Objeto

EMASESA establece las normas para el uso seguro y adecuado de los recursos TIC en EMASESA, incluyendo equipos, software, dispositivos, Internet y acceso a datos. Su propósito es proteger a la empresa y sus grupos de interés ante riesgos por un mal uso de la información y sistemas electrónicos. Entre otros objetivos, se persigue:

- **Proteger** la confidencialidad, integridad y disponibilidad de la información generada y recibida por EMASESA.
- **Asegurar** el uso responsable de los recursos tecnológicos.
- **Cumplir** con leyes y normativas sobre protección de datos, seguridad y ciberseguridad.
- **Preservar** la reputación e imagen pública de EMASESA y su personal.
- **Garantizar** las capacidades de prevención, detección y respuesta ante incidentes de seguridad, así como evitar fugas de información.

EMASESA

NURTI

Terceros

Normas de Uso de los Recursos Tecnológicos y de Información para terceros*

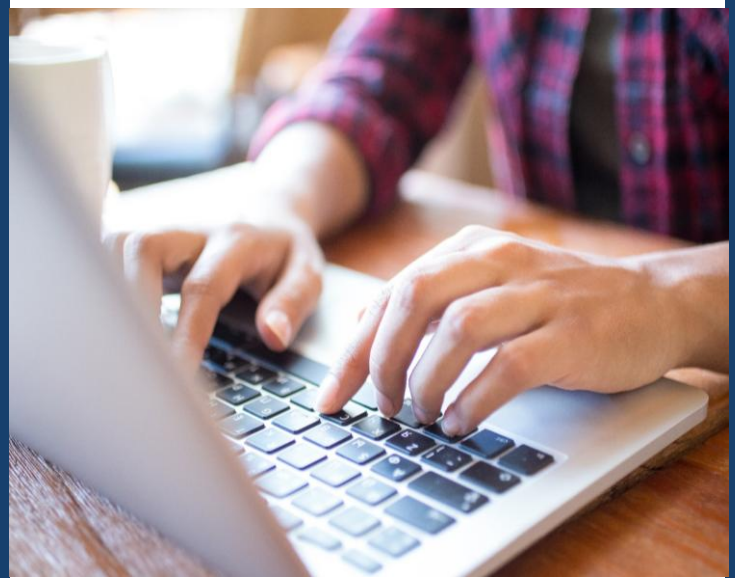
*Este documento es un extracto del documento completo "Normas de Uso de los Recursos Tecnológicos y de Información Terceros" (GE.010.05-01) disponible en la intranet corporativa de EMASESA.

Propiedad de los activos de información

EMASESA proporciona recursos como información, servicios, dispositivos y red a personal externo autorizado, exclusivamente para uso profesional. Estos activos pertenecen a la empresa y están sujetos a políticas de monitorización. Cualquier uso indebido será gestionado según el apartado "Incumplimiento" y la persona usuaria asumirá la responsabilidad por posibles daños. Toda la información almacenada o transmitida mediante estos sistemas está protegida y controlada por EMASESA. Está prohibido cualquier uso comercial o privado que infrinja estas normas.

Uso de los ordenadores

- No modificar la configuración física o lógica de los equipos, ni instalar o desinstalar software, ni conectar dispositivos no autorizados. Tampoco cambiar su ubicación, salvo en el caso de portátiles autorizados.
- No conectar a la red corporativa equipos no autorizados.
- No almacenar información de trabajo en el equipo asignado, al no realizarse copias de seguridad. Utilizar los sistemas corporativos o repositorios habilitados (aplicaciones corporativas, carpetas compartidas, Teams/SharePoint, u otros).
- No crear carpetas compartidas ni cifrar información en los equipos de trabajo sin autorización.
- No utilizar, copiar ni transmitir información propiedad de EMASESA para fines privados o distintos de los profesionales.



- Está terminantemente prohibido:

○ Realizar actividades ilegales o ilícitas, ni difundir contenidos ofensivos, discriminatorios, pornográficos, violentos o contrarios a los derechos humanos o a los valores de EMASESA.

○ Introducir, ejecutar o propagar virus, malware u otros elementos que puedan dañar los sistemas de EMASESA, de terceros o de proveedores.

○ Acceder sin autorización a sistemas, equipos o recursos de la organización.

