Normativa de Seguridad

Esquema Nacional de Seguridad

Fecha: 02/03/2026

Versión 0.1

Uso de la información Interna

Índice

Control de Versiones

Versión	Autor	Revisión	Aprobado	Fecha	Descripción
0.1	Responsable de Seguridad		Dirección	02/03/2026	Versión inicial

1. Introducción y objeto

La presente normativa tiene por objeto la regulación del uso de los recursos informáticos y servicios de INFORMACIÓN DEL TERRITORIO con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, de la información.

Esta norma general establece una serie de prácticas que regulan el adecuado uso y disponibilidad de los recursos informáticos, comprometiéndose INFORMACIÓN DEL TERRITORIO a su difusión hacia todo el personal laboral.

Así mismo, los usuarios que, de forma reiterada, deliberada o por negligencia los infrinjan, quedarán sujetos a las actuaciones técnicas o disciplinarias que se estimen oportunas. Los usuarios se comprometen a colaborar con el Administrador de sistemas de la INFORMACIÓN DEL TERRITORIO, en adelante Administrador de sistemas para llevar a cabo toda investigación que tenga por objeto encontrar las posibles causas derivadas del mal uso de los recursos tecnológicos.

2. Ámbito de aplicación

Esta política es de obligado cumplimiento para el personal de INFORMACIÓN DEL TERRITORIO, así como para todas aquellas personas físicas, profesionales u organizaciones que pudieran tener acceso a los sistemas de información, debiéndose respetar y seguir cada una de las medidas que se indican en esta Política de Uso Aceptable de los Sistemas de la Información, así como todas aquellas medidas adicionales que pueda comunicar LOS RESPONSABLES de INFORMACIÓN DEL TERRITORIO como de obligado cumplimiento.

Además, también quedan sujetos a las normas y condiciones contenidas en este documento, todos los equipos y Sistemas de Información y Comunicaciones de INFORMACIÓN DEL TERRITORIO, ya sean personales o compartidos, y estén o no conectados a la red. Aquellos equipos que no sean propiedad de INFORMACIÓN DEL TERRITORIO pero que se conecten a la red de la empresa o usen los servicios y recursos de la misma, también deberán cumplir con esta normativa de uso. Los servicios y recursos ofrecidos por la empresa a sus usuarios serán utilizados en las condiciones previstas en cada caso. Dichas condiciones estarán recogidas en normativas específicas de uso o en su defecto, por la normativa que con carácter general define el presente documento.

3. Medidas de Control sobre Sistemas de Información

Dentro del ámbito de potestades de control del empresario que figuran en el Art. 20.3 del Estatuto de los Trabajadores, INFORMACIÓN DEL TERRITORIO realiza las investigaciones y aplica los controles que considera necesarios, tanto en los equipos como en las herramientas facilitadas al usuario, lo que incluye, entre otros, el correo electrónico corporativo, ordenadores…

El control y acceso a los SI facilitados por INFORMACIÓN DEL TERRITORIO, incluyendo los documentos que los mismos generan, y las comunicaciones implementadas en dichos sistemas, puede llevarse a cabo sin una justificación específica, de forma temporal o permanente, dada la naturaleza de las herramientas para el trabajo facilitadas por INFORMACIÓN DEL TERRITORIO que disponen estos equipos.

Mediante la presente política, el usuario tiene pleno conocimiento de la existencia del control sobre estos medios, y del objetivo que éste persigue. Los controles se llevan a cabo sin dañar ni atentar la dignidad o la intimidad del usuario y siempre atendiendo a criterios objetivos, no abusivos y plenamente justificados.

