos de información".

En relación con el uso de Internet no están permitidas las siguientes actividades:

- La compartición de contenidos no vinculados a las funciones del puesto de trabajo, en el caso de personal interno, o actividad prestada en la organización, en el caso de terceros (descarga de archivos de música, vídeo, etc.).

- La transmisión o recepción de material protegido por la Ley de Protección Intelectual.

- La transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

- La transferencia a terceras partes de material de EMASESA sin la debida autorización.

- La transmisión o recepción sin autorización de ficheros sujetos al cumplimiento de las leyes y regulaciones en materia de Protección de Datos de Carácter Personal.

- La transmisión o recepción de cualquier tipo de dato e información no relacionados con la actividad de EMASESA.

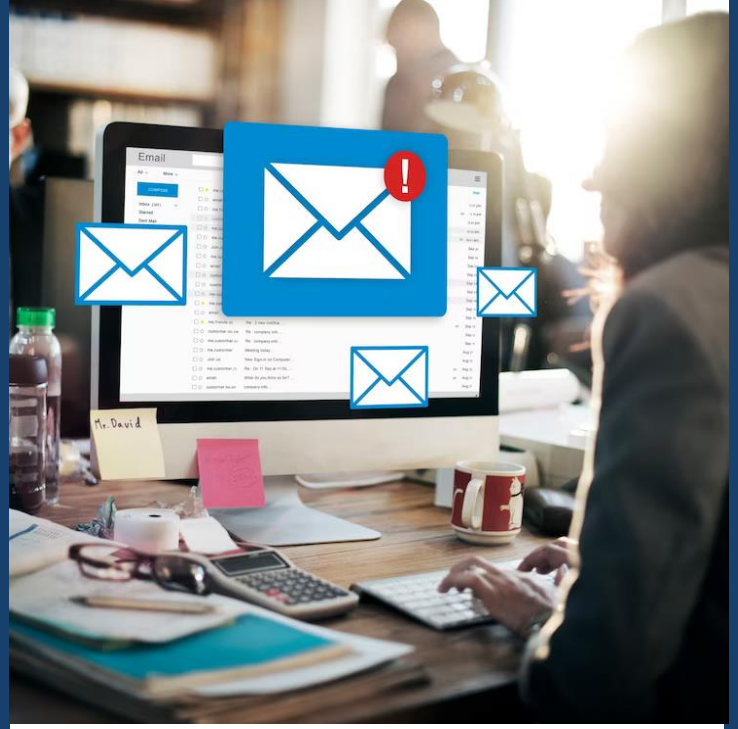
- La participación en actividades de Internet como grupos de noticias, juegos, visionado de televisión, u otras que no estén directamente relacionadas con la actividad de EMASESA.

- La realización de actividades que puedan dañar la buena reputación de EMASESA.

Uso del correo electrónico corporativo

El correo electrónico es un instrumento básico de trabajo, pero también un vector preferente de los cibercriminales para atacar a una organización. Por ello es necesario ser especialmente diligente en su uso de forma adecuada y segura, para lo cual se seguirán las siguientes directrices:

- El correo electrónico corporativo está destinado, prioritariamente, a su uso profesional, en los términos que se recogen en el apartado "Propiedad de los activos de información".
- No está permitido el uso de la dirección de correo electrónico corporativo como dato de contacto para el alta de servicios que no estén directamente vinculados con la actividad laboral (comercios, redes sociales, etc.).
- Se evitará el envío de correos con ficheros adjuntos de gran tamaño (mayores de 10 Mb), utilizándose alternativamente el sistema de transferencia de archivos corporativo de EMASESA.
- No se debe acceder a los enlaces, ni abrir los ficheros incluidos como adjuntos en los correos electrónicos que resulten sospechosos o de los que no se conozca su procedencia.



