FINALIDAD	La presente Política de Ciberseguridad tiene como finalidad establecer los lineamientos, controles, principios y responsabilidades necesarios para proteger la información, los activos tecnológicos, los sistemas digitales, las comunicaciones y la infraestructura tecnológica de Juva Group frente a amenazas internas o externas que puedan comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de la información corporativa. Asimismo, esta política busca prevenir incidentes de ciberseguridad, accesos no autorizados, pérdida de información, ataques informáticos, fraudes digitales, fuga de datos y cualquier actividad que represente un riesgo operativo, reputacional, financiero o legal para la organización, sus clientes, aliados comerciales y colaboradores.
ALCANCE	La presente política aplica de manera obligatoria para: • Todos los colaboradores, directivos, accionistas, contratistas, proveedores, freelancers, aliados estratégicos y terceros que tengan acceso a información o sistemas de Juva Group. • Todos los equipos tecnológicos corporativos o personales utilizados para actividades relacionadas con la organización. • Todas las plataformas digitales, sistemas informáticos, correos electrónicos corporativos, bases de datos, redes, servidores, aplicaciones, dispositivos móviles y herramientas tecnológicas utilizadas por la compañía. • Todas las operaciones nacionales e internacionales desarrolladas bajo las marcas, unidades de negocio o filiales de Juva Group. El cumplimiento de esta política será obligatorio independientemente de la modalidad de trabajo presencial, híbrida o remota.
IMPLEMENTACIÓN	Juva Group implementará medidas técnicas, administrativas y operativas orientadas a fortalecer la seguridad digital de la organización, incluyendo pero sin limitarse a: • Gestión segura de contraseñas y autenticación multifactor. • Restricción y control de accesos según roles y niveles de autorización. • Monitoreo continuo de amenazas y eventos de seguridad. • Copias de seguridad periódicas y planes de recuperación. • Protección antivirus, antimalware y firewalls corporativos. • Cifrado de información sensible y confidencial. • Capacitación periódica en ciberseguridad y prevención de fraudes digitales. • Protocolos de respuesta ante incidentes de seguridad informática. • Evaluación periódica de vulnerabilidades y riesgos tecnológicos. • Políticas de uso adecuado de dispositivos, internet y correos corporativos. La Gerencia y las áreas responsables podrán actualizar, modificar o fortalecer los mecanismos de seguridad cuando las condiciones tecnológicas, regulatorias o de riesgo así lo requieran.
LEYES APLICABLES	Colombia • Ley 1273 de 2009 — Protección de la información y de los datos. • Ley 1581 de 2012 — Protección de Datos Personales. • Decreto 1377 de 2013. • Ley 1266 de 2008. • Código Penal Colombiano en materia de delitos informáticos. Normativa y estándares internacionales de referencia • Reglamento General de Protección de Datos (GDPR) — Unión Europea. • ISO/IEC 27001 — Sistemas de Gestión de Seguridad de la Información. • NIST Cybersecurity Framework. • Buenas prácticas internacionales de seguridad digital y gestión de riesgos tecnológicos.

NORMAS CORP. APLICABLES	a) Código Corporativo. b) Directrices Corporativas. c) Lineamientos de la Certificación MECEI360°.
DICCIONARIO	• Activo digital: Cualquier recurso tecnológico o información con valor para la organización. • Ciberseguridad: Conjunto de prácticas, tecnologías y procesos destinados a proteger sistemas, redes y datos frente a amenazas digitales. • Dato sensible: Información que puede afectar la privacidad o seguridad de una persona o de la organización. • Incidente de seguridad: Evento que compromete o puede comprometer la seguridad de la información o los sistemas. • Phishing: Técnica de fraude digital utilizada para obtener información confidencial mediante engaños. • Malware: Software malicioso diseñado para afectar, dañar o infiltrarse en sistemas informáticos. • Acceso no autorizado: Ingreso a sistemas, plataformas o información sin permiso válido. • Autenticación multifactor (MFA): Método de verificación que requiere múltiples formas de autenticación para acceder a un sistema.
