POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
BEOTEC INGENIERÍA S.A.S.

Beotec Ingeniería S.A.S. reconoce que la información es un activo estratégico para la organización, sus clientes y aliados. La presente política establece los principios y lineamientos para proteger la información frente a accesos no autorizados, pérdida, alteración, divulgación o uso indebido, garantizando su confidencialidad, integridad y disponibilidad, y contribuyendo a la continuidad y sostenibilidad del negocio.

La seguridad de la información es responsabilidad de todos los colaboradores, contratistas y aliados que tengan acceso a los sistemas, procesos o datos de la organización.

Alcance

Esta política aplica a:
• Toda la información física y digital de Beotec.
• Información de clientes administrada en el marco de servicios tecnológicos o de seguridad.
• Datos personales tratados en el marco de la legislación aplicable en Colombia.
• Sistemas tecnológicos propios y de terceros utilizados en la operación.
• Infraestructura tecnológica, redes, centros de monitoreo y plataformas de gestión.
• Colaboradores, contratistas, proveedores y aliados estratégicos.

Incluye información técnica, comercial, contractual, financiera, operativa y cualquier otra que sea considerada relevante para la organización o sus clientes.

Principios de Seguridad de la Información

Confidencialidad
La información solo será accesible a personas autorizadas y para los fines establecidos en el desarrollo de sus funciones.

Integridad
La información debe mantenerse completa, exacta y protegida frente a modificaciones no autorizadas o accidentales.

Disponibilidad
Los sistemas y la información deberán estar disponibles para el negocio cuando sean requeridos.

Responsabilidad
Cada colaborador es responsable del uso adecuado y protección de la información a la que tenga acceso.

Principio de mínimo privilegio
Los accesos a información y sistemas se otorgarán únicamente en la medida necesaria para el desempeño de las funciones asignadas.

Trazabilidad y auditoría
Las actividades relevantes sobre sistemas e información crítica deberán generar registros que permitan su monitoreo y auditoría cuando sea necesario.

Lineamientos Generales

Control de Acceso
• Los accesos a sistemas y plataformas estarán definidos según roles y responsabilidades.
• Se utilizarán credenciales individuales para cada usuario.
• Está prohibido compartir usuarios o contraseñas.
• Los accesos serán revocados al finalizar la relación laboral o contractual.
• Cuando sea posible se aplicarán mecanismos de autenticación fuerte o multifactor.
• Las cuentas privilegiadas deberán utilizarse únicamente para tareas administrativas.
• Los accesos a sistemas de clientes deberán registrarse y auditarse.

Protección de Información de Clientes
La información técnica y operativa de clientes es estrictamente confidencial. No podrá ser compartida sin autorización expresa del cliente.
La toma de capturas de pantalla o registro fotográfico para los aplicativos o instalaciones del cliente, deberá limitarse a actividades de soporte o diseño autorizadas.

Uso Seguro de Equipos y Sistemas
• Solo se utilizarán herramientas tecnológicas autorizadas por la empresa.
• Los equipos deberán mantener actualizaciones de seguridad, antivirus y parches.
• Se realizarán copias de seguridad periódicas de la información crítica.
• Se promoverá el uso seguro de redes, dispositivos y plataformas digitales.

Clasificación y Manejo de la Información
Beotec adopta el protocolo TLP (Traffic Light Protocol) versión 2.0 para clasificar la información:

TLP:RED – Información estrictamente restringida.
TLP:ÁMBAR – Información limitada a la organización y socios de confianza.
TLP:VERDE – Información compartida dentro de comunidades de confianza.
TLP:BLANCO / TRANSPARENTE – Información pública.

La información sensible deberá almacenarse y transmitirse mediante mecanismos que garanticen su protección.

Gestión de Incidentes de Seguridad
Todo incidente o sospecha de incidente deberá ser reportado inmediatamente al responsable designado.
Los incidentes deberán documentarse y se tomarán acciones orientadas a:
• contener el incidente
• mitigar impactos
• analizar causas
• prevenir recurrencias

Seguridad en Proveedores y Terceros
Los proveedores o aliados que tengan acceso a información o sistemas de Beotec deberán cumplir con los lineamientos de seguridad establecidos por la organización y podrán requerir acuerdos de confidencialidad.

Continuidad del Negocio
Beotec promoverá medidas razonables para procurar la continuidad de sus servicios incluyendo respaldos de información y procedimientos de recuperación ante fallas.

Gestión de Activos de Información
La organización mantendrá un inventario básico de activos de información relevantes para la prestación de servicios, identificando responsables, nivel de sensibilidad y ubicación de los activos.

Gestión de Riesgos de Seguridad de la Información
Beotec promoverá un enfoque progresivo de gestión de riesgos mediante revisiones internas, análisis de incidentes y evaluación de amenazas relevantes para sus operaciones.

Registro y Monitoreo
Los sistemas utilizados deberán generar registros que permitan identificar accesos, cambios relevantes y eventos de seguridad.

Gestión de Vulnerabilidades
Se promoverá la reducción de vulnerabilidades mediante actualización de software, seguimiento de alertas de fabricantes y aplicación de parches de seguridad cuando sea posible.

Formación y Concienciación
Beotec promoverá la concienciación del personal en buenas prácticas de seguridad de la información mediante capacitaciones y socialización de esta política.

Gestión de Incidentes con Clientes
Cuando un incidente pueda afectar información o servicios de un cliente, se evaluará el evento, se implementarán medidas de contención y se notificará al cliente cuando corresponda.

Cumplimiento Legal
La organización cumplirá con la legislación aplicable y con los compromisos relacionados con la protección de información, incluyendo la Ley 1581 de 2012 de protección de datos personales en Colombia.

Gobierno de Seguridad de la Información
La Dirección de Beotec designará un responsable interno para coordinar la implementación progresiva de las prácticas de seguridad de la información.

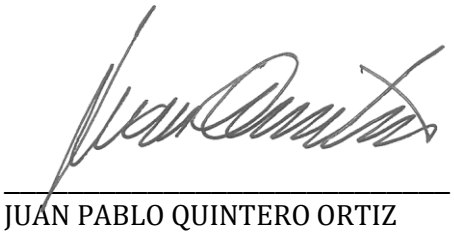
Sus responsabilidades incluyen:
• promover la aplicación de esta política
• apoyar la gestión de incidentes
• mantener comunicación con clientes frente a temas de seguridad
• proponer mejoras en la gestión de seguridad de la información

Cumplimiento
El incumplimiento de esta política podrá generar medidas disciplinarias conforme a la normatividad interna de la empresa y la legislación aplicable.

Compromiso de la Dirección
La Dirección de Beotec se compromete a:
• promover una cultura organizacional orientada a la protección de la información
• asignar recursos razonables para fortalecer la seguridad de la información
• integrar la seguridad de la información en los procesos estratégicos y operativos
• revisar periódicamente esta política

Revisión de la Política

Esta política será revisada al menos una vez al año o cuando se presenten cambios significativos en la operación, los sistemas tecnológicos, los riesgos identificados o los requerimientos de los clientes.



JUAN PABLO QUINTERO ORTIZ

Representante Legal