- Los correos que se destinen a un gran número de usuarios, internos o externos, se realizarán sólo en los casos autorizados en función de las necesidades del puesto (por ejemplo, personal de Marketing, avisos de seguridad, etc.) y serán solo los estrictamente necesarios para no provocar un colapso del sistema de correo, de acuerdo a las indicaciones del personal del área TIC.
- Sólo podrá enviar correos con fines publicitarios el personal autorizado para ello en función de su puesto en la organización y, en este caso, siempre que se cuente con el consentimiento del destinatario y se garantice el cumplimiento de las regulaciones en materia de privacidad y protección de datos de carácter personal.

No está permitido:

- La compartición de contenidos no vinculados a las funciones del puesto de trabajo, en el caso de personal interno, o actividad prestada en la organización, en el caso de terceros (descarga de archivos de música, vídeo, etc.).
- La transmisión o recepción de material protegido por la Ley de Protección Intelectual.
- La transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- La transferencia a terceras partes, o a una dirección de correo personal externa, de material de EMASESA sin la debida autorización.
- La transmisión o recepción sin autorización de ficheros sujetos al cumplimiento de las leyes y regulaciones en materia de Protección de Datos de Carácter Personal.
- La transmisión o recepción de cualquier tipo de dato e información no relacionados con la actividad de EMASESA.

Uso de memorias USB

- Sólo está permitido la utilización de memorias USB corporativas suministradas por EMASESA según el procedimiento establecido. Por tanto, no se permite la conexión a los ordenadores corporativos de ninguna memoria USB que haya sido proporcionada por un tercero, salvo que haya sido expresamente revisada y autorizada por el Responsable de Seguridad de la Información.
- El dispositivo es propiedad de EMASESA y se entrega en calidad de préstamo. Sólo se utilizará para uso profesional y se devolverá a la finalidad del préstamo, o antes si EMASESA así lo requiere.
- No se alterará ni eliminará la función de acceso por contraseña y cifrado de información que incluye el dispositivo.
- No se prestará el dispositivo a terceros y se mantendrá en todo momento bajo vigilancia y custodia.

• El Usuario se asegurará, en la medida de lo posible, de que el equipo al que se conecta la memoria USB dispone de antivirus actualizado y operativo.

• El Usuario se responsabilizará de realizar copia de seguridad de los archivos almacenados en el dispositivo.

Uso de carpetas compartidas

La documentación de trabajo debe estar almacenada preferentemente en los Sistemas de Información correspondientes (AquaWS, SAP, etc.) o en su defecto, en las carpetas compartidas dispuestas por EMASESA a este efecto.

Estos sistemas cuentan con suficientes garantías de seguridad, como sistemas de respaldo y copias de seguridad.

Los ordenadores asignados a los usuarios no disponen de estas medidas, por lo que no debe almacenarse en éstos información corporativa.

Se deberán cumplir las siguientes directrices:

- No está permitido el uso de las carpetas compartidas para el almacenamiento de información privada, ajena al objeto del puesto de trabajo del usuario.
- No está permitido el acceso a la documentación almacenada en carpetas compartidas a las que no se haya sido expresamente autorizado en función de las necesidades del puesto, incluso aunque el intento de acceso no fuera bloqueado por los mecanismos de seguridad implementados. En caso de detectarse esta situación se comunicará al CAU para la subsanación del error en la asignación de los permisos de acceso.
- Se eliminará de las carpetas compartidas toda información que por su obsolescencia o cualquier otra causa haya dejado de ser relevante o útil para la compañía.
- No se almacenarán documentos que contengan datos de carácter personal y que no hayan sido expresamente autorizados.

Almacenamiento en la nube

El uso de servicios en internet (nube pública) para el almacenamiento, transferencia o tratamiento de documentos y archivos expone a terceros información propiedad de EMASESA y conlleva riesgos adicionales para la seguridad de la información. Por ello se establecen las siguientes directrices respecto a su uso:

- No está permitido el almacenamiento de información de EMASESA en servicios en la nube pública (Dropbox, Google Drive, etc.). Alternativamente, los usuarios autorizados podrán hacer uso del servicio en la nube privada de EMASESA o del MS365 corporativo.
- No está permitido el uso de servicios en internet para tratamiento de documentos o archivos (edición de imágenes, edición de vídeos, edición de documentos, etc.). Alternativamente se solicitarán y utilizarán las aplicaciones o programas informáticos disponibles en el Catálogo Corporativo de Aplicaciones.

