Normas de Uso de Sistemas de Información para Proveedores

Historial de Versiones

Fecha	Versión	Elaborado por	Descripción de cambios
09/02/2026	1.0	Javier Bermejo	Primera Versión

Información del documento

Nombre	Normas de Uso de Sistemas de Información para Proveedores
Versión	1.0
Creado por	Javier Bermejo
Aprobado por	

NORMAS DE USO DE SISTEMAS DE INFORMACIÓN EN DANOBATGROUP PARA PROVEEDORES

1. OBJETO Y ÁMBITO DE APLICACIÓN

1.1. El presente documento tiene por objeto establecer las condiciones generales de acceso, uso, custodia y seguridad de los sistemas de información, redes, plataformas digitales y equipos de DANOBATGROUP por parte de los proveedores que, en el marco de una relación contractual o comercial, necesiten acceder a dichos sistemas o tratar información del Grupo.

1.2. Estas normas se aplican a todas las sociedades integrantes de DANOBATGROUP (en adelante, "DANOBATGROUP") y resultan obligatorias para cualquier proveedor, subcontratista o tercero autorizado (en adelante, el "PROVEEDOR") que, directa o indirectamente, acceda, almacene, procese o gestione información, datos, software o infraestructuras tecnológicas propiedad de DANOBATGROUP.

1.3. Las presentes normas son de aplicación con independencia del canal o medio de acceso utilizado, incluyendo, entre otros, la Extranet de proveedores, la plataforma electrónica de compras (SRM), conexiones VPN, sistemas ERP, correo electrónico corporativo, aplicaciones internas, herramientas de colaboración o futuras plataformas digitales que puedan implantarse.

1.4. La aceptación del presente documento constituye condición indispensable para la concesión o mantenimiento de los permisos de acceso a los sistemas de información de DANOBATGROUP, y su incumplimiento podrá dar lugar a la suspensión inmediata de los accesos y a la adopción de medidas contractuales o legales.

2. IDENTIFICACIÓN DE LAS PARTES

- DANOBATGROUP, S. COOP., con domicilio en Arriaga Kalea, 20, Elgoibar Guipúzcoa, España, titular de los sistemas de información y responsable de su gestión.
- El PROVEEDOR, persona jurídica o física que mantiene relaciones comerciales o contractuales con cualquiera de las empresas de DANOBATGROUP y que accede, por sí o a través de su personal o subcontratistas, a dichos sistemas.

3. PRINCIPIOS GENERALES Y OBLIGACIONES DEL PROVEEDOR

3.1. El PROVEEDOR se compromete a cumplir en todo momento con la "Política de Seguridad de la Información de Danobatgroup", así como con la normativa vigente aplicable, incluyendo el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018, la Ley 11/2022 General de Telecomunicaciones y las normas derivadas de la ISO/IEC 27001 y 27002.

3.2. El PROVEEDOR será responsable de que su personal, subcontratistas o colaboradores cumplan igualmente las obligaciones establecidas en este documento.

3.3. El acceso a los sistemas se concederá bajo el principio de privilegio mínimo, de forma que únicamente se habilitarán los permisos estrictamente necesarios para el desempeño de las tareas asignadas.

3.4. El PROVEEDOR se obliga a utilizar los sistemas de información con buena fe, diligencia y finalidad legítima, evitando cualquier uso indebido, ilícito o contrario a los intereses de DANOBATGROUP.

4. CREDENCIALES Y CONTROL DE ACCESO

4.1. Las credenciales de acceso (usuario, contraseña o certificado digital) serán personales e intransferibles. El PROVEEDOR será plenamente responsable de su custodia y uso.

4.2. Queda expresamente prohibido compartir credenciales, utilizar las de otro usuario o emplearlas para acceder a información o sistemas no autorizados.

4.3. El PROVEEDOR se compromete a cambiar la contraseña con la periodicidad que indique DANOBATGROUP y a comunicar de inmediato cualquier sospecha de compromiso o pérdida de sus credenciales.

4.4. Cualquier alta, baja o modificación de accesos deberá ser solicitada y gestionada a través de los canales definidos por el departamento de IT de DANOBATGROUP.

