## Ciberseguridad Ampliada Para Todas las Cosas de la Vida

**Oruss.com & Cía. Ltda. ®**

Colombia, Bogotá
Calle 93 11 a 63
+57-639-5000

Portugal Lisboa
Rua José Augusto Seabra
nº17B, Esc. C 1500-675
+351-913 943 714

Francia, Paris
140 bis Rue de Rennes,
75006

www.grupooruss.com

El Grupo Oruss es una compañía formada por expertos en proveer servicios de ciberseguridad y seguridad digital. Especialistas en hacking ético, análisis de vulnerabilidades, pruebas de intrusión y operaciones especiales informáticas con el objetivo principal de fortalecer las defensas tecnológicas en su organización.

Contamos con 24 años de experiencia que representan solidez, experiencia y efectividad teniendo como objetivo principal asegurar su compañía.

# Cultura Operativa Grupo Oruss

Trabajo inteligente, confidencialidad y operación remota segura

## Sobre el trabajo seguro, remoto, eficiente y orientado a resultados.

| | |
|---|---|
| **Nombre del documento** | Cultura Operativa Grupo Oruss |
| **Propósito** | En Grupo Oruss entendemos que la confianza se construye con claridad. Este documento de Cultura Operativa presenta los principios que orientan nuestra forma de trabajar, colaborar, proteger la información y cuidar a nuestro equipo. Se definir la forma de trabajo, colaboración, confidencialidad, acceso remoto seguro y uso responsable de recursos. |
| **Alcance** | Empleados, colaboradores, consultores, aliados, proveedores y terceros que participen en actividades de Grupo Oruss o sus clientes. |
| **Horario principal** | Lunes a viernes, de 9:00 a.m. a 4:00 p.m. hora Colombia, con ajustes previamente aprobados para ventanas de clientes, proyectos internacionales o actividades críticas. |
| **Modelo de operación** | Trabajo remoto, cultura de alto desempeño, seguridad por diseño, BYOD controlado y acceso mediante agentes Zero Trust o mecanismos equivalentes aprobados. |
| **Versión** | Versión 8.1 \| junio de 2026 |

**Nota de uso**

Este documento presenta lineamientos culturales y operativos. No sustituye contratos, acuerdos de confidencialidad, políticas legales, reglamento interno de trabajo, políticas de tratamiento de datos ni disposiciones laborales aplicables. Cuando exista conflicto entre documentos, prevalecerá el instrumento legal, contractual o regulatorio correspondiente.

*Documento cultural-operativo para empleados, colaboradores, aliados y contratistas*

## Mapa del documento

Este documento está diseñado para ser claro, práctico y reutilizable. Puede funcionar como guía interna y como base para una versión resumida publicable en el sitio web de Grupo Oruss.

# 1 Declaración cultural y propósito

Grupo Oruss opera bajo una cultura de ciberseguridad ampliada, trabajo inteligente y confianza responsable. Nuestro modelo de trabajo remoto no es una concesión operativa: es una decisión estratégica para atraer talento, optimizar recursos, proteger la información y entregar servicios especializados con alta claridad técnica y ejecutiva.

La Cultura Operativa Grupo Oruss define cómo trabajamos, cómo colaboramos, cómo cuidamos la confidencialidad de nuestros clientes y cómo usamos la tecnología para mantener una operación boutique, eficiente, segura y a la vanguardia.

**Idea central**

Trabajamos con libertad operativa, pero bajo disciplina de seguridad. La flexibilidad existe porque hay confianza, trazabilidad, criterio profesional y responsabilidad sobre la información.

### Objetivos del documento

Alinear a empleados, colaboradores, aliados y contratistas sobre la forma de trabajo de Grupo Oruss.
Definir horarios, disponibilidad, canales de comunicación y criterios de coordinación remota.
Establecer lineamientos de confidencialidad, manejo de información y protección de evidencias.
Regular el uso de dispositivos personales bajo un enfoque BYOD seguro y verificable.
Formalizar el uso de acceso remoto seguro mediante agentes Zero Trust o mecanismos equivalentes aprobados.
Promover una cultura de eficiencia, documentación, mejora continua y alto desempeño.
Mostrar, de forma publicable, cómo Grupo Oruss optimiza recursos y opera con estándares modernos de ciberseguridad.