Las finalidades genéricas de este control son, entre otras, las siguientes:

- Cumplimiento de la legalidad vigente en materia de protección de datos, confidencialidad, propiedad intelectual y seguridad de la información.
- Protección de los sistemas de información y la red corporativa, y de los equipos que lo conforman, a fin de salvaguardar su integridad y disponibilidad.
- Protección de la información corporativa ante usos inadecuados, tanto externos como internos, sean de tipo malintencionado o accidental.
- Garantizar la continuidad del desarrollo de las actividades habituales asignadas a cada usuario en el caso de que éste se ausente por razón de enfermedad, vacaciones u otras similares.
- Prevención de la responsabilidad frente a terceros.
- Comprobación de la existencia o no de uso abusivo de los medios tecnológicos que INFORMACIÓN DEL TERRITORIO facilita, durante el horario laboral. Por tanto, todos los contenidos, informaciones, ficheros almacenados en estos medios, incluida la información temporal, podrán ser accedidos y monitorizados por parte de INFORMACIÓN DEL TERRITORIO a través de los responsables designados a tal efecto.

4. Políticas de seguridad relativas a los dispositivos móviles

Esta normativa pretende establecer la manera correcta de utilizar los dispositivos y líneas móviles facilitados por INFORMACIÓN DEL TERRITORIO. Fuera de este ámbito, no está permitido el uso de “pendrives” y discos duros externos para almacenar la información, excepto a los miembros de los Dptos. de Dirección y Sistemas encargados de formatear los equipos informáticos.

Queda terminantemente prohibido al usuario:

Realizar prácticas de “Mobbing” o cualquier forma de acoso laboral a compañeros, así como el acoso telefónico a personas ajenas a INFORMACIÓN DEL TERRITORIO.

En general, realizar cualquier práctica que vulnere la legalidad vigente cometida utilizando cualquiera de las posibilidades de comunicación que ofrece el recurso móvil.

La creación, distribución o intercambio de contenidos ofensivos u obscenos, incluyendo material pornográfico.

El envío de mensajes con contenido que promocione la discriminación basada en raza, sexo, nacionalidad, edad, estado civil, orientación sexual o discapacidad.
El envío de mensajes amenazantes o violentos.
El envío de información corporativa propiedad de INFORMACIÓN DEL TERRITORIO, secretos comerciales o cualquier otra información confidencial.
La creación, envío, reenvío o intercambio de mensajes comerciales no solicitados (SPAM), mensajes en cadena, solicitudes, anuncios, bulos o falsas alarmas.
La creación, el almacén o intercambio de contenidos que violen las leyes de derechos de autor y derechos de copia.
Para el uso de estos dispositivos se ha de tener en cuenta:
Utilizar la protección por contraseña para bloquear el dispositivo.
Habilitar la password de SIM.
Utilización de bloqueo automático después de un cierto tiempo si no se utiliza.
Denegar el acceso inmediato del proveedor de telefonía móvil en caso de pérdida.
Comunicar a la compañía en caso de robo o pérdida.
Habilitar el modo pérdida cuando el dispositivo lo permita

El almacenamiento de datos de INFORMACIÓN DEL TERRITORIO en entornos o dispositivos de terceros está expresamente prohibido. Esto también es válido para dispositivos de almacenamiento que no son propiedad de INFORMACIÓN DEL TERRITORIO.

¡Nunca deje sin vigilancia los dispositivos móviles o se los deje a personas no autorizadas!

5. Seguridad de los equipos fuera de las instalaciones / teletrabajo / protección de los equipos.

Por criterio general sólo los equipos portátiles y aquellos que no siendo portátiles estén autorizados a teletrabajar, pueden salir de las instalaciones. En este caso es responsabilidad del usuario del equipo garantizar su seguridad evitando situaciones de riesgo, garantizando su estado físico y controlando su ubicación segura en todo momento.

Los equipos están protegidos por contraseña siguiendo la política de la organización.

Los equipos se protegen de forma que se reduzcan los riesgos durante su utilización. Los equipos de trabajo en la oficina están protegidos mediante los controles de acceso a la oficina y las medidas de seguridad intrínsecas del trabajo en nuestras propias instalaciones. La información crítica está protegida en los servidores.

El usuario debe extremar el cumplimiento de las buenas prácticas que le son de aplicación recogidas en este documento.

