1. MISIÓN CODALTEC

CODALTEC integra, adapta, apropia y desarrolla soluciones TIC innovadoras para el sector de seguridad y defensa en Colombia y la región, fomentando la integración entre el sector público, la academia y el sector privado, contribuyendo a una economía sostenible basada en alto valor agregado, empleo de calidad y generación de conocimiento, tanto para el mercado interno como para el externo. (PEC 2023-2026).

2. ALCANCE POLÍTICA

La presente política es de obligatorio cumplimiento para todos los funcionarios, contratistas, pasantes, proveedores, aliados y terceros que tengan acceso a información, sistemas, plataformas, redes, servicios en la nube o activos tecnológicos de CODALTEC.

Aplica a toda la información en cualquier formato (digital, físico o verbal) y a todos los entornos de operación (instalaciones, trabajo remoto, dispositivos móviles y servicios en la nube).

3. OBJETIVO DE LA POLÍTICA

Establecer lineamientos obligatorios para la protección de la confidencialidad, integridad y disponibilidad de la información de CODALTEC, previniendo accesos no autorizados, pérdida de información, uso indebido de activos tecnológicos o cualquier afectación a la continuidad operativa y reputacional de la Corporación.

4. MARCO NORMATIVO DE LA POLÍTICA

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002:2022 – Controles de Seguridad de la Información.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1273 de 2009 – Delitos Informáticos.
- Decreto 1377 de 2013 – Reglamentación de Datos Personales.
- CONPES 3995 de 2020 – Política de Seguridad Digital.
- Reglamento Interno de Trabajo – CODALTEC – Código: AP-TH-RG-03.
- COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN – Código: AP-TI-FR-01.

5. POLÍTICA

La presente política establece disposiciones obligatorias y claras para la protección de la información corporativa de CODALTEC, alineadas con ISO/IEC 27001:2022. Su finalidad es prevenir, detectar, controlar y sancionar cualquier conducta que comprometa la confidencialidad, integridad, disponibilidad y trazabilidad de la información, así como proteger a la Corporación frente a riesgos operativos, disciplinarios, contractuales y legales.

5.1 PROPIEDAD, USO Y RESPONSABILIDAD SOBRE LA INFORMACIÓN.

5. POLÍTICA

Toda la información generada, recibida, procesada, almacenada o transmitida mediante los recursos tecnológicos de CODALTEC es propiedad exclusiva de la Corporación de Alta Tecnología para la Defensa - CODALTEC. Su uso se limita estrictamente al cumplimiento de funciones laborales o contractuales.

Queda estrictamente prohibido:

- Utilizar información corporativa para fines personales, comerciales o ajenos a la Corporación.
- Copiar, extraer, descargar, fotografiar, replicar o transferir información sin autorización expresa.
- Divulgar información a terceros por cualquier medio sin autorización previa y escrita.
- Conservar información corporativa al finalizar el vínculo laboral o contractual.

Nota: *La responsabilidad sobre la información es personal e indelegable. El usuario responderá por cualquier uso indebido, pérdida, alteración o divulgación atribuible a su gestión.*

5.2 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DEL PERSONAL.

La seguridad de la información será evidente durante la vinculación, permanencia, cambio de cargo, cambio de funciones y finalización del vínculo laboral, contractual o funcional de todo funcionario, contratista, pasante, proveedor, aliado o tercero que tenga acceso a información, sistemas, plataformas, redes, servicios en la nube o activos tecnológicos de CODALTEC.

Toda persona que acceda a información o recursos tecnológicos de la Corporación deberá conocer, aceptar y cumplir las políticas, protocolos, compromisos de confidencialidad, lineamientos de ciberseguridad y demás disposiciones aplicables. La asignación de cuentas, accesos, equipos, permisos o perfiles estará condicionada al cumplimiento de los requisitos definidos por la Dirección TIC en materia de seguridad y privacidad de la información.

Queda estrictamente prohibido:

- Acceder a información, sistemas, plataformas o activos tecnológicos sin autorización formal.
- Omitir la suscripción de compromisos de confidencialidad cuando sea requisito para acceder a información o recursos tecnológicos.
- Conservar información, credenciales, equipos, documentos, copias físicas o digitales después de finalizado el vínculo laboral, contractual o funcional.
- Utilizar información conocida durante la relación con la Corporación para beneficio propio, de terceros o para finalidades ajenas a CODALTEC.

5. POLÍTICA

- Divulgar información de la Corporación, durante la etapa contractual y postcontractual, sin contar con autorización expresa para ello.

Nota: *Al finalizar el vínculo laboral, contractual o funcional, deberán revocarse los accesos, reintegrarse los activos informáticos asignados y verificarse la entrega de la información bajo responsabilidad del usuario.*

5.3 SEGURIDAD FÍSICA Y CONTROL DE ACCESO A LAS INSTALACIONES.

El acceso físico a las instalaciones, áreas de trabajo y zonas donde se encuentren equipos tecnológicos, cableado, comunicaciones, documentos, información corporativa o activos de información deberá realizarse de manera autorizada.