# 2 Principios de cultura operativa

| Principio | Descripción |
|---|---|
| **Seguridad por diseño** | Toda actividad se planifica considerando autorización, confidencialidad, trazabilidad, mínimo privilegio y protección de datos. |
| **Trabajo por resultados** | El desempeño se mide por cumplimiento, calidad, claridad, oportunidad y valor entregado, no por presencialismo digital. |
| **Confianza verificable** | La confianza se acompaña de controles: autenticación fuerte, registro de accesos, documentación, revisión y mejora continua. |
| **Cero papel cuando sea posible** | Se prioriza la documentación digital, la firma electrónica, repositorios controlados y flujos que reduzcan fricción administrativa. |
| **Eficiencia elegante** | Usamos automatización, plantillas, dashboards y reutilización de conocimiento para liberar tiempo del equipo y mejorar la experiencia del cliente. |
| **Claridad ejecutiva** | Los entregables deben ser comprensibles para audiencias técnicas y de negocio, con riesgos, impacto y próximos pasos bien definidos. |
| **Ética profesional** | La actividad de seguridad ofensiva se realiza únicamente con autorización, alcance definido y respeto por personas, sistemas, datos y clientes. |

Estos principios deben aplicarse en decisiones diarias: desde cómo se agenda una reunión hasta cómo se protege una evidencia crítica de un ejercicio de pentesting.

# 3 Horario de trabajo y disponibilidad

El horario principal de trabajo de Grupo Oruss es de lunes a viernes, de 9:00 a.m. a 4:00 p.m., tanto en la base principal América como la Unión Europa. Este bloque concentra la coordinación operativa, atención interna, comunicación con clientes, seguimiento comercial, ejecución de tareas y revisión de entregables.

| | |
|---|---|
| **Horario principal** | 9:00 a.m. a 4:00 p.m de lunes a viernes. |
| **Modalidad** | Remota, con coordinación digital y disponibilidad responsable durante el horario definido. |
| **Pausas y enfoque** | Se promueven pausas razonables, bloques de concentración y organización de tareas por prioridad. |

| | |
|---|---|
| **Ventanas especiales** | Las pruebas nocturnas, actividades en horarios de clientes internacionales, respuesta a incidentes o ventanas críticas deben ser aprobadas y coordinadas previamente. |
| **Disponibilidad extendida** | No se presume disponibilidad permanente fuera del horario principal, salvo acuerdos expresos por proyecto, incidente o contrato. |

### Criterios de disponibilidad

- Mantener canales acordados activos durante el horario principal: correo, mensajería corporativa, gestor de proyectos o herramientas equivalentes
- Responder comunicaciones críticas con prioridad, especialmente cuando involucren cliente, continuidad operativa, incidentes o entregables próximos.
- Informar ausencias, bloqueos operativos o cambios de disponibilidad con anticipación razonable.
- Respetar la planeación de ventanas técnicas, pruebas nocturnas o actividades fuera del horario habitual cuando hayan sido aceptadas por el equipo y el cliente.
- Evitar reuniones innecesarias cuando una actualización escrita, dashboard o checklist resuelva el objetivo con mayor eficiencia.

**Cuidado operativo**

El horario 9 a 4 funciona como un núcleo de coordinación. Para proyectos de ciberseguridad, puede existir trabajo técnico por ventanas específicas, siempre bajo autorización, trazabilidad y alcance definido.

## 4 Trabajo remoto, colaboración y productividad

Grupo Oruss adopta el trabajo remoto como un modelo de operación estratégico. Esto permite reducir desplazamientos, optimizar costos, mejorar la concentración técnica, ampliar la disponibilidad de talento y mantener una operación ágil para clientes en distintas geografías.

### Lineamientos del trabajo remoto

- Cada persona debe contar con un entorno de trabajo adecuado, privado y con conectividad suficiente para cumplir sus funciones.
- La información de clientes, evidencias, credenciales, reportes y datos internos no debe quedar expuesta a terceros, pantallas compartidas no autorizadas o conversaciones en espacios públicos.
- Las reuniones deben tener objetivo, responsables, decisiones y próximos pasos. El tiempo del equipo es un recurso estratégico.
- Las tareas deben quedar documentadas en las herramientas aprobadas, evitando depender únicamente de conversaciones informales.
- La productividad se mide por entregables, cumplimiento, calidad, documentación y valor generado para el cliente.
- Se promueve el uso de plantillas, automatización, checklists y dashboards para estandarizar tareas repetibles.