Para aquellos equipos que salgan fuera de las instalaciones de la organización, se seguirán los siguientes principios básicos de seguridad:

- No se conectarán a redes Wifi desconocidas, o potencialmente inseguras.
- Se bloquearán siempre que no estén siendo usados.
- Cuando sea posible, se cifrarán los discos duros.
- Se almacenarán siempre en un lugar seguro (cuarto cerrado con llave, armario cerrado con llave, caja fuerte, etc).
- Para las conexiones remotas a la oficina, se utilizarán conexiones seguras.
- En el caso de viajes en transporte público (tren, avión, bus, etc), se evitará mostrar información confidencial que pueda ser visualizada por personal ajeno a la organización.

6. Política de equipo de usuario desatendido

Cuando un usuario abandona su puesto de trabajo, tiene que bloquear el equipo, en caso de no hacerlo a los 5 minutos se activa el salvapantallas, bloqueando el equipo automáticamente. Para continuar la actividad anterior al bloqueo, será necesario introducir contraseña.

7. Política de escritorio limpio

El puesto de trabajo debe estar despejado y limpio de papeles. El escritorio de nuestro equipo informático debe estar libre de iconos de acceso directo a carpetas o aplicaciones que contengan datos sensibles. En caso de ausentarse de su puesto poco tiempo, se pondrá boca abajo los documentos para evitar que sea visto, también se bloqueará el equipo para que no pueda acceder nadie.

8. Uso de internet

Internet se considera hoy día como la herramienta más valiosa para la obtención de información, así como para la distribución de esta. Además, facilita la comunicación rápida y eficaz, y el acceso a información en un ámbito global, ofreciendo la oportunidad de aprovechar nuevos mercados y áreas de negocio.

Es preciso tener presente, que el uso de Internet no es gratuito. INFORMACIÓN DEL TERRITORIO incurre en costes asociados, tanto en forma tangible (tarifas de las líneas de comunicaciones, hardware, software, mantenimiento) como intangible (riesgos de seguridad inherentes).

El uso que desde INFORMACIÓN DEL TERRITORIO se espera que se realice de esta herramienta se orienta a los siguientes aspectos:

- Comunicación, incluyendo correo electrónico, proyectos colaborativos de investigación e intercambio de información con clientes y proveedores.
- Acceso a fuentes de información (webs, grupos de noticias, foros, listas de correo, boletines) que permitan al empleado mantenerse al día acerca de nuevas noticias, desarrollos técnicos, oportunidades, o investigación en su área de trabajo.
- Búsqueda de información relacionada con proyectos de trabajo.

- Marketing y promoción de INFORMACIÓN DEL TERRITORIO y su imagen.
- Desarrollo de actividades de negocio solamente posibles mediante la interconexión universal proporcionada por Internet.

El uso indiscriminado de Internet puede exponer a INFORMACIÓN DEL TERRITORIO a riesgos significativos; riesgos que pueden llegar a tener efectos apreciables en la reputación de la empresa ante sus clientes. En consecuencia, se establecen, los siguientes protocolos de buen uso:

- El uso de la web está restringido a propósitos legítimos de negocio.
- El uso personal de Internet está permitido siempre y cuando se cumpla con las reglas contenidas en este documento, con las siguientes dos restricciones adicionales:
- Los recursos consumidos deberán ser inapreciables.

No se visitarán intencionadamente sitios web cuyo contenido sea:

- Difamatorio, amenazante, ofensivo o degradatorio hacia personas, entidades o colectivos de tipo alguno.
- Sexualmente explícito, bien sea en imagen o en lenguaje.
- Ilegal, o que contenga información orientada a la comisión de actos ilegales. En particular, descargas (gratuitas o de pago) de software, de música o vídeos, o de otro material cuya distribución está restringida por leyes de propiedad intelectual (p.e., libros o publicaciones cuyo copyright no ha expirado).
- Todas las comunicaciones que se establezcan desde las oficinas o las máquinas de INFORMACIÓN DEL TERRITORIO estarán asociadas con la empresa. Es, por tanto, indispensable reflejar los más altos estándares de profesionalidad en la utilización de Internet.
- La descarga de información desde sitios web desconocidos no está permitida. El usuario no descargará ítem alguno de fuentes que no sean de confianza. La instalación de software adicional (legal o no) necesitará la previa autorización del Responsable de seguridad

Es responsabilidad de cada empleado mantenerse alerta ante las posibles amenazas o riesgos para la información proveniente de Internet, y utilizar los recursos que INFORMACIÓN DEL TERRITORIO pone a su disposición de un modo racional de manera que se minimice el riesgo.