Acceso remoto

En el caso de usuarios autorizados a acceder desde ubicaciones remotas serán de aplicación con carácter general todas las directrices recogidas en el presente documento, además de las siguientes específicas:

- El usuario accederá exclusivamente a los recursos autorizados y durante el periodo de tiempo permitido.
- El usuario dispondrá de sus correspondientes credenciales de acceso, cuyo uso cumplirá lo previsto en el apartado "Uso de contraseñas".
- En ningún caso se dejará el equipo remoto desatendido y con la sesión abierta.
- El usuario se asegurará de que el equipo remoto disponga de un antivirus activo y con la base de datos de firmas de virus más reciente, tenga el sistema operativo debidamente actualizado y con los parches de seguridad aplicados, y no exista sospecha o síntoma alguno de que pueda estar comprometido. EMASESA podrá establecer mecanismos de seguridad que verifiquen automáticamente estas políticas e impidan el acceso a la red corporativa en caso de detectar algún incumplimiento.

- No está permitido el acceso remoto a los sistemas de información de EMASESA, mediante VPN (Virtual Private Network) e Internet de forma concurrente ("Dual Homing" o "Split Tunnelling.
- En caso de que el equipo remoto no sea propiedad de EMASESA, el usuario será responsable de instalar el cliente de conexión, y establecer la configuración necesaria, por sus propios medios y de acuerdo al manual de usuario proporcionado por EMASESA, que no tendrá obligación alguna de prestar soporte técnico al tratarse de un equipo ajeno.

Uso de redes sociales

- Con carácter general sólo se podrá publicar información relativa al cargo ocupado en la organización y duración en el mismo, no así otra información como datos de contacto (teléfono y/o dirección de correo electrónico corporativo, etc.) o de cualquier otra índole, y en todo caso exclusivamente en redes sociales de tipo profesional (como Linkedin o Xing), pero no en aquellas otras de corte generalista y/o de ocio (como Facebook, Tuenti o Twitter, entre otras).
- Se deberá asegurar que la información publicada es veraz y que se encuentra debidamente actualizada.
- Sólo podrán publicar información en términos distintos a los anteriores y en otro tipo de redes sociales aquellas personas expresamente autorizadas en razón de su actividad en la organización (Personal del área de Marketing u otro autorizado).
- Se adoptará en todo momento un uso del lenguaje adecuado y acorde con la cultura organizacional y valores de EMASESA. Queda terminantemente prohibido utilizar términos o expresiones que puedan resultar ofensivos, discriminatorios, sexistas o inapropiados en general, así como el uso del lenguaje vulgar o soez.

Grabación de imágenes

- No se permite la grabación de imágenes de ningún tipo (video o fotografía) en las instalaciones de EMASESA salvo que hayan sido expresamente autorizadas por el Responsable del Centro correspondiente. En caso de tratarse de grabaciones en Áreas restringidas (CPD, Centros de Control, Instalaciones industriales), será además necesario requerir la autorización del Responsable de Seguridad Física.
- En caso de que en las imágenes aparezcan personas que puedan ser identificables, deberá solicitarse su autorización expresa por escrito en cumplimiento de la legislación en materia de protección de datos de carácter personal.

Monitorización y supervisión

Con la finalidad de verificar el cumplimiento de esta norma, y para la gestión de incidentes de seguridad, EMASESA dispone de herramientas que monitorizan y registran la actividad en sus sistemas de información, redes de telecomunicaciones y equipamiento ofimático. Estas herramientas generan alertas automáticas cuando se detecta cualquier actividad inusual que pueda comprometer la información de EMASESA o la de los sistemas donde se almacena, procesa o transmite. También se generan informes estadísticos de uso de dichos recursos.

En particular se tienen implementadas las siguientes medidas de control:

- Internet; registro de las páginas visitadas (URL y dirección IP) con identificación del usuario, equipo origen, fecha, hora y duración del acceso, tipología de la web, nombre y tamaño de los ficheros enviados o recibidos, y detección automática de patrones de datos de carácter personal o información sensible.