4.5. DANOBATGROUP podrá suspender o revocar, en cualquier momento y sin previo aviso, los permisos de acceso por motivos de seguridad, finalización de contrato, incumplimiento o por cambios en la organización del servicio.

5. USO DE EQUIPOS Y DISPOSITIVOS CORPORATIVOS

5.1. Los equipos (portátiles, ordenadores de sobremesa, teléfonos móviles o tablets) que DANOBATGROUP entregue o ponga a disposición del PROVEEDOR son de uso exclusivo para fines profesionales vinculados a los servicios contratados.

5.2. Se prohíbe expresamente:

- Instalar software no autorizado o sin licencia.
- Conectar dispositivos externos sin validación previa (USB, discos duros, etc.).
- Modificar configuraciones de seguridad o intentar obtener privilegios de administrador.
- Acceder a contenidos o servicios que puedan comprometer la seguridad de la red (Dark Web, torrents, etc.).

5.3. DANOBATGROUP podrá instalar herramientas de **gestión remota, inventariado, cifrado, EDR, antivirus corporativo o MDM** con el fin de controlar la seguridad, realizar actualizaciones, aislar equipos comprometidos y garantizar la trazabilidad de las acciones.

5.4. El PROVEEDOR no dispondrá de permisos de administrador local salvo autorización escrita.

5.5. Los equipos deberán mantenerse físicamente protegidos (bloqueo de sesión en ausencias, almacenamiento seguro fuera del horario laboral, prohibición de uso compartido).

5.6. En caso de pérdida, robo o deterioro del equipo, el PROVEEDOR deberá notificarlo inmediatamente al departamento de IT o mediante correo a **zibersegurtasuna@danobatgroup.com**.

6. ACCESOS REMOTOS Y CONEXIONES EXTERNAS

6.1. Los accesos remotos deberán realizarse exclusivamente mediante VPN corporativa u otros mecanismos cifrados aprobados por DANOBATGROUP.

6.2. Los equipos desde los que se establezca la conexión deberán contar con antivirus actualizado, cortafuegos activo, parches de seguridad al día y configuración de red protegida.

6.3. Queda prohibido conectarse desde redes públicas o no seguras (por ejemplo, wifi abiertas de aeropuertos o cafeterías) sin emplear una VPN.

6.4. El PROVEEDOR no podrá instalar ni utilizar herramientas de acceso remoto (TeamViewer, AnyDesk, etc.) sin autorización expresa y escrita.

7. GESTIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN

7.1. Toda la información y documentación propiedad de DANOBATGROUP deberá almacenarse en las unidades de red, servidores o plataformas oficiales designadas para cada proyecto.

7.2. No se permite la copia, traslado o almacenamiento de información corporativa en dispositivos personales, servicios de nube pública o soportes externos no autorizados.

7.3. DANOBATGROUP no será responsable de la pérdida o destrucción de datos almacenados fuera de sus entornos autorizados.

7.4. Los datos e información generados o tratados por el PROVEEDOR en el marco de su relación con DANOBATGROUP tendrán carácter confidencial y pertenecerán exclusivamente a DANOBATGROUP.

7.5. A la finalización del contrato o servicio, el PROVEEDOR deberá devolver o eliminar toda la información y documentación que obre en su poder, sin conservar copia alguna, salvo obligación legal de conservación.

8. CONFIDENCIALIDAD

8.1. Se entenderá por “Información Confidencial” toda aquella información de carácter técnico, comercial, financiero, operativo, estratégico o de cualquier otra índole a la que

el PROVEEDOR tenga acceso como consecuencia de su relación con DANOBATGROUP, ya sea en soporte escrito, oral o electrónico.

8.2. El PROVEEDOR se obliga a:

- No divulgar ni comunicar la Información Confidencial a terceros sin autorización previa y escrita.
- Utilizarla exclusivamente para el cumplimiento de las obligaciones contractuales.
- Adoptar medidas razonables para evitar su pérdida, alteración o acceso no autorizado.

8.3. La obligación de confidencialidad se extenderá a todo el personal, subcontratistas o terceros implicados en la prestación del servicio.

8.4. La obligación de confidencialidad permanecerá vigente durante toda la relación contractual y durante un periodo mínimo de cinco (5) años tras su terminación.