○ Interferir en el funcionamiento normal de los sistemas de información.

○ Acceder sin autorización a información de otras personas usuarias o vulnerar su privacidad o interferir en su actividad profesional.

○ Eludir los mecanismos de seguridad.

Uso de aplicaciones

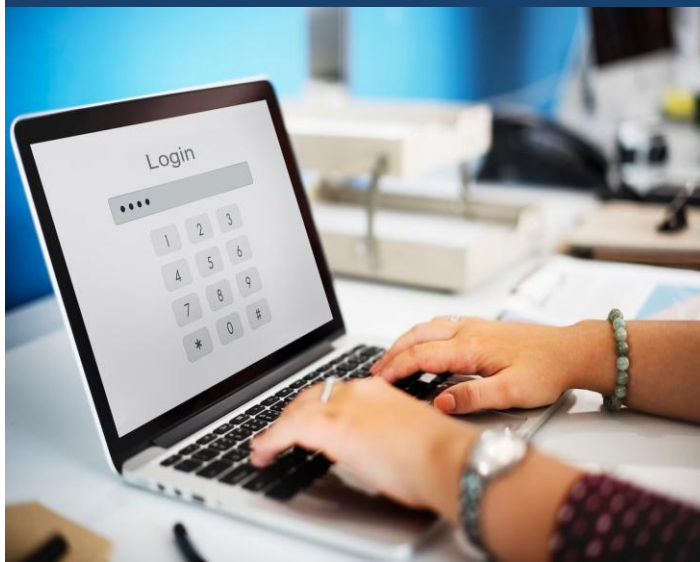
- No se instalarán, ejecutarán o descargarán aplicaciones o programas informáticos en el ordenador de trabajo. Se incluyen las aplicaciones conocidas como portables, ficheros ofimáticos no corporativos con macros, o cualquier otro tipo de archivos ejecutables, aunque no requieran instalación. Cualquier aplicación que se requiera para la actividad laboral, deberá ser solicitada siguiendo los procedimientos internos de EMASESA.
- 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 en los equipos.
- 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.
- No se permite el uso de aplicaciones de mensajería no corporativas en los ordenadores de trabajo, ya sea a través del navegador o utilizando la versión de escritorio de estas (por ejemplo, WhatsApp, Telegram, Google Chat, entre otras).

Uso de ficheros informáticos

- No se permite el uso, almacenamiento, reproducción, cesión, modificación o difusión pública de obras o documentos protegidos por derechos de propiedad intelectual o industrial, o que carezcan de la licencia correspondiente.
- No está permitida la apropiación de archivos o ficheros propiedad de EMASESA para uso particular y/o de terceros no autorizados.
- No se permite la copia, total o parcial, de ficheros que contengan datos personales u otro tipo de información sensible de EMASESA en el ordenador de trabajo, memorias USB u otros soportes de información, incluidos servicios en la nube (almacenamiento, transferencia o tratamiento de documentos), salvo autorización expresa según el puesto de la persona usuaria.
- Está estrictamente prohibida la extracción de cualquier información, soporte, programa o documento de EMASESA obtenido durante el desempeño de la actividad profesional.

Uso de contraseñas

- Las contraseñas de acceso a los equipos, sistemas de información y/o a la red son personales e intransferibles. Cada persona usuaria es responsable de su uso, custodia y de las consecuencias derivadas de su divulgación, pérdida o uso indebido.
- No está permitido:
  - Obtener o utilizar las credenciales de otras personas usuarias, salvo en casos excepcionales debidamente autorizados por el área de Seguridad de la Información.
  - Acceder o modificar los registros de acceso de los sistemas.
  - Intentar eludir las medidas de autenticación establecidas.
  - Anotar contraseñas en claro en lugares visibles o accesibles por terceros.



