



POLÍTICA DE CIBERSEGURIDAD

Protección de información, activos digitales e infraestructura tecnológica.

01	FINALIDAD Y ALCANCE Qué protege la política y a quién aplica
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.
PRINCIPIO DE SEGURIDAD JUVA Group establece controles orientados a proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información corporativa.	

MEDIDAS DE SEGURIDAD

Juva Group implementará medidas técnicas, administrativas y operativas orientadas a fortalecer la seguridad digital de la organización, incluyendo pero sin limitarse a:

- 2.1 Gestión segura de contraseñas y autenticación multifactor.
- 2.2 Restricción y control de accesos según roles y niveles de autorización.
- 2.3 Monitoreo continuo de amenazas y eventos de seguridad.
- 2.4 Copias de seguridad periódicas y planes de recuperación.
- 2.5 Protección antivirus, antimalware y firewalls corporativos.
- 2.6 Cifrado de información sensible y confidencial.
- 2.7 Capacitación periódica en ciberseguridad y prevención de fraudes digitales.
- 2.8 Protocolos de respuesta ante incidentes de seguridad informática.
- 2.9 Evaluación periódica de vulnerabilidades y riesgos tecnológicos.
- 2.10 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.

MFA Autenticación multifactor y gestión segura de contraseñas.	ACCESS Control de accesos por rol y autorización.	MONITOR Monitoreo de amenazas y eventos.
BACKUP Copias de seguridad y recuperación.	PROTECT Antivirus, antimalware, firewalls y cifrado.	TRAIN Capacitación y respuesta ante incidentes.

03		MARCO LEGAL Y CORPORATIVO	
		Leyes, estándares y normativa interna	
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.			
Leyes Aplicables en países operativos de Juva Group.			
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 CORPORATIVAS		Código Corporativo. Directrices Corporativas. Lineamientos de la Certificación MECEI360°.	
04		DICCIONARIO DE CIBERSEGURIDAD	
		Conceptos clave	
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.

05		PRINCIPIOS	
		Base de la seguridad de la información	
COMPROMISO			
Juva Group adopta los siguientes principios fundamentales:			
CONFIDENCIALIDAD		INTEGRIDAD	
La información sólo podrá ser accesible por personas autorizadas.		Los datos deberán mantenerse completos, precisos y protegidos contra alteraciones indebidas.	
DISPONIBILIDAD		RESPONSABILIDAD	
Los sistemas y la información deberán estar disponibles cuando sean requeridos.		Todo usuario será responsable del uso adecuado de los recursos tecnológicos asignados.	
PREVENCIÓN		LEGALIDAD	
La organización priorizará medidas preventivas frente a amenazas digitales.		Todas las actividades tecnológicas deberán desarrollarse conforme a la normativa vigente.	
TRAZABILIDAD			
Toda actividad crítica podrá ser monitoreada, registrada y auditada.			

PROHIBICIONES

Conductas expresamente no permitidas

TOLERANCIA CERO

Queda estrictamente prohibido:

- 6.1 Compartir contraseñas o credenciales de acceso.
- 6.2 Instalar software no autorizado por la organización.
- 6.3 Utilizar dispositivos corporativos para actividades ilícitas o personales no autorizadas.
- 6.4 Acceder, modificar, copiar o eliminar información sin autorización.
- 6.5 Descargar archivos sospechosos o ingresar a sitios inseguros.
- 6.6 Divulgar información confidencial de clientes, empleados o de la empresa.
- 6.7 Desactivar sistemas de protección o seguridad informática.
- 6.8 Realizar actos que puedan comprometer la estabilidad tecnológica de la organización.
- 6.9 Utilizar redes WiFi-inseguras para acceder a información corporativa sensible.
- 6.10 Suplantar identidades digitales o utilizar cuentas ajenas.

OBLIGACIONES DE USUARIOS Y COLABORADORES

- 7.1 Los dispositivos deben bloquearse al ausentarse del puesto de trabajo.
- 7.2 La información personal de candidatos, clientes y empleados debe almacenarse en plataformas seguras y autorizadas.
- 7.3 Queda prohibido descargar, copiar o transferir información sensible a dispositivos personales o unidades externas sin autorización.
- 7.4 Todos los correos, documentos y archivos que contengan datos sensibles deben estar cifrados o protegidos con contraseña.
- 7.5 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.
- 7.6 Todos los sistemas y aplicaciones deben mantenerse actualizados.
- 7.7 Responsabilidad de aplicar los parches de seguridad recomendados por los proveedores.
- 7.8 La empresa realizará respaldos automáticos de la información crítica de forma periódica.
- 7.9 Todos los colaboradores deberán guardar documentos importantes en las carpetas o nubes designadas por la empresa.
- 7.10 Todos los nuevos colaboradores deberán firmar un documento de cumplimiento de políticas y acuerdo de confidencialidad antes de recibir acceso a los sistemas.

✓	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.

08

SANCIONES POR INCUMPLIMIENTO

Consecuencias disciplinarias, civiles, contractuales y penales

RÉGIMEN DE SANCIONES

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:

- 8.1 Llamados de atención.
- 8.2 Suspensión temporal de accesos y privilegios tecnológicos.
- 8.3 Procesos disciplinarios internos.
- 8.4 Terminación del contrato laboral o comercial.
- 8.5 Acciones legales por daños y perjuicios.
- 8.6 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.

09

CANALES DE COMUNICACIÓN

Reporte de incidentes, indicios o sospechas

COMUNICACIÓN SEGURA

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



SECURE BY DESIGN.

JUVA Group • Cybersecurity • Resilience • Trust