Todo empleado es responsable de la actividad de red efectuada con su nombre de usuario.

Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial, control de virus, phishing y pharming.

La empresa se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa. Esta revisión sólo podrá llevarse a cabo cuando exista una sospecha

razonable de la comisión de un delito, una falta, una infracción administrativa o un incumplimiento grave de estas normas que comprometa la seguridad del sistema.

9. Uso de redes

En INFORMACIÓN DEL TERRITORIO, existe segregación de redes ya que existe una red wifi solo habilitada para la navegación por Internet, la cual es para invitados y móviles personales, y luego hay otra Wifi para usos corporativos a la que únicamente se puede acceder si la Mac Adress del dispositivo está registrada.

- Red VPN: Esta red es accesible para todo el personal de la de la empresa in situ. En remoto también para el personal que disponga de equipo o móvil a través de un software concreto y usando las credenciales que la empresa proporciona.

1 Acceso remoto

INFORMACIÓN DEL TERRITORIO cuenta con un acceso remoto a los sistemas de información.

El empleado debe hacer uso de dicha conexión remota únicamente para finalidades estrictamente laborales, cumpliendo en todo momento con las obligaciones que se desprenden del Compromiso de Confidencialidad.

Esta autorización se encuentra directamente vinculada a la relación laboral con INFORMACIÓN DEL TERRITORIO, así como al rol desempeñado en la misma. En el momento en el que finalice su relación laboral con la organización, o cambie su rol, no requiriendo de este acceso remoto, dicha autorización quedará cancelada, no teniendo así autorización para la conexión remota a los sistemas de información.

10. Información confidencial

Los documentos que manejamos habitualmente pueden contener información altamente confidencial acerca de clientes. En consecuencia, todo Empleado deberá tomar las medidas de control necesarias para asegurar, dentro de su ámbito de alcance, que dicha información no llegue a manos de personas no autorizadas a tener acceso a la misma. Para garantizar este punto y minimizar el riesgo de posibles filtraciones o accesos no deseados, se deberán tener en cuenta los siguientes puntos:

- Los documentos propios de un proyecto no deberán estar a la vista pública en lugares donde puedan acceder personas no autorizadas. En particular, la mesa y el entorno de trabajo no deben tener a la vista papeles o notas con información confidencial.
- Los documentos que ya no se estimen de utilidad y que no vayan a ser archivados, sea en formato papel o electrónico, deberán ser destruidos físicamente. En el caso del formato papel, existen dos tipos de contenedores: los ordinarios, destinados al depósito

de residuos con carácter general, y los destinados a la “destrucción confidencial” de documentación.

- En la medida de lo posible, los papeles de trabajo se guardarán al finalizar la jornada laboral; caso de no disponer de un sitio adecuado para ello, se procurará tomar las medidas oportunas para evitar su acceso por personas no autorizadas.
- Se evitará utilizar la Información Confidencial para cualquier otro propósito, distinto de aquél para el que fue solicitada.
- El uso de dispositivos de almacenamiento de información distintos a los homologados, inventariados y autorizados por INFORMACIÓN DEL TERRITORIO deberá ser autorizado expresamente por Seguridad Informática.
- Cualquier soporte de información, informático, en papel o de cualquier otro tipo, que un usuario localice en los locales de INFORMACIÓN DEL TERRITORIO o sus inmediaciones que tenga la apariencia de haber sido extraviado, será entregado de forma inmediata a Seguridad Informática.
- Al finalizar la relación laboral o de cualquier otra índole con INFORMACIÓN DEL TERRITORIO, se deberán devolver todos los dispositivos asignados en el transcurso de la relación con la Entidad. Estos dispositivos deben ser devueltos en buen estado.
- Se limitará al mínimo imprescindible el número de personas que tendrán acceso a la Información Confidencial y cumplirán con lo dispuesto en la legislación sobre protección de datos de carácter personal.
- Cuando se trate de enviar borradores de informes o similares a clientes, se recomienda enviarlos en formato PDF.