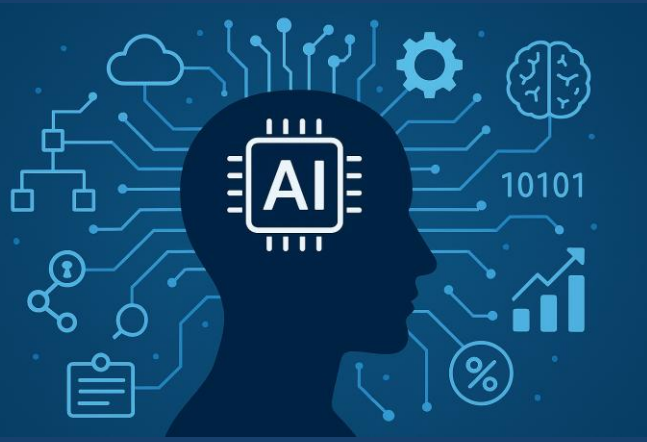
Uso de la red corporativa

- Está prohibida cualquier acción que degrade intencionadamente la calidad del servicio o el funcionamiento de la red.
- No se permiten actividades que pongan en riesgo el trabajo de otras personas usuarias o que permitan el acceso no autorizado a su información.
- El uso de Internet se limita a fines estrictamente profesionales.
- No se permite la conexión a la red de dispositivos no corporativos o no autorizados expresamente.
- No está permitida la conexión a las redes WiFi corporativas sin autorización.
- En relación con el uso de Internet quedan prohibidas las siguientes actividades:

- Transmitir o recibir información no relacionada con la actividad laboral.
- Compartir material protegido por derechos de propiedad intelectual sin autorización.
- Difundir contenidos ilegales, ofensivos, discriminatorios o de carácter sexual explícito.
- Transferir información o material corporativo a terceros sin autorización.
- Tratar datos personales sin cumplir la normativa aplicable o sin la debida autorización.
- Participar en actividades de ocio (juegos, grupos de noticias, visionado de contenidos, etc.) no relacionadas con la actividad profesional.
- Realizar acciones que puedan dañar la imagen o reputación de EMASESA.

Uso de la inteligencia artificial

- No está permitido el uso de plataformas públicas de inteligencia artificial (por ejemplo, ChatGPT, GeminiAI, Deepseek, etc.).
- No está permitido desarrollar herramientas, modelos o entrenamientos de IA no autorizados.



Uso de memorias USB

- No se permite la conexión a los ordenadores corporativos de EMASESA de ninguna memoria USB no corporativa.

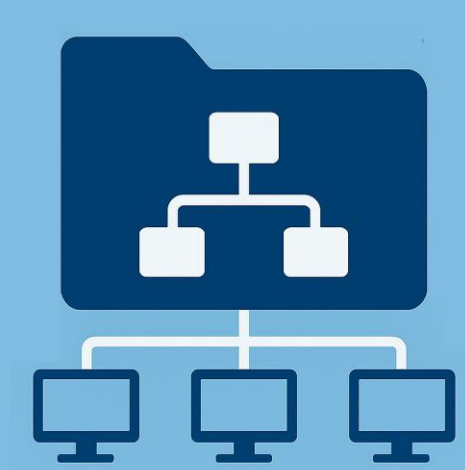
Uso del correo electrónico

En casos excepcionales autorizados EMASESA proporciona cuentas de correo electrónico a personal externo. Se establecen las siguientes directrices para su uso:

- El correo corporativo deberá utilizarse exclusivamente para fines profesionales.
- No se permitirá su uso para el registro en servicios ajenos a la actividad laboral.
- Se evitará el envío de archivos adjuntos de gran tamaño (superiores a 10 MB), utilizando los sistemas corporativos de transferencia de archivos habilitados.
- El envío de correos masivos requerirá autorización previa y deberá realizarse conforme a las directrices del área de TIC.
- Solo el personal autorizado podrá enviar correos con fines publicitarios, siempre con el consentimiento expreso del destinatario y cumpliendo la normativa de protección de datos.
- No se deberán abrir enlaces ni archivos adjuntos de correos sospechosos o de origen desconocido.

No está permitido:

- Compartir contenidos no relacionados con las funciones laborales.
- Enviar o recibir material protegido por derechos de propiedad intelectual sin autorización.
- Difundir contenidos ilegales, ofensivos, discriminatorios o de carácter sexual explícito.
- Transferir información sensible de EMASESA a terceros o a cuentas personales sin autorización. Se prohíbe expresamente el reenvío automático de correos entre cuentas corporativas y personales.
- Tratar datos personales sin la debida autorización o en incumplimiento de la normativa aplicable.
- Transmitir o recibir información no relacionada con la actividad profesional.