Queda estrictamente prohibido:

- Permitir el ingreso de personas no autorizadas a áreas donde se almacene, procese, consulte o custodie información corporativa.
- Compartir, prestar, divulgar o facilitar medios de acceso físico, llaves, tarjetas, claves, mecanismos biométricos, códigos o cualquier elemento de autenticación física.
- Forzar, manipular, alterar, deshabilitar, evadir o vulnerar controles de acceso físico instalados por la Corporación.
- Ingresar a áreas restringidas sin autorización o sin el acompañamiento correspondiente.
- Dejar puertas, accesos, oficinas, salas técnicas o áreas sensibles abiertas, sin supervisión o sin las medidas de cierre establecidas.
- Permitir el ingreso de visitantes, proveedores o terceros sin registro, autorización o acompañamiento (cuando aplique).

5.4 USO DE EQUIPOS, RED CORPORATIVA Y DISPOSITIVOS.

El acceso, uso, conexión, revisión, mantenimiento o intervención de equipos tecnológicos en la red corporativa estará permitido únicamente para equipos autorizados, inventariados y administrados por la Dirección TIC, y deberá ser realizado exclusivamente por dicha Dirección o por personal expresamente autorizado por esta.

Queda estrictamente prohibido:

- Conectar equipos personales (portátiles, celulares, tablets, USB u otros) a la red corporativa sin autorización expresa.
- Compartir el acceso a redes cableadas o inalámbricas con terceros no autorizados.

5. POLÍTICA

- Utilizar la red corporativa para actividades no relacionadas con el objeto laboral o contractual.
- Destapar, desensamblar o intervenir físicamente equipos corporativos sin autorización de la Dirección TIC.
- Retirar, cambiar o manipular componentes internos como memoria RAM, discos duros, tarjetas, procesadores, baterías o cualquier otro elemento de hardware.
- Alterar la configuración física o técnica del equipo asignado.
- Conectar equipos personales o no corporativos a la red sin autorización expresa.
- Conectar equipos personales autorizados que tengan software pirata, no licenciado, crackeado, activadores ilegales o herramientas no autorizadas.
- Permitir que terceros usen equipos corporativos o accedan a la red corporativa.

Nota: *Todo equipo personal o no corporativo autorizado para conectarse a la red deberá contar con software legal, licenciado, actualizado y libre de herramientas no autorizadas. La Dirección TIC podrá negar, bloquear o retirar el acceso cuando el equipo represente riesgo para la seguridad, continuidad o legalidad de la Corporación.*

5.5 USO DE SOFTWARE, LICENCIAMIENTO Y SEGURIDAD TÉCNICA.

Solo se permitirá el uso de software autorizado, validado y debidamente licenciado por CODALTEC.

Queda estrictamente prohibido:

- Instalar, descargar o ejecutar software pirata, ilegal o sin licenciamiento.
- Instalar aplicaciones sin validación de la Dirección TIC.
- Utilizar activadores, cracks, seriales no autorizados, keygens o cualquier mecanismo destinado a evadir licenciamiento.
- Ejecutar software portable, herramientas de hacking, escaneo, interceptación, evasión, anonimización o acceso remoto no autorizado.
- Descargar juegos, instaladores, extensiones o aplicaciones que no tengan relación con las funciones asignadas.

Nota: *El uso de software no autorizado podrá generar responsabilidades disciplinarias, contractuales, civiles y penales.*

5.6 GESTIÓN Y ALMACENAMIENTO DE LA INFORMACIÓN (GOOGLE DRIVE).

Toda la información corporativa deberá almacenarse exclusivamente en las Unidades Compartidas de la nube corporativa (Google Drive), garantizando su

5. POLÍTICA

disponibilidad, control de acceso y trazabilidad, conforme a la directriz corporativa vigente.

Queda estrictamente prohibido:

- Utilizar "Mi unidad" para la gestión de información corporativa.
- Almacenar información en nubes personales, dispositivos locales o repositorios externos no autorizados.
- Gestionar información crítica fuera de las Unidades Compartidas.

Nota: *Cada dependencia será responsable de asegurar que la información bajo su gestión se encuentre organizada, actualizada, accesible y correctamente administrada en los repositorios definidos.*

5.7 ELIMINACIÓN, MODIFICACIÓN Y CONTROL DE LA INFORMACIÓN.

La eliminación, modificación o disposición de la información deberá realizarse únicamente bajo lineamientos autorizados y controlados.