11. Políticas de seguridad aplicadas dependientes de SO

Los sistemas operativos permitidos a los empleados de la compañía se restringen a los listados a continuación. En todo momento es obligación del empleado cumplir con los criterios de seguridad descritos:

- Windows:
    - Utilización de un Antivirus y malware
    - El equipo Windows debe de tener en todo momento un antivirus y antimalware.
    - Uso de firewall
    - El equipo Windows debe de tener activado el firewall.
    - Actualizaciones del SO
    - En todo momento el equipo Windows debe de estar actualizado.
    - Política de Contraseñas

12. Política sobre licencias de software y copyright

La política de uso y adquisición de software de INFORMACIÓN DEL TERRITORIO abarca las condiciones y procedimientos para la adecuada adquisición, utilización y control del uso del software en el ámbito de la organización.

Con carácter general, los productos software utilizados en el ámbito de INFORMACIÓN DEL TERRITORIO estarán dentro de uno de los siguientes casos:

- Productos desarrollados por terceros que licencian el producto software a INFORMACIÓN DEL TERRITORIO, mediante el correspondiente contrato de licencia de uso, ya sea para personas, puestos o máquinas específicas, o genérica para un departamento o toda la organización.
- Software de Fuentes Abiertas, con su correspondiente licencia de uso, distribución y modificación.
- Productos desarrollados por la propia organización.

En consecuencia, la titularidad y propiedad de los derechos sobre los productos software empleados en el ámbito de INFORMACIÓN DEL TERRITORIO, corresponden bien a la propia entidad o bien a los terceros proveedores de software propietario, debiendo por tanto el usuario abstenerse de realizar cualesquiera acciones contrarias a aquellas para las que se halle expresamente autorizado. En particular, se deberán tener en cuenta las normas establecidas en la presente política de uso y adquisición de software.

Toda aplicación deberá ser aprobada e instalada por el departamento de sistemas.

13. Normas generales de uso de software

Ningún miembro de la empresa utilizará programas para los que no esté autorizado, bien a nivel personal, bien a nivel departamental. El uso de productos no autorizados podrá dar lugar a responsabilidades derivadas de la legislación vigente en materia de competencia desleal, laboral, civil y penal.

14. Normas para la adquisición de productos de software

INFORMACIÓN DEL TERRITORIO proporcionará al personal las licencias de uso de lo que se considera software básico para el desempeño de su actividad profesional.

Cualquier adquisición de nuevos productos software para uso general deberá ser gestionada de forma centralizada por el departamento de sistemas, el cual tras su aprobación dotará presupuestariamente para poder realizar esta compra.

15. Política de instalación de software

La instalación de cualquier software tiene que ser realizada por el departamento de sistemas y aprobada previamente por su responsable y posteriormente autorizada por el director de informática, comprando previamente las licencias correspondientes.

INFORMACIÓN DEL TERRITORIO permite cualquier tipo de programas para la consecución de las tareas del ámbito laboral. No obstante, los programas y el software utilizado para cualquiera de las funciones en la empresa deben ajustarse a la legalidad y al cumplimiento de las leyes vigentes. Para más detalle sobre este tema véase el punto “Política sobre licencias de software y copyright”.