Recursos compartidos

- Utilizar los recursos compartidos únicamente para almacenar información relacionada con la actividad prestada para EMASESA.
- La documentación de trabajo debe almacenarse exclusivamente en los Sistemas de Información corporativos (AquaWS, SAP, etc.) o, en su defecto, en los recursos compartidos habilitados por EMASESA para este fin (carpetas compartidas, Teams/SharePoint u otros que se establezcan).
- No se almacenará información corporativa en los ordenadores de trabajo.
- Sólo se accederá a la documentación para la que se tenga autorización expresa, incluso cuando los sistemas de seguridad no impidan otros accesos. En este caso, debe comunicarse de forma inmediata al responsable por parte de EMASESA.

Almacenamiento en la nube

- No está permitido el almacenamiento de información de EMASESA en servicios en la nube pública (Dropbox, Google Drive, etc.). Alternativamente, las personas usuarias autorizadas podrán hacer uso del servicio en la nube privada de EMASESA (MS365 o el servicio que se determine en cada momento).
- No está permitido el uso de servicios públicos de internet para el tratamiento de imágenes, vídeos, ficheros en formato "pdf" o de cualquier otro tipo.

Telefonía móvil

- La persona usuaria es responsable de la custodia del dispositivo y su contenido.
- El terminal no debe compartirse, salvo en los casos en que así esté previsto y autorizado, dejarlo desatendido ni usarlo de forma insegura, especialmente en lugares públicos.
- Deben adoptarse medidas razonables para evitar la pérdida, robo o sustracción del dispositivo. En caso de incidente, se deberá presentar denuncia y comunicarlo al responsable por parte de EMASESA.
- Como norma general, no debe almacenarse ni transportarse información sensible en el dispositivo.
- El teléfono y la tarjeta SIM corporativa forman un conjunto único y no pueden separarse, sustituirse ni combinarse con tarjetas personales.
- No está permitido modificar la configuración original del dispositivo, eliminar aplicaciones corporativas o de seguridad, ni desactivar los mecanismos de protección.
- Está terminantemente prohibido realizar procesos de "root" o "jailbreak" en el dispositivo.
- Solo podrán instalarse aplicaciones autorizadas por EMASESA. Cualquier aplicación adicional deberá solicitarse para su análisis y aprobación.
- La persona usuaria deberá mantener actualizado el sistema operativo y las aplicaciones.
- Las conexiones inalámbricas deberán mantenerse desactivadas cuando no se estén utilizando.
- El dispositivo solo podrá conectarse a redes WiFi seguras y confiables; queda prohibido el uso de redes públicas abiertas.
- Funcionalidades como Bluetooth, punto de acceso u otras sólo podrán utilizarse si el servicio así lo requiere previa autorización por parte de EMASESA.

Acceso remoto

Para las personas usuarias autorizadas a conectarse de forma remota, se les aplicarán todas las directrices generales presentes en este documento y adicionalmente las siguientes:

- Se accederá exclusivamente a los recursos autorizados y durante el periodo de tiempo permitido.
- En ningún caso se dejará el equipo remoto desatendido y con la sesión abierta.
- El equipo para acceso remoto debe tener un antivirus actualizado, el sistema operativo al día con sus parches de seguridad y no presentar signos de compromiso (actividad de malware u otra actividad sospechosa). EMASESA se reserva el derecho de utilizar herramientas de seguridad para verificar estas políticas y denegar el acceso a la red corporativa si detecta incumplimientos.
- Si el equipo remoto no pertenece a EMASESA, la persona usuaria deberá instalar por sí mismo el cliente de conexión y configurarlo siguiendo las instrucciones del manual proporcionado. EMASESA no está obligada a ofrecer soporte técnico para equipos que no sean de su propiedad.

Uso de redes sociales

- No está permitido compartir ficheros, datos o información relativa a EMASESA en redes sociales.

Grabación de imágenes

- Queda prohibido tomar fotografías o grabar vídeos dentro de las instalaciones de EMASESA sin el consentimiento previo y conforme al protocolo interno establecido.