### Rituales mínimos sugeridos

| Ritual | Propósito |
|---|---|
| **Inicio de semana** | Revisión de prioridades, proyectos activos, riesgos, entregables y necesidades comerciales. Ejercicios de mindfulness, Tinnitus Relief y sugeridos por el equipo de salud neuropsicológica. |
| **Diario o por proyecto** | Actualización breve de avances, bloqueos, hallazgos relevantes y próximos pasos. |
| **Cierre de proyecto** | Revisión de aprendizajes, evidencias, oportunidades de mejora, activos reutilizables y posibles upsells. |
| **Mensual** | Revisión de eficiencia, plantillas, automatización, satisfacción del cliente y oportunidades comerciales. |

## 5 Acceso remoto seguro: BYOD y Zero Trust Agents

El acceso remoto en Grupo Oruss debe estar alineado con un enfoque de seguridad moderna: mínimo privilegio, autenticación fuerte, verificación continua, protección de dispositivos y segmentación del acceso según función, proyecto y necesidad real.

### Modelo BYOD controlado

BYOD significa que ciertos empleados o colaboradores pueden utilizar dispositivos propios para actividades autorizadas, siempre que cumplan requisitos mínimos de seguridad, configuración y trazabilidad. BYOD no significa acceso libre, informal o sin controles.

| Control BYOD | Expectativa |
|---|---|
| **Dispositivo autorizado** | El equipo debe estar identificado, actualizado y autorizado para actividades de Grupo Oruss o sus clientes. |
| **Sistema actualizado** | Debe contar con sistema operativo y software crítico al día, sin configuraciones inseguras conocidas. |
| **Cifrado y bloqueo** | Debe tener cifrado de disco, bloqueo automático, contraseña robusta y mecanismo biométrico seguro. |
| **Antimalware/EDR** | Debe contar con solución de seguridad activa, cuando aplique, y no presentar señales de compromiso. |
| **No jailbreak/root** | No se permiten dispositivos manipulados, rooteados, con jailbreak o con controles de seguridad deshabilitados. Eventualmente máquinas virtuales creadas y adaptadas. |
| **Separación de información** | La información corporativa y de clientes debe mantenerse en repositorios, perfiles o herramientas aprobadas. |
| **Uso no compartido** | El dispositivo usado para trabajo no debe ser compartido con terceros cuando exista acceso a información de Grupo Oruss o clientes. |

### Zero Trust Agents y acceso remoto

Cuando el acceso remoto a recursos, laboratorios, repositorios, ambientes de cliente o plataformas internas lo requiera, se utilizarán agentes Zero Trust, ZTNA, VPN segura, SSO, MFA, controles de postura del dispositivo o mecanismos equivalentes aprobados por Grupo Oruss.

- Todo acceso debe estar asociado a una identidad individual, no compartida.
- El acceso debe otorgarse bajo mínimo privilegio y solo durante el tiempo necesario.
- Los accesos a ambientes de cliente deben respetar alcance, ventanas, credenciales, restricciones y autorizaciones acordadas.
- Las credenciales deben almacenarse en herramientas aprobadas; no deben compartirse por chats abiertos, correos no protegidos o documentos sin control.
- Los agentes Zero Trust o mecanismos equivalentes no deben ser desinstalados, evadidos, deshabilitados o alterados sin aprobación.
- Toda anomalía de acceso, pérdida de equipo, sospecha de compromiso o exposición de credenciales debe reportarse inmediatamente.

**Regla de oro del acceso remoto**

Ningún acceso remoto debe depender únicamente de la ubicación, confianza previa o comodidad operativa. La identidad, el dispositivo, el contexto y la necesidad deben validarse continuamente.

# 6 Confidencialidad, clasificación y manejo de información

La confidencialidad es un principio esencial de Grupo Oruss. Nuestro trabajo puede involucrar información sensible de clientes, vulnerabilidades, evidencias, credenciales, arquitectura, datos personales, contratos, estrategias comerciales y hallazgos técnicos que deben protegerse con el máximo cuidado.