Para determinadas actividades involucradas con la comunicación y el envío de la información INFORMACIÓN DEL TERRITORIO establece una serie de servicios y plataformas que deben ser utilizadas convenientemente:

- Videoconferencia
  - Teams
  - Zoom
  - Meet
- Correo electrónico
  - Exchange
- Navegadores
  - Microsoft Edge (el uso de Internet Explorer queda restringido a los casos de determinados entes públicos que no admiten otro navegador. En cualquier otro caso queda prohibido.
  - Mozilla Firefox
  - Chrome
  - Opera

16. Seguridad de las comunicaciones

Por criterio general INFORMACIÓN DEL TERRITORIO ha destinado formas estandarizadas para la comunicación en la empresa, todas las comunicaciones del ámbito deben restringirse a los programas y las vías establecidas en este documento. Cualquier información que se traslade por otros medios y/o programas debe ser comunicada y autorizada por INFORMACIÓN DEL TERRITORIO.

17. Comunicación de los incidentes de seguridad

Es obligación de todos los usuarios de INFORMACIÓN DEL TERRITORIO comunicar al área de sistemas por medio de un mail.

Asimismo, debe informarse de inmediato sobre cualquier robo o pérdida de hardware o dispositivo móvil.

18. Acciones disciplinarias

El proceso disciplinario se llevará a cabo basándose en los requerimientos establecidos en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, y en el convenio colectivo de aplicación.

19. Política de control de acceso físico

Con carácter general, el acceso a las instalaciones de INFORMACIÓN DEL TERRITORIO, estará restringido al personal que realice su trabajo en las mismas.

Todos los visitantes son acompañados por personal de la organización durante la visita por las instalaciones en todo momento.

La organización dispondrá de zonas de acceso controlado y de zonas de acceso restringido. Las zonas de acceso controlado son áreas abiertas al personal de la organización, mientras que las zonas de acceso restringido están limitadas al personal de la organización que realice su trabajo en las mismas o a quienes se les haya aprobado el acceso de forma expresa. Las puertas de acceso a todo el recinto deberán permanecer siempre cerradas.

20. Políticas y procedimientos de intercambio de información

Se establecen políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

- Protección de la información confidencial intercambiada, mediante los permisos de acceso.
- Definición de responsabilidades para los activos información, concienciación del personal sobre la seguridad de la información y acuerdos de confidencialidad.
- Concienciación del personal en evitar mantener conversaciones confidenciales en lugares públicos, oficinas o salas de reuniones abiertas.
- Se controla no dejar información confidencial o crítica en medios impresos al alcance de personas no autorizadas a su acceso.
- Se controla no dejar mensajes conteniendo información confidencial en contestadores automáticos; ni almacenados en sistemas comunitarios.

21. Transporte de soportes de información

Toda información clasificada o de carácter sensible deberá trasladarse utilizando canales y soportes protegidos, garantizando en todo momento su confidencialidad, integridad y trazabilidad. Se priorizará el uso de mecanismos de cifrado robustos en las comunicaciones electrónicas, así como contenedores y dispositivos físicos debidamente protegidos frente a accesos no autorizados, pérdida o manipulación. El personal implicado en estas actividades deberá estar expresamente autorizado, instruido en los procedimientos vigentes y registrar cada operación de transporte, incluyendo origen,

destino, fecha, hora y responsable de la custodia durante el trayecto, de manera que pueda reconstruirse la cadena completa de movimientos de la información en caso de incidente o auditoría.

22. Custodia de soportes de información

Se establecerán procedimientos formales que definan las condiciones de almacenamiento seguro, los controles de acceso físico y lógico, y las responsabilidades de los custodios designados. Los soportes que contengan datos sensibles deberán permanecer en áreas controladas, con acceso restringido y registrado, aplicando medidas de protección frente a robo, extravío, degradación o destrucción no autorizada, incluyendo la correcta gestión de copias de seguridad. Cualquier transferencia de custodia entre personas u organizaciones deberá documentarse explícitamente, indicando el estado del soporte, las medidas de protección asociadas y los compromisos de uso, conservación y devolución o destrucción segura al finalizar la relación o cuando deje de ser necesaria su conservación.