9. PROTECCIÓN DE DATOS PERSONALES

9.1. Si el PROVEEDOR accede a datos personales responsabilidad de DANOBATGROUP, actuará como Encargado del Tratamiento, debiendo suscribir el correspondiente acuerdo regulador conforme al artículo 28 del RGPD.

9.2. El PROVEEDOR únicamente tratará los datos personales conforme a las instrucciones documentadas de DANOBATGROUP, quedando prohibido su uso para fines propios o cesión a terceros.

9.3. El PROVEEDOR garantizará la aplicación de medidas técnicas y organizativas adecuadas que aseguren la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales tratados.

9.4. En caso de violación de la seguridad de los datos personales, el PROVEEDOR deberá comunicarlo de inmediato a DANOBATGROUP, y en todo caso dentro de las 24 horas siguientes a su detección.

9.5. A la finalización de la relación contractual, el PROVEEDOR deberá eliminar o devolver los datos personales y cualquier copia, acreditando documentalmente su destrucción.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD

10.1. El PROVEEDOR deberá implantar procedimientos internos de detección, notificación y gestión de incidentes de seguridad que afecten a sistemas o información de DANOBATGROUP.

10.2. Cualquier incidente deberá ser comunicado de forma inmediata y sin dilación a la dirección de correo zibersegurtasuna@danobatgroup.com, indicando:

- Fecha y hora de detección.
- Naturaleza del incidente.

- Sistemas o información afectados.
- Medidas adoptadas de contención y mitigación.

10.3. El PROVEEDOR será responsable de ejecutar las acciones de corrección y contención necesarias para evitar la propagación o impacto del incidente y deberá remitir un informe completo de resolución en un plazo máximo de 72 horas.

10.4. DANOBATGROUP podrá exigir evidencias o auditorías adicionales derivadas del incidente.

11. AUDITORÍAS Y VERIFICACIONES DE CUMPLIMIENTO

11.1. DANOBATGROUP podrá, directamente o mediante terceros designados, realizar auditorías periódicas o puntuales sobre los procedimientos de seguridad del PROVEEDOR para verificar el cumplimiento del presente documento.

11.2. El PROVEEDOR se compromete a colaborar plenamente, facilitando el acceso a la información, documentación y evidencias necesarias.

11.3. DANOBATGROUP podrá requerir la corrección de deficiencias detectadas, debiendo el PROVEEDOR implementar las acciones correctivas en los plazos que se le indiquen.

12. RESPONSABILIDAD Y SANCIONES

12.1. El PROVEEDOR será responsable de los daños y perjuicios directos o indirectos que su incumplimiento cause a DANOBATGROUP, incluyendo pérdidas económicas, sanciones administrativas o daños reputacionales.

12.2. El incumplimiento de las presentes normas podrá suponer la suspensión inmediata de los accesos, la resolución del contrato y/o la reclamación de daños y perjuicios.

12.3. DANOBATGROUP no será responsable de los daños ocasionados por el uso indebido de los sistemas o por actuaciones negligentes del PROVEEDOR.

13. DURACIÓN Y VIGENCIA

13.1. Las presentes normas serán de aplicación desde la fecha de su aceptación por el PROVEEDOR y permanecerán en vigor durante toda la relación contractual y mientras el PROVEEDOR mantenga accesos activos a los sistemas de DANOBATGROUP.

13.2. DANOBATGROUP podrá modificar las presentes normas en cualquier momento, notificando las actualizaciones a los proveedores afectados o publicándolas en las plataformas oficiales. La continuación en el uso de los sistemas implicará su aceptación.

14. LEGISLACIÓN APLICABLE Y JURISDICCIÓN

El presente documento se regirá e interpretará conforme a la legislación española. Para la resolución de cualquier controversia derivada del mismo, las partes se someten

expresamente a los Juzgados y Tribunales de Éibar, con renuncia a cualquier otro fuero que pudiera corresponderles.

15. ACEPTACIÓN

El PROVEEDOR declara haber leído, comprendido y aceptado íntegramente las presentes Normas de Uso de Sistemas de Información en Danobatgroup, comprometiéndose a su cumplimiento y al de su personal, colaboradores y subcontratistas.

Sello/Nombre, Fecha y Firma del proveedor