## Clasificación de información

| Clasificación | Descripción |
|---|---|
| **Pública** | Información aprobada para sitio web, redes sociales, comunicados o materiales comerciales. |
| **Interna** | Información operativa de Grupo Oruss que no debe circular fuera del equipo o aliados autorizados. |
| **Confidencial** | Información de clientes, propuestas, contratos, metodologías, reportes, evidencias, accesos, hallazgos o datos comerciales sensibles. |
| **Restringida / Crítica** | Credenciales, llaves, tokens, datos personales, evidencias explotables, información regulada, datos de incidentes o material que pueda causar impacto si se divulga. |

## Obligaciones de confidencialidad

- Cumplir a cabalidad los NDA y las directrices realizadas por Grupo Oruss.
- No divulgar información interna, confidencial o restringida sin autorización expresa.
- No compartir nombres de clientes, hallazgos, evidencias o resultados de pruebas como material comercial.
- No reutilizar evidencias reales en presentaciones, redes, capacitaciones o contenidos públicos sin anonimización y autorización.
- No almacenar información sensible en dispositivos, nubes personales, repositorios no aprobados o canales informales.
- No capturar pantallas, grabar reuniones o copiar información sensible sin justificación operativa y autorización cuando aplique.
- Reiteramos cumplir acuerdos de confidencialidad, contratos, NDA, políticas de clientes y restricciones específicas de cada proyecto.
- Aplicar criterio profesional: si existe duda sobre si algo puede compartirse, debe tratarse como confidencial hasta recibir autorización.

## Manejo de evidencias de ciberseguridad

Las evidencias de pentesting, ingeniería social, análisis de aplicaciones, APIs, móviles, infraestructura, cloud, SCADA/OT o investigaciones OSINT deben conservarse solo en los repositorios autorizados, con nomenclatura clara, acceso restringido y ciclo de retención definido por proyecto o contrato.

| Etapa | Lineamiento |
|---|---|
| **Captura** | Tomar únicamente la evidencia necesaria para demostrar riesgo, impacto y reproducibilidad. |
| **Almacenamiento** | Guardar en repositorios aprobados con control de acceso y trazabilidad. |
| **Anonimización** | Ocultar datos personales, secretos o información innecesaria cuando la evidencia se use en entregables ejecutivos. |
| **Transferencia** | Usar canales aprobados y evitar envíos no cifrados cuando el contenido sea sensible. |
| **Retención** | Conservar según contrato, política interna o requerimiento del cliente; eliminar o archivar de forma segura cuando corresponda. |

# 7 Uso responsable de recursos, herramientas e inteligencia artificial

Grupo Oruss optimiza sus recursos mediante trabajo remoto, cero papel, automatización, documentación reutilizable, herramientas colaborativas y uso responsable de inteligencia artificial. Esta eficiencia debe fortalecer la calidad, nunca debilitar la seguridad o la confidencialidad.

## Herramientas y recursos tecnológicos

- Utilizar únicamente herramientas autorizadas o aceptadas para proyectos, comunicaciones, gestión documental y pruebas técnicas.
- Mantener licencias, accesos y herramientas bajo uso profesional y conforme a los términos permitidos
- Evitar duplicidad de archivos, versiones paralelas o información dispersa fuera de los repositorios definidos.
- Reportar oportunamente necesidades de recursos, herramientas, automatizaciones o mejoras de proceso.
- Proteger credenciales, llaves API, tokens, certificados, VPN, agentes de acceso y secretos técnicos.

## Uso responsable de inteligencia artificial

La inteligencia artificial puede apoyar redacción, análisis, clasificación, generación de ideas, automatización, revisión de calidad y productividad. Su uso debe respetar confidencialidad, propiedad intelectual, protección de datos y seguridad de la información.

| Criterio | Lineamiento |
|---|---|
| **Permitido** | Usar IA para estructurar ideas, mejorar redacción, crear plantillas, resumir información no sensible o apoyar automatización autorizada. |
| **Con control** | Usar IA con información interna o de cliente solo cuando exista herramienta aprobada, configuración adecuada, anonimización o autorización. |
| **No permitido** | Ingresar credenciales, tokens, datos personales, evidencias explotables, código sensible, información regulada o datos confidenciales en herramientas públicas no aprobadas. |
| **Validación humana** | Todo resultado generado por IA debe ser revisado por una persona responsable antes de enviarse a clientes o usarse en decisiones críticas. |

# 8 Comunicación, reuniones y documentación

La comunicación en Grupo Oruss debe ser clara, respetuosa, documentada y orientada a la acción. Una operación remota madura necesita menos ruido y más trazabilidad.

