CINESI

Consultoria de **mobilitat i transport**

NORMATIVA DE SEGURIDAD

Realizado por	Revisado y aprobado por
Responsable del SGSI	Dirección

Edición	Fecha revisión	Observaciones	Aprobado
1.0	12/12/2025	Versión inicial. Implantación.	12/12/2025

ÍNDICE

ÍNDICE **3**
1. OBJETIVO **4**
2. ALCANCE **4**
3. DEFINICIONES **4**
4. REVISIÓN Y EVALUACIÓN **4**
5. DESARROLLO **5**
5.1. Cómo crear contraseñas robustas 5
5.1.1. Cambio de contraseñas 6
5.2. Normas para USB (pendrives) 6
5.3. Normas para equipos portátiles y móviles 7
5.4. Puesto de trabajo despejado 7
5.5. Otros dispositivos conectados a la red: impresoras y fotocopiadoras 8
5.6. Normas para el uso del correo electrónico corporativo 8
5.6.1. Usos especialmente prohibidos para el uso del correo electrónico corporativo 9
5.7. Normas para el uso de internet. 9
5.7.1. Usos especialmente prohibidos de internet 10
5.8. Uso de redes 10
5.9. Instalación de software 10
5.10. Seguridad física 11
5.11. Tratamiento de la información 11
5.12. Datos de carácter personal 11
5.13. Comunicación de incidentes/brechas de seguridad 12
5.14 Procedimiento para la comunicación del robo 12
6. MONITORIZACIÓN Y APLICACIÓN DE ÉSTA NORMATIVA **12**
7. INCUMPLIMIENTO DE ÉSTA NORMATIVA **12**
8. ANEXOS **13**
8.1. Aceptación y compromiso de cumplimiento 13
8.2. Aceptación de entrega de credenciales 13

1. OBJETIVO

El objetivo de la presente normativa es regular el uso aceptable por parte de los usuarios de los Sistemas de Información de CINESI, desde las distintas sedes o a través de ellas, posibilitando la homogeneización de criterios dentro de sus departamentos y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

Este documento se considera de uso interno de CINESI y, por tanto, no podrá ser divulgado salvo autorización del Responsable de Seguridad.

2. ALCANCE

El presente documento será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en CINESI, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información de CINESI.

3. DEFINICIONES

La presente guía ha sido aprobada por el Comité de Seguridad de CINESI, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que CINESI 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 CINESI.
Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta normativa.

4. REVISIÓN Y EVALUACIÓN

La gestión de esta guía corresponde al Comité de Gestión que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario 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 aprobación.

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. DESARROLLO

5.1. Cómo crear contraseñas robustas

Es necesario que las contraseñas que se utilicen como mecanismo de autenticación sean robustas, es decir: difícilmente vulnerables.

En este sentido, se han definido las siguientes reglas, que deberán ser seguidas por todos los usuarios a la hora de la definición o creación de contraseñas:

Longitud mínima de la contraseña: 8 caracteres, deben incluir al menos caracteres de tres de las siguientes categorías:

- Mayúsculas (de la A a la Z)
- Minúsculas (de la a a la z)
- Caracteres alfanuméricos (1,2,3....)
- Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %)
- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- No conviene que posea caracteres idénticos consecutivos.
- Idealmente, la contraseña no debería ser igual a ninguna de las 24 últimas contraseñas usadas.
- La contraseña deberá cambiarse cada 6 meses, o siempre que se entienda que ha podido ser puesta en compromiso.

Además:

- Las contraseñas no deberán estar basadas en algún dato propio que otra persona pueda adivinar u obtener fácilmente (nombre, apellidos, fecha de nacimiento, número de teléfono, etc.).
- Las contraseñas deberán ser fáciles de recordar. Se hace necesario, por tanto, encontrar una solución de compromiso entre la robustez de la contraseña y la facilidad con la que se puede recordar.
- Hay que evitar apuntar las contraseñas en papel.
- No utilizar la misma contraseña para distintos servicios web o dispositivos.
- Cada usuario será responsable único del mantenimiento de la confidencialidad de sus identificadores de usuario y de sus contraseñas.
- Queda expresamente prohibido comunicar los identificadores de usuario y las contraseñas de acceso a terceras personas. En caso de incumplimiento de esta prohibición el usuario será el único responsable de los actos realizados por aquellos que los utilicen de forma no autorizada.