Queda estrictamente prohibido:

- Eliminar información sin autorización expresa.
- Alterar, modificar o sobrescribir información sin control y sin dejar registro.
- Eliminar información al momento de retiro, entrega de cargo o finalización del contrato.
- Borrar registros, evidencias digitales, logs o cualquier traza de auditoría.

5.8 CONTROL DE ACCESOS, CREDENCIALES Y AUTENTICACIÓN.

El acceso a la información, sistemas, plataformas, carpetas, aplicaciones y servicios corporativos se asignará bajo el principio de mínimo privilegio, de manera que cada usuario cuente únicamente con los permisos estrictamente necesarios para el cumplimiento de sus funciones, actividades u obligaciones contractuales. Los accesos deberán corresponder al rol, dependencia, responsabilidad, necesidad operativa y nivel de autorización definido por CODALTEC.
Queda estrictamente prohibido:

- Compartir usuarios y contraseñas.
- Utilizar credenciales de otros usuarios.
- Mantener sesiones abiertas sin supervisión.
- Registrar el correo corporativo en plataformas, aplicaciones, boletines, servicios o sitios web no autorizados.

5. POLÍTICA

- Usar el correo corporativo para crear cuentas personales en redes sociales, juegos, apuestas, entretenimiento, compras, suscripciones o servicios ajenos a la Corporación.
- Comprar juegos, licencias personales, aplicaciones, servicios digitales o productos no autorizados usando el correo corporativo.
- Asociar el correo corporativo a medios de pago, billeteras digitales, cuentas personales o plataformas comerciales no autorizadas.
- Usar el correo corporativo para recuperar, validar o administrar cuentas personales.

Nota: *El correo corporativo deberá utilizarse exclusivamente para comunicaciones relacionadas con las funciones, obligaciones y actividades propias de CODALTEC. Su uso indebido podrá dar lugar al bloqueo o suspensión de la cuenta, revisión del buzón, investigación interna y aplicación de las acciones disciplinarias, contractuales o legales correspondientes.*

Las credenciales deberán cumplir como mínimo con los siguientes requisitos:

- ✓ Longitud mínima de ocho (8) caracteres.
- ✓ Inclusión de letras mayúsculas, minúsculas, números y caracteres especiales.
- ✓ Uso obligatorio de autenticación en dos factores (2FA) cuando esté disponible.
- ✓ Cambio obligatorio de contraseña cada noventa (90) días o ante sospecha de compromiso.
- ✓ Prohibición de almacenamiento de contraseñas en medios inseguros.

Las credenciales son personales, intransferibles y cifradas. El titular será responsable de toda actividad realizada con las mismas.

5.9 USO DE CORREO ELECTRÓNICO Y COMUNICACIONES.

El correo corporativo es un activo de CODALTEC y su uso está limitado a funciones laborales.

Queda estrictamente prohibido:

- Enviar información corporativa a cuentas personales.
- Abrir enlaces o archivos de origen desconocido.
- Compartir credenciales o información sensible por correo.

La Corporación podrá acceder, auditar y revisar el contenido de los correos cuando sea necesario para continuidad operativa, auditorías o investigaciones.

5. POLÍTICA

5.10 USO DE INTERNET Y SERVICIOS EN LÍNEA.

Queda estrictamente prohibido:

- Acceder a sitios web ilegales, no laborales o que representen riesgo para la seguridad.
- Descargar contenido no autorizado o potencialmente malicioso.
- Utilizar servicios en línea no autorizados para el manejo de información corporativa.
- La navegación será monitoreada y registrada.

5.11 SEGURIDAD DE LOS EQUIPOS Y CONTROLES OPERATIVOS.

Queda estrictamente prohibido:

- Desactivar antivirus, firewall o controles de seguridad.
- Manipular configuraciones del sistema sin autorización.
- Conectar dispositivos externos sin validación.

Los equipos deberán mantenerse actualizados, protegidos y bajo control del usuario asignado.

5.12 ESCRITORIO LIMPIO Y PANTALLA LIMPIA.

Todo usuario deberá mantener su puesto de trabajo físico y digital en condiciones que reduzcan el riesgo de acceso no autorizado, pérdida, consulta indebida, exposición o divulgación de información corporativa. La información física o digital deberá conservarse únicamente en los repositorios, archivadores, sistemas o medios autorizados por CODALTEC.

Queda estrictamente prohibido:

- Dejar documentos, notas, credenciales, contratos, informes, soportes, medios extraíbles o información corporativa expuesta sobre escritorios, impresoras, salas de reunión o zonas comunes.
- Mantener información crítica o corporativa en el escritorio digital del computador cuando deba estar almacenada en repositorios autorizados.
- Dejar sesiones abiertas, pantallas desbloqueadas o sistemas activos sin supervisión.
- Imprimir información corporativa sin recogerla de manera inmediata o dejarla expuesta a terceros.
- Guardar contraseñas en notas visibles, libretas, archivos sin protección, pantallas, correos personales o medios inseguros.

