JUSTECH SRL

Centro Legal y de Cumplimiento

Política de Seguridad de la Información

Código: **JT-POL-SEG-001**

Versión 1.0 · Emisión / Vigencia: 13 de julio de 2026

Próxima revisión: 13 de julio de 2027

Clasificación: Pública · Aprobado por: Gerencia General

Documento corporativo verificable. No declara certificaciones no confirmadas.

Código: JT-POL-SEG-001

Empresa: Justech SRL **País:** República Dominicana **Dominio:** justech.do **Versión:** 1.0 **Fecha de emisión:** 13 de julio de 2026 **Fecha de vigencia:** 13 de julio de 2026 **Próxima revisión:** 13 de julio de 2027 **Clasificación:** Pública (documento corporativo) **Aprobado por:** Gerencia General **Estado:** Publicado para consulta pública; valores operativos marcados como pendientes permanecen sujetos a confirmación de Gerencia.

Control del documento

Campo	Valor
Código	JT-POL-SEG-001
Título	Política de Seguridad de la Información
Versión	1.0
Emisión	13 de julio de 2026
Vigencia	13 de julio de 2026
Próxima revisión	13 de julio de 2027
Propietario	Gerencia General / Responsable de Tecnologías
Aprobación	Gerencia General
Clasificación	Pública

Historial de cambios

Versión	Fecha	Descripción	Autor
1.0	13 de julio de 2026	Emisión inicial para Centro Legal y de Cumplimiento	Justech SRL

1. Objetivo

Establecer los principios, responsabilidades y controles razonables que Justech SRL aplica para proteger la confidencialidad, integridad y disponibilidad de la información que procesa en el marco de sus servicios tecnológicos, incluyendo plataformas, sitios web, correo electrónico, soportes a clientes y operación interna.

Esta política **no afirma** la posesión de certificaciones ISO, PCI DSS, SOC 2 u otras no confirmadas.

2. Alcance

Aplica a:

• colaboradores, contratistas y personal temporal de Justech SRL;

• sistemas, cuentas, dispositivos y repositorios utilizados para prestar servicios;

• información de clientes, proveedores, prospectos y usuarios del sitio web justech.do;

• proveedores de tecnología y de nube que actúan como encargados o subcontratistas, en la medida contractual aplicable.

3. Principios de seguridad

Justech SRL se guía por:

• **Confidencialidad:** acceso a la información solo por personas autorizadas.

• **Integridad:** prevenir alteraciones no autorizadas o no detectadas.

• **Disponibilidad:** mantener operativos los servicios críticos dentro de objetivos prudentes.

• **Mínimo privilegio:** permisos limitados a lo necesario.

• **Defensa en profundidad:** controles complementarios (técnicos, administrativos y físicos razonables).

• **Responsabilidad y auditoría:** acciones relevantes deben poder trazarse.

4. Roles y responsabilidades

Rol	Responsabilidad
Gerencia General	Aprobar la política, asignar recursos y revisar incumplimientos graves
Responsable de Tecnologías / Operaciones	Implementar controles, gestionar accesos, incidentes y proveedores
Personal	Cumplir esta política, reportar incidentes y proteger credenciales
Proveedores	Cumplir obligaciones contractuales de seguridad y confidencialidad

Pendiente de confirmación por Gerencia: *cualquier dato no verificado en el sitio oficial o en registros internos confirmados.*

5. Control de acceso y gestión de usuarios

• Las cuentas de acceso a sistemas corporativos son personales e intransferibles.

• El alta, modificación y baja de usuarios se realiza mediante solicitud autorizada.

• Se revisan periódicamente privilegios de cuentas privilegiadas.

• Las cuentas de ex colaboradores se deshabilitan de forma oportuna al cese.

• Se evita el uso de cuentas genéricas salvo justificación documentada.

6. Contraseñas y autenticación

• Se requieren contraseñas robustas y no reutilizadas entre sistemas críticos.

• Se prohíbe compartir contraseñas por canales inseguros.

• Donde la plataforma lo permita, se habilita **autenticación multifactor (MFA)**, priorizando consolas de administración, correo y paneles de hosting/nube.