5.1.1. Cambio de contraseñas

Si un usuario entiende que su contraseña ha quedado comprometida o la ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debe sustituir la contraseña por otra que no hubiera sido comprometida, de manera inmediata.

Por otro lado, el usuario deberá realizar una petición de cambio de contraseña al Departamento TI cuando se produzca alguna de las situaciones siguientes:

- Olvidé la contraseña.
- Bloqueo del acceso a través de contraseña tras superar el número máximo de intentos fallidos.

En estos casos, como norma general, el cambio de contraseña por una contraseña provisional (de un solo uso) será realizado por personal técnico del Departamento TI, que comunicará esta contraseña al usuario, sin intermediarios.

Las contraseñas proporcionadas por el Departamento TI, tras la petición de cambio de contraseña de un equipo y/o aplicaciones, son consideradas contraseñas “provisionales”. Por ello, el usuario deberá proceder a sustituir la contraseña “provisional” por una contraseña personal que cumpla con los requisitos indicados en el apartado anterior. El usuario deberá realizar este cambio durante el primer inicio de sesión en su puesto de usuario.

Ningún usuario está autorizado acceder a los servicios internos de CINESI utilizando credenciales de otros usuarios, incluyendo el simple conocimiento de la contraseña de otro usuario. Esta práctica compromete la confidencialidad de la información, y por supuesto, la autenticidad de quién accede a ella.

5.2. Normas para USB (pendrives)

Con carácter general, el uso de memorias USB en CINESI no está autorizado. En su caso, la autorización deberá proporcionarla el Departamento de IT.

Por razones de seguridad, los interfaces USB de los puestos de usuario estarán deshabilitados. En caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe del Departamento de IT.

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 el Departamento de IT.

Estas memorias USB serán de uso exclusivo en los puestos de usuario de CINESI no debiendo ser usados fuera de éstos.

Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento.

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

5.3. Normas para equipos portátiles y móviles

Los equipos portátiles y móviles serán asignados por el Departamento de IT.

Existirá un inventario actualizado de los equipos portátiles y móviles. El Departamento de IT será la unidad encargada de gestionar dicho inventario.

Este tipo de dispositivos estará bajo la custodia del usuario que los utilice. 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 IT 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 y autorizados, especialmente cuando se usen fuera de las instalaciones de CINESI.

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

En general, los equipos portátiles no deberán conectarse directamente a redes externas no seguras.

5.4. Puesto de trabajo despejado

Se habilitan armarios para guardar la información física que no esté siendo utilizada de tal manera que las mesas deber estar despejadas de información y otros materiales cuando los usuarios asignados no están en su puesto de trabajo.

Además:

Siempre que por cualquier motivo un usuario abandone su puesto de trabajo bloqueará su equipo para evitar que terceros puedan acceder a los recursos y aplicaciones a las que el usuario legítimo esté autorizado. Para bloquear un equipo basado en Windows basta con pulsar la combinación de teclas [Windows]+[L].
Los equipos deben tener configurado el bloqueo de sesión automático en caso de inactividad de forma que los equipos se bloquean automáticamente después de 15 minutos sin actividad.

5.5. Otros dispositivos conectados a la red: impresoras 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 CINESI 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 del sistema o la Dirección.

5.6. Normas para el uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de CINESI para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.
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 CINESI.
El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, quedando totalmente prohibido el uso privado del mismo.
Se deberá notificar al Departamento IT cualquier tipo de anomalía detectada, así como los 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 ejecutarse 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 IT.
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.
Asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.
Evitar, en la medida de lo posible, el uso ineficiente en los envíos de correo: agrupar los envíos a múltiples destinatarios en un solo mensaje, evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos (ya que incrementan innecesariamente el tamaño y volumen de estos), envíos innecesarios, etc.

5.6.1. Usos especialmente prohibidos para el uso del correo electrónico corporativo

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. El sistema evitará el intercambio de correos de tamaños superiores a 25 Mb.

- La utilización del correo corporativo para recoger correo de buzones que no pertenezcan a CINESI o el reenvío automático del correo corporativo a buzones ajenos a la organización. Para ello se necesitará la autorización expresa del Departamento IT.