PRINCIPIOS	Juva Group adopta los siguientes principios fundamentales: • Confidencialidad: La información sólo podrá ser accesible por personas autorizadas. • Integridad: Los datos deberán mantenerse completos, precisos y protegidos contra alteraciones indebidas. • Disponibilidad: Los sistemas y la información deberán estar disponibles cuando sean requeridos. • Responsabilidad: Todo usuario será responsable del uso adecuado de los recursos tecnológicos asignados. • Prevención: La organización priorizará medidas preventivas frente a amenazas digitales. • Legalidad: Todas las actividades tecnológicas deberán desarrollarse conforme a la normativa vigente. • Trazabilidad: Toda actividad crítica podrá ser monitoreada, registrada y auditada.
PROHIBICIONES	Queda estrictamente prohibido: • Compartir contraseñas o credenciales de acceso. • Instalar software no autorizado por la organización. • Utilizar dispositivos corporativos para actividades ilícitas o personales no autorizadas. • Acceder, modificar, copiar o eliminar información sin autorización. • Descargar archivos sospechosos o ingresar a sitios inseguros. • Divulgar información confidencial de clientes, empleados o de la empresa. • Desactivar sistemas de protección o seguridad informática.

	• Realizar actos que puedan comprometer la estabilidad tecnológica de la organización. • Utilizar redes WiFi-inseguras para acceder a información corporativa sensible. • Suplantar identidades digitales o utilizar cuentas ajenas.
OBLIGACIONES	• Los dispositivos deben bloquearse al ausentarse del puesto de trabajo. • La información personal de candidatos, clientes y empleados debe almacenarse en plataformas seguras y autorizadas. • Queda prohibido descargar, copiar o transferir información sensible a dispositivos personales o unidades externas sin autorización. • Todos los correos, documentos y archivos que contengan datos sensibles deben estar cifrados o protegidos con contraseña. • Verificar siempre el remitente de un correo antes de responder o proporcionar información. En caso de recibir un correo de phishing, reenviar inmediatamente al área de soporte técnico y no interactuar con su contenido. • Todos los sistemas y aplicaciones deben mantenerse actualizados. • Responsabilidad de aplicar los parches de seguridad recomendados por los proveedores. • La empresa realizará respaldos automáticos de la información crítica de forma periódica. • Todos los colaboradores deberán guardar documentos importantes en las carpetas o nubes designadas por la empresa. • Todos los nuevos colaboradores deberán firmar un documento de cumplimiento de políticas y acuerdo de confidencialidad antes de recibir acceso a los sistemas.
SANCIONES POR INCUMPLIMIENTO	El incumplimiento de la presente Política de Ciberseguridad podrá generar medidas disciplinarias, civiles, contractuales y/o penales, dependiendo de la gravedad de la conducta. Las sanciones podrán incluir: a) Llamados de atención. b) Suspensión temporal de accesos y privilegios tecnológicos. c) Procesos disciplinarios internos. d) Terminación del contrato laboral o comercial. e) Acciones legales por daños y perjuicios. f) Reportes ante autoridades competentes en caso de delitos informáticos o violaciones legales. Juva Group se reserva el derecho de realizar auditorías, monitoreos y verificaciones sobre el uso de sus sistemas tecnológicos para garantizar el cumplimiento de esta política y la protección de sus activos digitales.
CANALES DE COMUNICACIÓN	Juva Group agradece y valora positivamente la comunicación de cualquier indicio o sospecha de violación de la legalidad por parte de cualquier miembro, persona u organización vinculada a nuestra compañía, por lo cual, agradecemos el mayor detalle posible en la exposición de los hechos denunciados/comunicados. Nuestra compañía ha dispuesto mecanismos y procesos internos seguros para garantizar la confidencialidad de las denuncias y comunicaciones recibidas, así como para proteger de cualquier tipo de amenaza o coacción a las personas que participen con nuestro objetivo de cumplimiento mediante la comunicación y denuncia. Para la máxima garantía de independencia, nuestra compañía ha designado a una empresa que vela por los Derechos Legales dentro de la compañía. **CANALES DISPONIBLES DE COMUNICACIÓN PARA QUEJAS/COMENTARIOS:** • Website: www.wearejuva.com/contact