Comunicación de incidencias y cambios

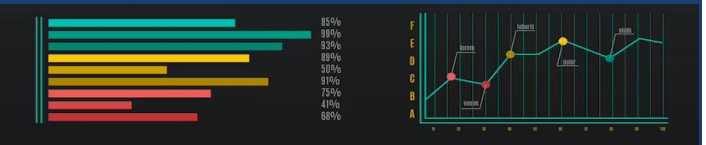
- Cualquier evento o sospecha de incidencia de seguridad deberá comunicarse de inmediato al responsable designado por EMASESA, al CAU o al área de Seguridad de la Información. Esto incluye tanto los fallos como las debilidades detectadas en los sistemas de información, así como en sus mecanismos de protección físicos o digitales.
- Cualquier cambio en la situación contractual de la persona o personas con acceso a los recursos de EMASESA deberá ser comunicada de forma inmediata al responsable del contrato para su actualización o baja.
- Las bajas implicarán revocación inmediata de credenciales, devolución de dispositivos/soporte y certificado de destrucción o devolución de la información en poder del tercero.

Monitorización y supervisión

Con el fin de garantizar 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, todo ello en aras del interés legítimo de EMASESA para la protección de sus activos e información (art. 6.1f RGPD). Además, se generan informes estadísticos de uso de dichos recursos y permiten, en caso necesario, la investigación detallada de cualquier incidente o sospecha de este.

En particular se tienen implementadas las siguientes medidas de monitorización, seguridad, y control :

- Internet; registro de las páginas visitadas (URL y dirección IP) con identificación de la persona usuaria, 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. Los correos detectados por el sistema como potencialmente peligrosos se envían completos al sistema de cuarentena.

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

- Copias de seguridad; todos los archivos digitales, sin importar su tipo (textos, imágenes, videos, correos electrónicos, etc.), almacenados en cualquier sistema de información de EMASESA (carpetas compartidas, servidor de correo, MS365, etc.), excepto en los ordenadores de trabajo, están protegidos con copias de seguridad que permiten su restauración en cualquier momento.

- Teléfonos móviles: registro de las aplicaciones instaladas, tanto en perfil para uso profesional como personal. Antivirus como herramienta de protección, instalado en ambos perfiles.

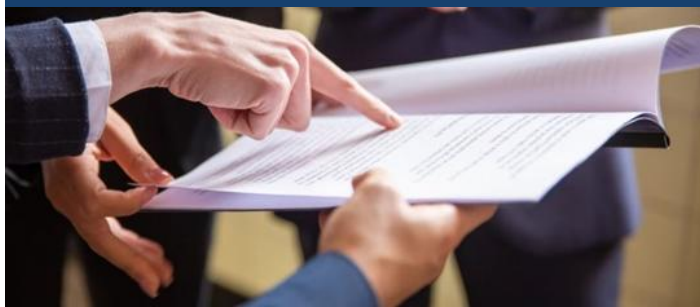
- Registro de accesos: en general, todos los sistemas registran los datos para identificar la persona usuaria que accede, incluida fecha, hora y recursos accedidos.

- En general, todo el tráfico puede ser filtrado e inspeccionado para fines de seguridad.

Esta relación no es exhaustiva y podría estar sujeta a cambios con la incorporación de nuevos sistemas y tecnologías en función de las necesidades de protección de EMASESA.

Para proteger los activos de información y al personal de EMASESA, puede ser necesario acceder de manera justificada a la información disponible en cualquier medio digital de la compañía en cualquier momento. Dado el propósito profesional de estos medios, no se puede garantizar la privacidad de la información contenida en ellos. Por lo tanto, no deben considerarse privados ni son adecuados para almacenar, tratar, o transmitir información de carácter privado.

En caso necesario, personal autorizado podrá realizar un análisis específico para identificar a la persona usuaria que ha llevado a cabo una determinada acción y obtener un mayor nivel de detalle sobre la misma. 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 fin de corregir acciones contrarias a esta norma o para gestionar un incidente de seguridad. Estas actividades se realizan proporcionalmente con minimización de datos y controles de acceso.



Excepciones

Cualquier excepción a esta norma deberá ser solicitada por la persona usuaria a través de su responsable en EMASESA para su gestión a través de los procedimientos establecidos.

