1. Gobierno y Organización de Seguridad

Establecer un marco de gobierno que defina la estructura, roles y responsabilidades para la gestión de la seguridad de la información.

- Se designará un Comité de Seguridad de la Información liderado por el CISO.
- Las políticas de seguridad deben ser aprobadas por la alta dirección y revisadas anualmente.
- Se asignarán responsables por cada dominio de seguridad.
- Todos los empleados deben conocer y cumplir las políticas de ciberseguridad.

2. Gestión de Riesgos

Identificar, evaluar y tratar los riesgos asociados a la información y sistemas críticos.

- Se debe realizar un análisis de riesgos semestralmente.
- Los activos críticos deben tener planes de mitigación y continuidad.
- Los riesgos serán clasificados según su impacto y probabilidad.
- Los resultados serán presentados a la alta dirección.

3. Seguridad del Recurso Humano

Asegurar que todos los empleados y contratistas comprendan sus responsabilidades antes, durante y después de su relación laboral.

- Contrataciones incluirán verificación de antecedentes.
- Todos deben firmar un acuerdo de confidencialidad.
- Capacitaciones periódicas en ciberseguridad son obligatorias.
- Al finalizar la relación laboral, se revocarán accesos y se realizará una entrevista de salida.

4. Gestión de Activos

Garantizar la protección y control de los activos de información.

- Todos los activos deben ser inventariados y clasificados.
- Se asignará un responsable a cada activo.
- El uso de activos debe estar restringido a propósitos autorizados.
- Equipos obsoletos o defectuosos deben ser eliminados de forma segura.

5. Gestión de Identidad y Acceso

Controlar el acceso a los sistemas y datos sensibles con base en el principio de mínimo privilegio.

- Se implementará autenticación multifactor para accesos críticos.
- Los accesos se conceden por roles definidos.
- Revisiones periódicas de accesos se realizarán cada trimestre.
- Las cuentas inactivas serán eliminadas tras 30 días.

6. Infraestructura / Seguridad Física

Proteger los entornos físicos donde se alojan activos de información.

- Acceso físico controlado mediante tarjetas electrónicas.
- Vigilancia CCTV en áreas críticas.
- Visitantes deben estar registrados y acompañados.
- Equipos deben estar ubicados en zonas seguras y refrigeradas.

7. Seguridad de la Red

Asegurar la disponibilidad, integridad y confidencialidad del tráfico de red.

- Uso de firewalls, IDS/IPS, segmentación de red.
- Redes Wi-Fi protegidas mediante WPA2/WPA3.
- Monitorización continua del tráfico de red.
- VPN obligatoria para conexiones remotas.

8. Seguridad de las Aplicaciones

Garantizar que las aplicaciones desarrolladas cumplan con principios de seguridad desde su concepción.

- Adopción del modelo DevSecOps.
- Pruebas de seguridad automatizadas en CI/CD.
- Revisión de código segura y análisis estático.
- Ciclos de vida del software deben incluir pruebas de vulnerabilidad.

9. Protección de Datos

Proteger la información sensible en todas sus formas contra accesos no autorizados.

- Datos sensibles deben cifrarse en tránsito y en reposo.
- Políticas de retención de datos definidas.
- Eliminación segura de información obsoleta.
- Control de acceso basado en clasificación de la información.

10. Privacidad de Datos Personales

Asegurar el cumplimiento de normativas de protección de datos personales (e.g. Ley 1581 de 2012 en Colombia, GDPR si aplica).

- Consentimiento informado obligatorio para recolección de datos.
- Se designará un Oficial de Protección de Datos.
- Procedimientos para atender solicitudes de titulares.
- Evaluaciones de impacto de privacidad en nuevos proyectos.

11. Operaciones de Seguridad

Garantizar la operación segura de los servicios y sistemas TI.

- Gestión de parches y actualizaciones.
- Backups automáticos y pruebas de restauración.
- Monitorización 24/7 con SIEM.
- Procedimientos definidos ante fallos de sistemas.

12. Gestión de Incidentes y Problemas

Detectar, reportar, analizar y responder de forma eficaz a incidentes de ciberseguridad.

- Canal único para reportar incidentes.
- Clasificación de incidentes por impacto y urgencia.
- Plan de respuesta a incidentes documentado.
- Lecciones aprendidas y mejora continua post-incidente.

Revisión y Actualización: Este manual debe ser revisado anualmente o cuando ocurran cambios significativos en el entorno tecnológico, regulatorio o de negocio.

Responsable: CISO – Chief Information Security Officer

Anexos

Anexo 1: Matriz de Clasificación de la Información

Clasificación	Descripción	Ejemplos	Controles sugeridos
Pública	Información que puede ser compartida libremente.	Contenidos del sitio web, comunicados de prensa.	Sin controles especiales.
Interna	Uso interno, no debe compartirse fuera de la organización.	Manuales internos, políticas.	Acceso con credenciales, sin cifrado requerido.
Confidencial	Información sensible que puede causar daño si se divulga.	Datos de clientes, proyectos en curso.	Cifrado en reposo y tránsito, acceso restringido.
Restrictiva	Información crítica cuyo acceso está altamente limitado.	Contraseñas, secretos comerciales.	Acceso mínimo, cifrado fuerte, monitoreo continuo.

Anexo 2: Formato de Reporte de Incidente de Seguridad

Fecha y hora del incidente: _____

Reportado por: _____

Descripción del incidente: _____

Activos afectados: _____

Impacto estimado: _____

Acciones tomadas: _____

¿Fue notificado al CISO? (Sí/No): _____

Recomendaciones o lecciones aprendidas: _____

Anexo 3: Lista de Verificación para Desarrollo Seguro (DevSecOps)

☐ ¿Se realizó análisis estático del código fuente?

☐ ¿Se aplicaron controles de acceso a entornos de desarrollo?

☐ ¿Se validan las entradas del usuario contra ataques comunes?

☐ ¿Las dependencias externas fueron auditadas?

☐ ¿Se implementó autenticación y autorización segura?

☐ ¿Se aplican políticas de gestión de secretos?

☐ ¿Se registran y monitorean eventos de seguridad relevantes?

Cordialmente,

LUIS HERNAN BONILLA CUERVO
Representante Legal