## Canales de comunicación

| Canal | Uso esperado |
|---|---|
| **Correo corporativo** | Comunicaciones formales, clientes, propuestas, aprobaciones, envíos oficiales y confirmaciones relevantes. |
| **Gestor de proyectos** | Tareas, responsables, fechas, estados, bloqueos, entregables y trazabilidad operativa. |
| **Mensajería corporativa** | Coordinación ágil, alertas, consultas breves y seguimiento inmediato. |
| **Repositorios autorizados** | Documentos, evidencias, plantillas, reportes, versiones y materiales de trabajo. |
| **Reuniones virtuales** | Alineación, decisiones, revisión de entregables, incidentes o temas que requieran interacción directa. |

## Buenas prácticas

- Toda reunión debe tener objetivo, asistentes necesarios, duración razonable y próximos pasos.
- Las decisiones relevantes deben quedar documentadas en correo, acta breve, tarea o comentario del proyecto.
- Evitar comunicaciones ambiguas; indicar responsable, fecha, prioridad y resultado esperado.
- Separar lo urgente de lo importante: no todo mensaje requiere interrupción inmediata.
- Usar lenguaje profesional, cordial y cuidadoso, especialmente en conversaciones con clientes y aliados.
- Mantener coherencia de marca: claridad, precisión, confianza, elegancia y orientación a solución.

# 9 Proyectos de ciberseguridad y ética profesional

Grupo Oruss realiza actividades de ciberseguridad ofensiva, consultoría, auditoría, análisis técnico bajo autorización, estudios neurológicos asociados a las reacciones relacionadas con comportamientos neuro-digitales con un alcance definido con criterios profesionales La confianza del cliente depende tanto de la calidad técnica como de la disciplina operativa.

## Reglas mínimas para actividades técnicas

- No ejecutar pruebas, explotación, escaneo intrusivo, ingeniería social o acceso a sistemas sin autorización expresa y alcance definido.
- Verificar fechas, ventanas, direcciones IP, dominios, credenciales, limitaciones y contactos de emergencia antes de iniciar actividades.
- Respetar restricciones del cliente, reglas de engagement, exclusiones, límites de impacto y condiciones de reporte.
- Documentar hallazgos con evidencia suficiente, reproducibilidad, impacto, criticidad, recomendación y referencias cuando aplique.
- Evitar acciones destructivas, persistencia innecesaria, extracción excesiva de datos o interrupción de servicios sin autorización explícita.
- Reportar de inmediato cualquier hallazgo crítico, exposición sensible, acceso no previsto o riesgo de alto impacto.
- No utilizar información obtenida en proyectos para beneficio personal, investigación no autorizada o divulgación pública.
- Todo proyecto de investigación se tratará como secreto industrial, hasta que se defina como diferente, comunicado debidamente a los participantes.

## Calidad de entregables

| Nivel | Criterio de calidad |
|---|---|
| **Técnico** | Evidencias claras, pasos de reproducción, vectores, impacto, CVSS/CWE/CVE cuando aplique y remediación verificable. |
| **Ejecutivo** | Lenguaje claro, impacto de negocio, priorización, riesgo residual, tendencia y recomendación accionable. |
| **Operativo** | Estado, responsables, fechas, re-test, trazabilidad de remediación y seguimiento. |
| **Comercial** | Identificación responsable de oportunidades de mejora, servicios complementarios o continuidad sin alarmismo ni presión indebida. |

# 10 Bienestar, desconexión y cuidado del equipo

Una operación de alto desempeño necesita cuidar la energía, la concentración y la salud del equipo. Grupo Oruss promueve una cultura exigente, pero humana: orientada a resultados, respeto, claridad y sostenibilidad.

- Respetar el horario ideal y evitar normalizar comunicaciones fuera de horario, salvo urgencias o acuerdos previamente definidos como las comunicaciones vía correo sin exigencia de respuesta inmediata.
- Promover pausas, bloques de enfoque, ejercicios mindfulness, tinnitus relief, dispositivos de ruido blanco, dispositivos “health wearables”, planificación realista de entregables.
- Evitar la sobrecarga por reuniones innecesarias, cambios de prioridad sin contexto o solicitudes ambiguas.
- Tratar a compañeros, clientes y aliados con respeto, profesionalismo y consideración. Todos somos iguales.
- Reportar tensiones operativas, riesgos de sobrecarga o burnout, bloqueos o necesidades de apoyo antes de que escalen.
- Favorecer una cultura de aprendizaje: errores, hallazgos y fricciones deben convertirse en mejoras de proceso.

En Grupo Oruss promovemos una cultura profesional basada en el respeto, la dignidad, la colaboración y la igualdad de trato. Valoramos a las personas por su ética, talento, criterio, desempeño, compromiso y capacidad par contribuir a un entorno seguro, confiable y de alto desempeño. Las creencias, convicciones, identidad, origen, orientación, condiciones personales y formas de pensamiento pertenecen al ámbito privado de cada persona. Por ello, no exigimos revelar información personal sensible ni aceptamos conductas de exclusión, burla, presión, hostigamiento o trato desfavorable por razones ajenas al trabajo, al mérito profesional o al cumplimiento de responsabilidades.