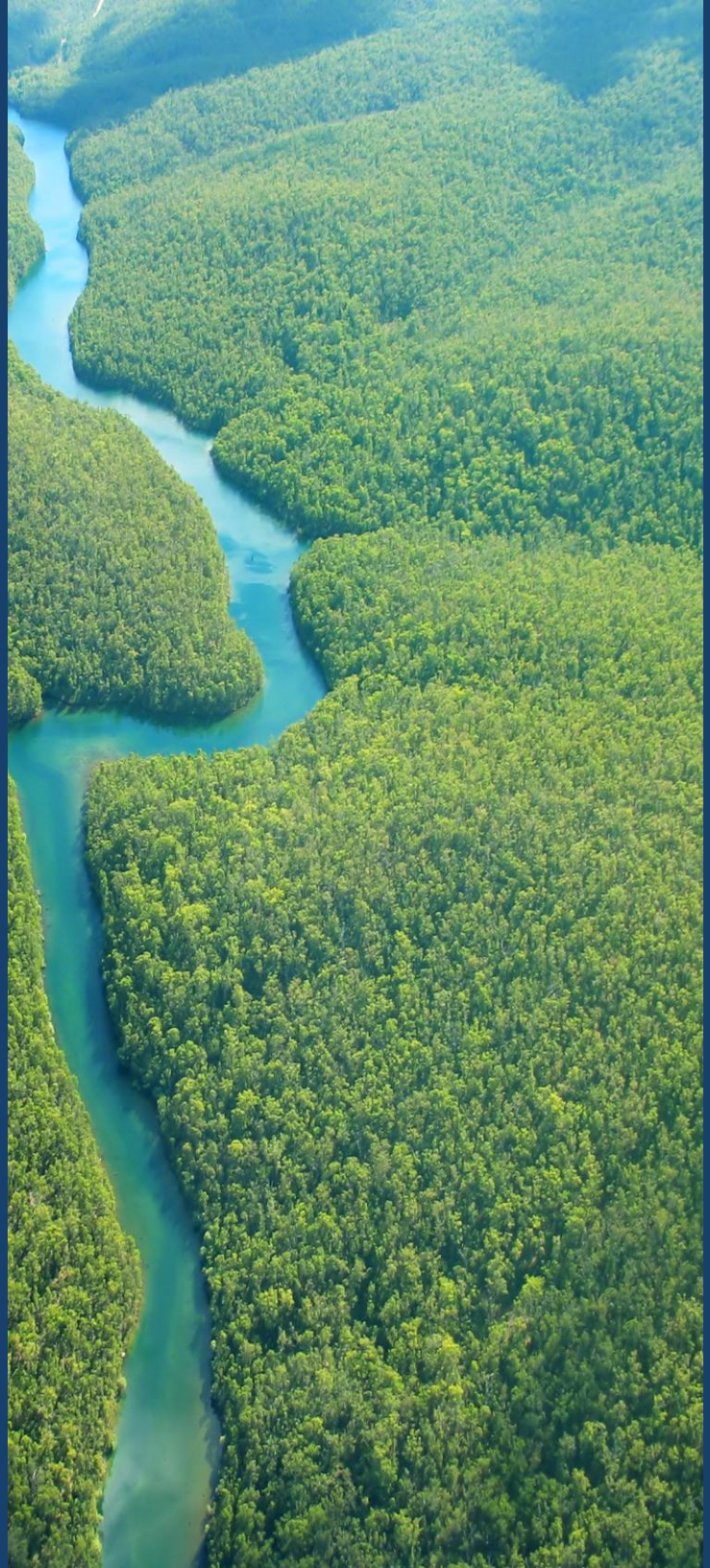
Incumplimiento

El incumplimiento de las presentes normas por parte del personal de terceros podrá dar lugar, de forma inmediata y sin necesidad de previo aviso, a la limitación, suspensión o revocación del acceso a los sistemas, aplicaciones, redes, instalaciones y demás recursos de EMASESA.

Dicho incumplimiento se considerará imputable tanto a la persona que lo cometa como, en su caso, a la entidad a la que pertenezca, que será responsable de garantizar el cumplimiento de estas normas por su personal.

EMASESA se reserva el derecho de ejercer cuantas acciones legales y/o contractuales (aplicación de penalidades contractuales previstas en los pliegos) resulten procedentes frente a la persona infractora y/o su organización, incluyendo la reclamación de daños y perjuicios que pudieran derivarse.

Asimismo, cuando el incumplimiento sea grave o reiterado, EMASESA podrá resolver o rescindir la relación contractual que existiera con la entidad responsable, sin perjuicio de las acciones adicionales que pudieran corresponderle.



EMASESA

Seguridad de la Información

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

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.