5. POLÍTICA

Nota: *Al ausentarse del puesto de trabajo, el usuario deberá bloquear la sesión del equipo y asegurar la información física bajo su custodia. Al finalizar la jornada o actividad, deberá garantizar que la información quede debidamente almacenada, protegida y fuera del alcance de personas no autorizadas.*

5.13 TRABAJO REMOTO Y ACCESO EXTERNO.

El acceso remoto deberá realizarse mediante mecanismos seguros definidos por la Corporación.

Queda estrictamente prohibido:

- Acceder a sistemas corporativos desde redes públicas o inseguras sin protección.
- Compartir equipos de trabajo con terceros.

5.14 GESTIÓN DE INCIDENTES DE SEGURIDAD.

Todo incidente, sospecha o evento de seguridad deberá ser reportado de manera inmediata a la Dirección TIC.

Queda estrictamente prohibido:

- Ocultar incidentes de seguridad.
- Manipular, eliminar o alterar evidencia relacionada con incidentes.

5.15 MONITOREO, REGISTRO Y CONTROL.

CODALTEC podrá monitorear, registrar, auditar y analizar el uso de sistemas, redes, dispositivos, correos y plataformas tecnológicas en cualquier momento y sin previo aviso.

No existe expectativa de privacidad en el uso de los recursos tecnológicos corporativos.

Nota: *Los registros digitales, logs y evidencias técnicas serán válidos como soporte en procesos disciplinarios, contractuales, administrativos y judiciales.*

5.16 RELACIÓN CON TERCEROS Y CONFIDENCIALIDAD.

Todo tercero que tenga acceso a información de la Corporación deberá cumplir los lineamientos de seguridad y suscribir el "COMPROMISO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN".

5. POLÍTICA

Queda estrictamente prohibido:

- Compartir información con terceros sin autorización.

Las obligaciones de confidencialidad se mantienen incluso después de finalizada la relación contractual.

5.17 SENSIBILIZACIÓN, APROPIACIÓN Y CULTURA DE SEGURIDAD DE LA INFORMACIÓN.

La sensibilización y apropiación de la seguridad de la información como parte de la cultura corporativa permitirá fortalecer el comportamiento responsable frente al uso de la información, los activos tecnológicos, las credenciales, los repositorios corporativos, el correo electrónico, la gestión de incidentes de seguridad y el cumplimiento de las obligaciones de confidencialidad.

Todo funcionario, contratista, pasante, proveedor, aliado o tercero que tenga acceso a información o recursos tecnológicos de CODALTEC deberá atender las actividades de sensibilización, inducción, reinducción, comunicación o socialización que la Corporación defina en materia de seguridad de la información.

Queda estrictamente prohibido:

- Omitir o desconocer los lineamientos de seguridad divulgados por la Corporación.
- Alegar desconocimiento de la política cuando esta haya sido comunicada, socializada o puesta a disposición por los canales corporativos.
- Desatender recomendaciones, alertas, directrices o comunicaciones emitidas por la Dirección TIC en materia de seguridad de la información.
- Replicar prácticas inseguras después de haber recibido lineamientos, advertencias o comunicaciones preventivas.

Nota: *La sensibilización no sustituye la responsabilidad individual de cumplimiento. La participación, conocimiento y acatamiento de las directrices de seguridad de la información serán considerados parte del deber de cuidado, reserva, diligencia y protección de la información corporativa.*

5.18 INCUMPLIMIENTO, RESPONSABILIDAD Y CONSECUENCIAS.

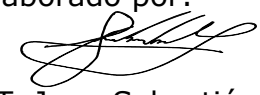
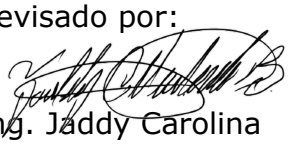
El incumplimiento de la presente política constituye falta grave y podrá generar, según la naturaleza del hecho:

- Sanciones disciplinarias internas.
- Terminación del vínculo laboral o contractual.
- Responsabilidad civil por daños y perjuicios.

5. POLÍTICA

- Responsabilidad penal conforme a la legislación vigente.
- Reportes a autoridades competentes cuando aplique.

Nota: *El desconocimiento de la presente política, la cual hace parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de CODALTEC, no exime de responsabilidad y su cumplimiento es obligatorio para todos los niveles de la Corporación.*

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado por:  ST. Juan Sebastián Segura Moya	Revisado por:  Ing. Jaddy Carolina Machado Barrios.	Aprobado por:  CR. Nilssen Janeth Gutiérrez Suárez.
Cargo: Director TIC.	Cargo: Profesional en Planeación.	Cargo: Gerente.
Fecha: 29/04/2026.	Fecha: 30/04/2026.	Fecha: 04/05/2026.