SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

De acuerdo con los lineamientos de la Circular 036 de la Superintendencia de la Economía Solidaria y en el contexto del fortalecimiento del Sistema de Gestión de Seguridad de la Información de la Cooperativa, durante la vigencia 2025 COOPRODECOL LTDA continuó desarrollando e implementando iniciativas orientadas a fortalecer la protección de los activos tecnológicos y la información institucional. Estas acciones estuvieron enfocadas en consolidar controles técnicos y administrativos que permitan garantizar la confidencialidad, integridad y disponibilidad de los datos, alineándose con las disposiciones regulatorias vigentes y con las mejores prácticas en seguridad de la información y Ciberseguridad.

En línea con este propósito, se implementó una solución de conectividad basada en tecnología SD-WAN con el operador CLARO, que permite la administración centralizada del tráfico de datos entre las sedes de la Cooperativa. Esta arquitectura mejora el control y la organización de las comunicaciones, facilitando la gestión de los enlaces y la aplicación unificada de políticas de seguridad, así como la priorización de las aplicaciones y los sistemas que soportan la operación institucional.

En línea con lo anterior, se incorporó un equipo de seguridad perimetral (Firewall) en cada una de las oficinas externas de COOPRODECOL LTDA y se integraron los dos enlaces de Internet de los operadores CLARO y GENESIS DATA dentro de la arquitectura SD-WAN. Cada extensión de caja cuenta ahora con un equipo firewall que gestiona los dos enlaces de forma simultánea, de modo que, si uno de los canales de internet falla, el tráfico se transfiere automáticamente al otro sin interrumpir los servicios.

La incorporación del equipo de seguridad perimetral (Firewall) en cada extensión de caja refuerza la protección de la infraestructura tecnológica al controlar y supervisar el tráfico de entrada y salida de cada oficina, aplicando políticas de acceso, filtrado de contenido y protección frente a amenazas externas. Esto permite gestionar la Ciberseguridad de manera centralizada, mantener un estándar de configuración en todas las sedes y reducir la exposición a riesgos que puedan afectar la continuidad y disponibilidad de los servicios tecnológicos de la Cooperativa.

De manera complementaria, se amplió el ancho de banda de los canales de Internet dedicados en la oficina principal y en las extensiones de caja, mejorando la capacidad de transmisión de datos y la estabilidad de las conexiones, lo que contribuye a un mejor desempeño de la red de internet y de los servicios tecnológicos.

Con el fin de asegurar la continuidad de los servicios críticos, en la oficina principal se incorporó un segundo equipo de seguridad perimetral (Firewall) bajo un esquema de alta disponibilidad (HA). Esta configuración permite que, ante la falla del equipo principal, el segundo dispositivo asuma automáticamente su función, manteniendo activos los controles de seguridad, aumentando la estabilidad de la infraestructura tecnológica y reduciendo riesgos de interrupción en la operación de los servicios de la Cooperativa.

Adicionalmente, COOPRODECOL LTDA cuenta con el servicio de seguridad administrada proporcionado por CLARO, mediante el cual el operador gestiona de manera centralizada los equipos de seguridad perimetral (Firewall). El servicio incluye monitoreo continuo y aplicación de políticas de acceso y filtrado, asegurando que los controles de seguridad permanezcan activos y que la infraestructura tecnológica mantenga su operatividad bajo supervisión constante.

A nivel de red interna, se fortalecieron los controles mediante la implementación de segmentación lógica, limitando el acceso a servidores y sistemas críticos únicamente desde redes autorizadas. Adicionalmente, se implementó filtrado de navegación web en todas las extensiones de caja, restringiendo el acceso a sitios web clasificados como de alto riesgo, con el fin de disminuir la probabilidad de incidentes relacionados con software malicioso, intentos de suplantación o descargas no autorizadas.

En cuanto a la protección de los equipos de usuario final, se reforzaron las políticas del antivirus corporativo mediante configuraciones centralizadas y ajustes en los perfiles de seguridad, fortaleciendo los mecanismos de prevención, detección y respuesta ante amenazas.

Con el objetivo de fortalecer la cultura organizacional en seguridad y privacidad de la información, se desarrollaron estrategias de capacitación y sensibilización dirigidas a todos los colaboradores, incluyendo directivos y personal nuevo. Estas jornadas reforzaron conocimientos en prevención de fraude a través de correo electrónico, identificación de intentos de suplantación, manejo adecuado de la información, tratamiento seguro de datos personales y responsabilidades individuales frente a la seguridad y privacidad de la información. Asimismo, se incorporó formalmente el componente de seguridad de la información dentro del proceso de inducción institucional, garantizando que cada nuevo colaborador conozca desde su vinculación las políticas de seguridad de la información y buenas prácticas establecidas por la Cooperativa.

Todas las acciones implementadas durante la vigencia 2025 permitieron consolidar un entorno tecnológico más seguro y confiable, reforzando el cumplimiento de los requisitos establecidos en la Circular 036 de la Supersolidaria, de manera que cada iniciativa implementada contribuye directamente a su cumplimiento. Asimismo, la seguridad de la información continúa integrada a la gestión institucional de la Cooperativa bajo un enfoque de revisión permanente y mejora continua, considerando la evolución del entorno tecnológico, la actualización normativa y los riesgos emergentes asociados a nuevas tecnologías.

Cordialmente;

Gabriel F. Anaya B

Ing. Gabriel Fernando Anaya Blanco
Director SGSI y Tecnología.