- Correo electrónico; registro de la dirección del remitente, destinatario y asunto del correo (excluyendo el cuerpo del correo) junto con fecha y hora de recepción o envío.

- Llamadas telefónicas; identificación del número llamante, llamado, fecha, hora y duración de la llamada.

En caso necesario es posible, mediante un análisis específico por parte de personal autorizado, identificar al usuario concreto que ha llevado a cabo una determinada acción, así como obtener un mayor nivel de detalle sobre la misma. En todo caso, esta identificación se realiza siempre salvaguardando el derecho al honor y a la intimidad de los interesados, y de acuerdo con la normativa sobre protección de datos personales y demás disposiciones aplicables, con el objeto de subsanar actuaciones contrarias a esta norma o para la gestión de un incidente de seguridad.

Durante el transcurso de un incidente de seguridad, el personal autorizado, a indicación del Responsable de Seguridad de la Información, podrá acceder, local o remotamente, y en todo momento, a cualquier ordenador y/o recurso ofimático o telemático propiedad de EMASESA (móvil, dispositivo USB, etc.) que puedan estar implicados en el incidente, con el fin de detectar y eliminar su origen, o para establecer medidas de contención que impidan su propagación al resto de la compañía.

Acceso y tratamiento de datos de carácter personal (ficheros informáticos)

El usuario que acceda y trate información de carácter personal en el desempeño de sus funciones y tareas (RGPD y LOPDGDD), deberá guardar el necesario secreto respecto a ésta, incluso una vez concluida su relación con EMASESA. A este efecto, tienen consideración de datos de carácter personal cualquier tipo de información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, relativa a un aspecto/s físico, psíquico, fisiológica, cultural, social o económico de la persona, susceptible de recogida, registro, tratamiento o transmisión, concerniente a una persona física identificada o identificable.

En particular, respecto a la información de carácter personal contenida en ficheros informáticos, deberá cumplir, en consonancia con lo expuesto en anteriores apartados, las siguientes directrices:

- Los ficheros con datos de carácter personal empleados se almacenarán en los sistemas de información o carpetas compartidas habilitados por EMASESA, a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.

- Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el Responsable de Seguridad de la Información.

- Los ficheros de carácter temporal o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir los niveles de seguridad que le correspondan. Éstos serán borrados o destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en el sistema de información o carpeta habilitados al efecto y debidamente protegidos. Si transcurrido un mes el usuario detecta la necesidad de continuar utilizando el fichero, deberá comunicárselo al Responsable de Seguridad de la Información, para adoptar las medidas oportunas sobre el mismo.

Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s.

Comunicación de incidencias

Los usuarios deberán comunicar al Responsable de Seguridad de la Información, con la mayor diligencia posible, cualquier incidencia o sospecha de incidencia de seguridad que detecten, así como los fallos de seguridad o vulnerabilidades que observen en los sistemas de información y en sus mecanismos de protección, tanto físicos como lógicos

Excepciones

Cualquier excepción a esta norma deberá ser solicitada y justificada para su revisión y aprobación, en su caso, por el Responsable de Seguridad de la Información.

Incumplimiento

EMASESA podrá limitar o suspender el uso de los recursos corporativos a aquellos usuarios que contravengan la presente norma. Asimismo, en caso de que el incumplimiento conlleve alguna de las faltas recogidas en el régimen disciplinario previsto en el Convenio Colectivo vigente en EMASESA, se aplicaran las sanciones correspondientes.

EMASESA
metropolitana

Seguridad de la Información en EMASESA

EMASESA tiene desarrollado e implantado un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma UNE-EN ISO/IEC 27001.

Más información en la web corporativa de EMASESA en:

https://www.emasesa.com/conocenos/calidad-de-la-gestion/seguridad-de-la-informacion/

El cuerpo normativo completo del SGSI está publicado en la intranet de EMASESA a disposición de las personas que hacen uso de los recursos tecnológicos y de información de la organización, siendo de obligado cumplimiento.