• Se deben cambiar credenciales ante sospecha de compromiso.

7. Clasificación y manejo de información

Categorías orientativas:

Clasificación	Ejemplos	Tratamiento
Pública	Contenido del sitio web corporativo	Puede difundirse
Interna	Procedimientos operativos	Solo personal autorizado
Confidencial	Datos de clientes, credenciales, tickets	Acceso restringido, cifrado en tránsito cuando aplique
Restringida	Secretos comerciales, claves	Mínimo privilegio y registro de acceso

La información confidencial no debe enviarse a buzones personales no corporativos ni publicarse en canales abiertos.

8. Protección de equipos y puesto de trabajo

• Sistemas con actualizaciones de seguridad aplicables.

• Protección antimalware en estaciones de trabajo donde corresponda.

• Bloqueo de pantalla ante ausencia.

• Prohibición de instalación de software no autorizado en activos corporativos.

• Dispositivos móvles usados para trabajo deben protegerse con código/biometría y actualizaciones.

9. Red, perímetro y cifrado

• Uso de firewalls y controles perimetrales del hosting/infraestructura contratada.

• Preferencia de HTTPS/TLS para sitios y servicios públicos.

• Credenciales y secretos no deben almacenarse en repositorios públicos ni en páginas web.

• Canales administrativos preferentemente cifrados (FTPS/SSH/VPN según corresponda).

Pendiente de confirmación por Gerencia: *cualquier dato no verificado en el sitio oficial o en registros internos confirmados.*

Detalle de arquitectura de red, WAF y esquemas de cifrado en reposo específicos de cada servicio.

10. Copias de seguridad

• Se realizan respaldos de información crítica según la criticidad del servicio.

• Los respaldos se almacenan de forma segregada cuando el servicio lo permite.

• Se prueban restauraciones de manera periódica razonable.

• RPO/RTO específicos: ver JT-POL-BCP-001 (valores pendientes de confirmación cuando no estén verificados).

11. Registros, auditoría y correo

• Se conservan registros técnicos y de acceso relevantes para investigación de incidentes, conforme a retención aplicable.

• El correo corporativo es un canal oficial; se recomienda verificar remitentes ante phishing.

• No se solicita a clientes contraseñas plenas por correo no validado.

12. Acceso remoto, teletrabajo y dispositivos móviles

• El trabajo remoto debe realizarse desde redes y dispositivos razonablemente seguros.

• Se evita el uso de Wi-Fi públicas sin protecciones adicionales para tareas privilegiadas.

• Documentos confidenciales no deben descargarse en dispositivos no controlados sin necesidad.

13. Proveedores y desarrollo seguro

• La contratación de proveedores tecnológicos considerará capacidad de seguridad y confidencialidad.

• Desarrollos y cambios deben evitar exposición accidental de datos y credenciales.

• Se gestionan vulnerabilidades con priorización según impacto y explotabilidad.

• No se publican pruebas de concepto explotables en entornos productivos.

14. Gestión de incidentes y evidencias

Ante un incidente de seguridad (acceso no autorizado, malware, filtración sospechosa, indisponibilidad por ataque):

• Contener y registrar.

• Escalar según JT-SOP-ATN-001 / JT-POL-BCP-001.

• Preservar evidencias (registros, capturas, correos) sin alterar indebidamente.

• Comunicar a afectados cuando la ley o el contrato lo requieran.

• Documentar lecciones aprendidas.

15. Capacitación e incumplimientos

• El personal recibe inducción/refuerzo sobre buenas prácticas de seguridad.

• El incumplimiento puede generar medidas disciplinarias y/o contractuales, sin perjuicio de acciones legales.

16. Revisión y control de cambios

Esta política se revisa al menos anualmente, o antes ante cambios materiales de servicios, amenazas o marco legal. Los cambios relevantes se versionan en el historial.

17. Contacto

Para consultas sobre esta política: **info@justech.do** Soporte técnico: **soporte@justech.do** (sujeto a confirmación operativa) · Portal: https://soporte.justech.do Teléfono publicado en sitio: **809-455-2372**