- Nuestra convivencia se basa en un principio simple: todas las personas deben ser tratadas con respeto, profesionalismo y consideración. La diversidad de experiencias, miradas y talentos fortalece nuestra capacidad de aprender, resolver problemas, innovar y proteger mejor a nuestros clientes.

**Cultura de cuidado**

La eficiencia no debe confundirse con prisa permanente. Un equipo unido y protegido piensa mejor, documenta mejor y entrega mejor.

# 11 Gestión de incidentes, excepciones y mejoras

## Reporte de incidentes o anomalías

Cualquier evento que pueda comprometer información, acceso, continuidad, reputación, disponibilidad o relación con clientes debe reportarse de inmediato al responsable interno correspondiente. Usar nuestro servicio de Inteligencia de Amenazas Cibernéticas como una autoevaluación es el paso esencial en la salud digital corporativa.

| Evento | Acción esperada |
|---|---|
| **Pérdida o robo de dispositivo** | Reportar inmediatamente, indicar equipo, accesos, hora estimada y posibles datos comprometidos. |
| **Credencial expuesta** | Revocar, rotar o solicitar bloqueo; documentar alcance y sistemas relacionados. |
| **Acceso no autorizado** | Suspender actividad, preservar evidencia y escalar al responsable designado. |
| **Error en prueba técnica** | Informar impacto, sistemas afectados, acciones realizadas y medidas de contención. |
| **Divulgación accidental** | Reportar destinatario, información compartida, canal usado y acciones de mitigación. |
| **Herramienta comprometida** | Aislar dispositivo o cuenta, suspender uso y activar revisión técnica. |

## Excepciones

Cualquier excepción a estos lineamientos debe estar justificada, aprobada y documentada. Las excepciones deben tener alcance limitado, responsable, duración definida y plan de cierre.

## Mejora continua

- Convertir incidentes, fricciones y aprendizajes en checklists, plantillas, automatizaciones o ajustes de proceso.
- Revisar periódicamente herramientas, accesos, repositorios y flujos de trabajo para reducir exposición y duplicidad.
- Identificar tareas repetibles que puedan convertirse en activos: guías, dashboards, scripts, plantillas o servicios empaquetables.
- Escuchar retroalimentación de clientes y equipo para mejorar claridad, tiempos, entregables y experiencia de servicio.
-

## 12 Gobierno, revisiones y aceptación

La Cultura Operativa Grupo Oruss debe ser revisada periódicamente para mantener coherencia con el crecimiento de la compañía, la evolución de amenazas, los requisitos de clientes y las mejores prácticas de operación remota segura. Nuestra cultura de confidencialidad se apoya en acuerdos, buenas prácticas y marcos regulatorios aplicables en Colombia, las Américas y la Unión Europea, de acuerdo con la naturaleza de cada proyecto, cliente o alianza.

| | |
|---|---|
| **Responsable sugerido** | Dirección / Operaciones / Seguridad de la Información. |
| **Frecuencia de revisión** | Al menos cada 6 meses o cuando existan cambios relevantes en operación, tecnología, clientes, regulación o riesgos. |
| **Gestión de cambios** | Toda modificación debe registrarse con versión, fecha, responsable y resumen del cambio. |
| **Aceptación** | Empleados, colaboradores, aliados y contratistas podrán confirmar lectura, comprensión y aceptación según corresponda. |

### Control de versiones

| Versión | Fecha | Descripción | Responsable |
|---|---|---|---|
| **8.1** | Junio de 2026 | Actualización del documento Cultura Operativa Grupo Oruss. | Dirección / Operaciones |

**Equipo de Cultura Corporativa.**

**Bogotá, Colombia**
**Calle 93 11 a 63**
**WhatsApp Américas: +57 333-6488961**

**Portugal, Lisbon**
**R. José Augusto Seabra n.º 17-B**
**WhatsApp Europa +351-935-181-287**

**Francia, Paris**
**140 bis Rue de Rennes, 75006**

comunicaciones@grupooruss.com
www.grupooruss.com
https://www.linkedin.com/in/grupoorussla

**Lo invitamos a visitar nuestro sitio web para obtener más información:**
**www.grupooruss.com**