5.7. Normas para el uso de internet.

El acceso a Internet deberá ser autorizado por CINESI siempre que se estime necesario para el desempeño de la actividad profesional del usuario o solicitante y exista disponibilidad para ello. En otro caso, se podrá acceder a Internet desde un puesto de acceso común habilitado para ese fin.
Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos.
El acceso a Internet para fines personales está totalmente prohibido para que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.
Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por el Departamento IT en los puestos de usuario.
No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del Departamento IT.
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.

- Debe tener en cuenta:
- No aceptar cookies de terceros.
- Bloquear pop-ups.
- Evitar el autocompletado.
- Borrar los ficheros temporales y cookies al cerrar el navegador.
- Bloquear la geolocalización.

Deberá notificarse al Departamento de IT cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

5.7.1. Usos especialmente prohibidos de internet

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 sin la autorización previa del Departamento IT o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- No visitar páginas de contenido poco ético, ofensivo o ilegal igualmente no visitar páginas no fiables o sospechosas.

5.8. Uso de redes

La segmentación de las redes se lleva a cabo mediante el empleo de “zonas” de Firewall y VLANs.

nivel de acceso y usos:

- ➔ Red corporativa: Único nivel de acceso para empleados
- ➔ Red de servidores: N/A
- ➔ VPN: La VPN da acceso a la red corporativa o la red de servidores dependiendo del perfil del usuario indicado por el servidor LDAP con el que se acceda por VPN.

Se dispone de una red Wifi en la que puede acceder cualquier persona que conozca la contraseña. No hay acceso al servidor desde la wifi de Cinesi por seguridad.

5.9. Instalación de software

Únicamente el personal Departamento IT podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.
No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.
Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de CINESI de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.
No se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por CINESI, especialmente aquellas relacionadas con la seguridad

5.10. Seguridad física

El acceso a la oficina de personal externo se controla desde la recepción. Como norma general, el personal ajeno a la entidad debe permanecer acompañado de personal autorizado mientras permanezca en las zonas que no son de acceso al público. La persona encargada de la recepción, llevará un control de todas las personas externas a CINESI que hayan visitado la oficina.

5.11. Tratamiento de la información

Toda la información contenida en los Sistemas de Información de CINESI o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a CINESI y a su personal.

Cualquier tratamiento en los Sistemas de Información de CINESI deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente, europea y nacional, en materia de Protección de Datos.

Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de CINESI en servidores externos, salvo autorización expresa.

5.12. Datos de carácter personal

La información contenida en las bases de datos de CINESI que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Ficheros o Tratamientos de datos de carácter personal gestionados por CINESI han de adoptar las

medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

Todo usuario (de CINESI o de terceras organizaciones) que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con CINESI.

5.13. Comunicación de incidentes/brechas 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 CINESI o su imagen, deberá informar inmediatamente al Responsable de Seguridad que lo registrará debidamente y elevará, en su caso.

5.14 Procedimiento para la comunicación del robo

La pérdida o robo del dispositivo o del portátil debe ser comunicada por el usuario a IT por medio de correo electrónico

6. MONITORIZACIÓN Y APLICACIÓN DE ÉSTA NORMATIVA

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

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

Monitorizará los accesos a la información contenida en sus sistemas.

Auditará la seguridad de las credenciales y aplicaciones.

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

7. INCUMPLIMIENTO DE ÉSTA NORMATIVA

Todos los usuarios de la CINESI están obligados a cumplir lo prescrito en la presente Normativa de Seguridad Interna.

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

8. ANEXOS

8.1. Aceptación y compromiso de cumplimiento

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, empleado de la empresa Cinesi, SLU, como usuario de recursos informáticos y sistemas de información de la Cinesi, declara haber leído y comprendido la Normativa de Seguridad Interna de la empresa y se compromete, bajo su responsabilidad, a su cumplimiento.

8.2. Aceptación de entrega de credenciales

El empleado acepta la entrega de las credenciales necesarias para acceder a los sistemas y recursos digitales de la empresa, incluyendo pero no limitado a nombres de usuario y contraseñas, comprende que estas creencias son confidenciales y de su responsabilidad exclusiva, y se compromete a no compartir, revelar ni permitir el uso no autorizado de las mismas.

Al firmar este documento el empleado reconoce que su firma electrónica o manuscrita equivale a una firma auténtica y representa su conformidad con los términos aquí expuestos.

<<En _____, a ____ de _____ de 20__>>

Trabajador (Nombre y Apellidos):
DNI número:
Firmado: