CORPORACIÓN DE ALTA TECNOLOGÍA PARA LA DEFENSA
CODALTEC

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado por:  My. Cristian Alexander Beltrán Morales Cargo: Director Dirección TICs T2. Chaves Roncancio Nelson Andrés Cargo: Jefe Departamento Soporte	Revisado por:  CR. Abelardo Moreno Lemos Cargo: Subgerente CODALTEC	Aprobado por:  CR. Nilssen Janeth Gutiérrez Suárez Cargo: Gerente CODALTEC
Fecha:2024.08.23	Fecha: 2024.08.23	Fecha:2024.08.23

CONTENIDO

1. INTRODUCCIÓN

Las políticas de seguridad de la información son un conjunto de directrices y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información de CODALTEC. Estas políticas establecen normas para el manejo, almacenamiento y transmisión de datos y así mismo abordan aspectos como el acceso a la información, el uso de sistemas informáticos y la gestión de riesgos. Su objetivo es prevenir la pérdida de datos, el acceso no autorizado y otros incidentes que puedan comprometer la seguridad de la información. Implementar políticas de seguridad de la información efectivas son esenciales para salvaguardar los activos de la Corporación y cumplir con regulaciones legales y normativas.

Este documento complementa los lineamientos emitidos en la "Política de Seguridad de la Información" que fue aprobada por la señora Coronel Nilssen Janeth Gutiérrez Suárez - Gerente General de CODALTEC, de acuerdo con lo consignado en la Orden de Gerencia No. 039/2024 del 19 de julio de 2024, la cual establece en su artículo noveno que:

La estrategia de ciberseguridad busca su alcance inicial de implementación en la Corporación de Alta Tecnología para la Defensa - CODALTEC, buscando garantizar niveles óptimos de integridad, disponibilidad y confidencialidad de los activos digitales. Nuestro enfoque incluirá la adopción de tecnologías para la detección temprana de amenazas, el diseño de políticas de seguridad, la capacitación regular del personal en prácticas de seguridad de la información y la implementación de protocolos de respuesta ante incidentes cibernéticos. Estas medidas no sólo fortalecerán la postura defensiva, sino que también asegurará que la Corporación opere con la máxima seguridad requerida en el entorno digital actual.

2. OBJETIVO

Establecer las directrices que son base fundamental para contrarrestar las amenazas informáticas que puedan afectar significativamente a CODALTEC, implementando la normatividad adecuada y definiendo claramente la gestión correspondiente a la seguridad de la información de los activos críticos y de su infraestructura tecnológica; protegiendo la información almacenada, procesada y transferida en sus procesos informáticos, conservando los principios de seguridad, confidencialidad, integridad y disponibilidad de la información.

3. ALCANCE

Estas políticas son de obligatorio cumplimiento e involucran todos los niveles de la Corporación (operativos, técnicos, administrativos y de control). Recaen directamente en todos los funcionarios, ya sea personal uniformado, de prestación de servicios, contratistas, pasantes, colaboradores y terceros que trabajan en CODALTEC, que interactúan con información, sistemas, plataformas y activos tecnológicos de la Corporación, específicamente los definidos en el alcance del Sistema de Gestión de Seguridad de la Información - SGSI.

4. TERMINOLOGÍA

INFORMACIÓN: La información es un activo que, al igual que otros activos comerciales importantes, es esencial para los negocios de una empresa. Por ello, necesita una protección adecuada.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información.

CONFIDENCIALIDAD: La información no está disponible ni se divulga a personas, entidades o procesos no autorizados.

INTEGRIDAD: Este término hace referencia a la precisión e integridad de la información.

DISPONIBILIDAD: Definido como la información accesible y utilizable bajo solicitud de un organismo autorizado para ello.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Este término describe una ocurrencia identificada en un sistema, servicio o estado de la red que indica una posible infracción de la política de seguridad de la información o un fallo en los controles. También puede tratarse de una situación previamente desconocida que puede ser relevante para la seguridad de la información.

INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN: Definido como el evento de seguridad de la información no deseado que tengan una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

INFORMACIÓN DOCUMENTADA: La información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida. Puede estar en cualquier formato y proceder de cualquier fuente y suele relacionarse con el sistema de gestión y sus procedimientos. Es la información creada para que la organización funcione y evidencia de los resultados logrados.

CONTROL DE ACCESO: Definido como los medios para asegurar que el acceso a los bienes está autorizado y restringido a los requisitos de seguridad de la empresa.

ACCESO AUTORIZADO: Permiso dado a un usuario para interactuar con ciertos recursos o datos según sus credenciales y roles.

AUTENTICACIÓN: Proceso de verificar la identidad de un usuario mediante credenciales como contraseñas, tarjetas inteligentes o autenticación multifactor.

CIFRADO (Encriptación): Método de convertir datos en un formato ilegible para protegerlos durante la transmisión o almacenamiento.

DATA BREACH (Violación de Datos): Incidente en el que la información sensible es accedida, divulgada o robada sin autorización.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: Conjunto de directrices y procedimientos diseñados para proteger la información dentro de una organización.

PROTECCIÓN DE DATOS: Medidas implementadas para asegurar la privacidad y seguridad de los datos personales y sensibles.

REDUNDANCIA: Creación de copias de seguridad o sistemas alternativos para asegurar la disponibilidad de la información en caso de fallos.

RIESGO: Posibilidad de que ocurra un evento que pueda causar daño a la información o a los sistemas.

SEGURIDAD FÍSICA: Protección de los equipos y datos contra daños físicos, robo o acceso no autorizado a las instalaciones.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Conjunto de políticas, procedimientos y controles implementados para gestionar la seguridad de la información en una organización.

USO ACEPTABLE: Reglas que definen cómo deben utilizarse los recursos tecnológicos y de información dentro de una organización.

VULNERABILIDAD: Debilidad en un sistema que puede ser explotada para comprometer la seguridad.

5. PROCEDIMIENTO

Las políticas de seguridad de la información de la Corporación constituyen un documento integral que establece la doctrina, reglamentación y directrices para la protección de los recursos tecnológicos y la información utilizada en las operaciones diarias de CODALTEC. Este manual proporciona un marco claro y detallado para salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas.

Las políticas abarcan todos los aspectos de la seguridad, desde el control de acceso y la gestión de datos hasta la protección física y la respuesta a incidentes. Se aplican a todos los empleados y contratistas a todos los niveles, asegurando que cada persona en la organización entienda sus responsabilidades y cumpla con las normas establecidas para proteger los activos informáticos de CODALTEC.

Además, las políticas son revisadas y actualizadas regularmente para adaptarse a nuevas amenazas, cambios en la tecnología y requisitos regulatorios, garantizando así una protección continua y eficaz en un entorno en constante evolución.

6. POLÍTICAS

CODALTEC establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

6.1 POLÍTICAS DE SEGURIDAD DE RECURSOS HUMANOS

- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.

- Todos los empleados nuevos deben completar un programa de inducción que incluya formación específica en políticas de seguridad de la información, manejo de datos confidenciales, y procedimientos de seguridad.

- Implementar un procedimiento para la terminación de empleo que incluya la revocación inmediata del acceso a sistemas y la recuperación de equipos, credenciales y documentos corporativos.

6.2 POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda la información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de CODALTEC.

- Los activos dispuestos por la Corporación para el apoyo de las labores desempeñadas por los funcionarios, contratistas o proveedores únicamente serán para la ejecución de tareas establecidas en el ámbito laboral de CODALTEC.

- Mantener el inventario actualizado de todos los activos de información.

6.3 POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Asignar permisos de acceso basados en el rol de cada empleado, limitando el acceso a los datos y sistemas solo a lo necesario para su trabajo.

- Revisar y ajustar permisos periódicamente.

- Implementar contraseñas robustas y autenticación multifactor (MFA) para todos los usuarios.

- Garantizar que los accesos se actualicen o revoken según los cambios de rol o la desvinculación de empleados.

- Monitorear el acceso a sistemas y datos, y realizar revisiones periódicas para detectar posibles anomalías.

6.4 CRIPTOGRAFÍA

- Utilizar protocolos de encriptación para proteger la información de la Corporación.

6.5 POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- Restringir el acceso a áreas sensibles mediante sistemas de control de acceso físico.

- Utilizar tarjetas de identificación y sistemas biométricos para controlar el acceso.

- Todas las personas que ingresen a las instalaciones deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

- Implementar sistemas para controlar temperatura y humedad en áreas críticas.

6.6 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Realizar copias de seguridad periódicas de datos críticos.

- Almacenar copias de seguridad en ubicaciones seguras.

6.7 POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- Utilizar dispositivos de seguridad perimetral.

- Utilizar dispositivos de seguridad a profundidad.

- Segmentar la red para limitar el acceso a sistemas y datos críticos.

- Utilizar encriptación para proteger correos electrónicos que contienen información sensible.

- Emplear protocolos de comunicación seguros (ej. HTTPS).

6.8 POLÍTICAS DE MANTENIMIENTO DE SISTEMAS

- Aplicar actualizaciones y parches de seguridad de manera oportuna para mitigar vulnerabilidades.

- Realizar actualizaciones regulares de los sistemas operativos, aplicaciones y software de seguridad.

- Establecer un calendario de mantenimiento regular para aplicar actualizaciones y realizar mantenimiento preventivo.

6.9 POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- Establecer acuerdos de seguridad con proveedores para asegurar la protección de la información.

- Revisar y monitorear el cumplimiento de los proveedores con las políticas de seguridad de la información.

- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

6.10 SEGURIDAD DE LA INFORMACIÓN (DRP - BCP)

- Plan DRP y BCP de la Corporación.

6.11 POLÍTICAS DE GESTIÓN DE INCIDENTES

- Procedimiento de gestión de incidentes de la Corporación.

6.12 POLÍTICAS DE CUMPLIMIENTO

- Realizar auditorías para verificar el cumplimiento de las normativas y políticas internas.

6.13 POLÍTICAS DE ESCRITORIO LIMPIO

- Asegurar que el área de trabajo esté libre de documentos y dispositivos no autorizados cuando no se esté utilizando.

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).

- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo o apagarlos si se retiran de la Corporación.

- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

6.14 POLÍTICAS USO ADECUADO DE INTERNET

- Está prohibido el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.

- Estará limitado el acceso a redes sociales en general.

- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

- La Dirección TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

6.15 POLÍTICAS USO ADECUADO DE CORREO ELECTRÓNICO

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a CODALTEC, por lo tanto, su contenido también es propiedad de la Entidad.

- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.

- La Dirección TIC podrá verificar el contenido de los buzones de los correos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

- Está prohibido almacenar **información personal** o que **no corresponda** a la misionalidad de CODALTEC en el sistema de almacenamiento Google Cloud, teniendo en cuenta que la capacidad de almacenamiento es limitada.

6.16 POLÍTICAS USO DE USUARIOS Y CONTRASEÑAS

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.

- Las credenciales son personales e intransferibles.

- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

- Implementar autenticación multifactor para acceder a sistemas críticos para aumentar la seguridad.

7. SENSIBILIZACIÓN Y COMUNICACIÓN

- Implementar y gestionar programas de sensibilización y comunicación en seguridad de la información utilizando canales de comunicación internos como correos electrónicos, boletines, intranet corporativa y reuniones para informar sobre políticas, actualizaciones y eventos de seguridad.

- Informar sobre incidentes de seguridad y posibles vulnerabilidades.

- Incluir una formación obligatoria sobre seguridad de la información en el programa de inducción para todos los nuevos empleados.

- Realizar evaluaciones para medir la comprensión de los empleados sobre los temas de seguridad de la información.

- Enviar actualizaciones regulares sobre temas de seguridad, nuevas políticas y cambios relevantes.

8. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

- El equipo de seguridad de la información redacta y documenta las políticas.

- El borrador se revisa internamente por la Subgerencia, áreas relevantes (TI) y Planeación de CODALTEC.

- La Gerencia de la Corporación aprueba y firma el manual para su implementación.

- Las políticas se revisan anualmente.

- Se informa a todos los empleados sobre cambios en las políticas a través de canales internos.

- Se realizan auditorías internas para verificar el cumplimiento y se generan informes.

9. ACCIONES LEGALES

Incumplimiento

- Acceso No Autorizado: Uso indebido o acceso no autorizado a la información.
- Violación de Políticas: Incumplimiento de las políticas y procedimientos de seguridad.
- Negligencia: Falta de diligencia que resulta en compromisos de seguridad.

Medidas Disciplinarias

- Primera Incidencia: Se emite una advertencia formal y se proporciona capacitación adicional si es necesario.
- Sanción Menor: Suspensión temporal de acceso o responsabilidades específicas.
- Sanción Grave: Despido, suspensión prolongada, o acciones legales en casos de violaciones graves o repetidas.

Proceso Disciplinario

- Investigación: Realizar una investigación para determinar los hechos y la gravedad de la violación.
- Audiencia: Permitir al empleado presentar su versión de los hechos antes de tomar una decisión.
- Decisión: La alta dirección o el comité de seguridad decide la sanción basada en la gravedad del incumplimiento.

Documentación y Revisión

- Registro de Incidencias: Documentar todas las violaciones y acciones disciplinarias tomadas.

10. CONCLUSIÓN

El presente manual de políticas de seguridad de la información es fundamental para establecer un marco detallado y coherente para la protección de los activos informáticos de la Corporación. Este manual no solo define y documenta las políticas y procedimientos esenciales para asegurar la confidencialidad, integridad y disponibilidad de la información, sino que también establece roles y responsabilidades claras para todos los miembros de la organización. Proporciona directrices específicas para el manejo seguro de datos, la gestión de accesos, la protección contra amenazas internas y externas, y el cumplimiento de regulaciones legales y normativas.

El manual también sirve como herramienta para la formación y sensibilización del personal, asegurando que todos los empleados, contratistas y terceros comprendan y apliquen las mejores prácticas en seguridad de la información. Facilita una respuesta coordinada y efectiva ante incidentes de seguridad al detallar procedimientos de reporte y manejo de incidentes. Al establecer un marco para la evaluación y revisión continua de las políticas, el manual ayuda a adaptar las medidas de seguridad a nuevas amenazas y cambios en el entorno tecnológico.

En última instancia, el manual de políticas de seguridad de la información fortalece la resiliencia de CODALTEC, protege su reputación y asegura la continuidad operativa al mitigar riesgos y responder de manera proactiva a desafíos de seguridad. Al proporcionar una base sólida para la gestión de la seguridad, el manual contribuye significativamente a la protección de los datos valiosos y al mantenimiento de la confianza de clientes, socios y otros stakeholders.

11. NATURALEZA DEL CAMBIO

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE CAMBIOS**
01	2024.08.23	Emisión inicial