



INFORME SGSI Y TECNOLOGIA PARA LA ASAMBLEA 2025

Durante el año 2024, COOPRODECOL LTDA dio pasos fundamentales para fortalecer la infraestructura tecnológica y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI), alineándose con los objetivos estratégicos establecidos. Como parte de estos esfuerzos, se realizó una inversión significativa en la actualización y expansión de nuestra infraestructura, incluyendo la adquisición de equipos de red avanzados y soluciones de seguridad, lo que optimizó el rendimiento de la red, mejoró la capacidad de respuesta ante amenazas externas y protegió los activos críticos de la cooperativa.

En el área de ciberseguridad, se llevó a cabo un análisis y remediación de vulnerabilidades en nuestra infraestructura, que incluyó la actualización de servidores y aplicaciones para mantenerlas alineadas con las últimas versiones y parches de seguridad, lo cual se hizo con la firma DOCUXER especialista en este tema. La implementación de controles de acceso, la segmentación de la red y la actualización de las políticas de seguridad reforzaron nuestra defensa frente a amenazas externas y mejoraron nuestra capacidad de detección y respuesta ante incidentes.

Como complemento a los controles de seguridad, de manera continua se realiza un monitoreo y protección a través del servicio de seguridad gestionada, contratado con nuestro aliado estratégico, Movistar. Este servicio, de forma articulada y coordinada, permite la vigilancia constante de la infraestructura tecnológica y la protección de la red corporativa contra amenazas externas.

Por otra parte, se desplegaron herramientas colaborativas como la suite de Microsoft Office 365, con el apoyo del proveedor Media Commerce, con el fin de fortalecer los procesos operativos a través de soluciones tecnológicas. Además, se capacitó al personal en el uso adecuado de estas herramientas, destacando aspectos clave como el manejo responsable del correo electrónico corporativo y el almacenamiento seguro en la nube mediante la herramienta OneDrive.

Para asegurar la continuidad operativa, se reestructuraron los esquemas de conectividad y se configuraron mecanismos de redundancia que garantizan la operatividad constante de nuestras plataformas tecnológicas, minimizando cualquier posible interrupción en los servicios. Este enfoque se complementó con un monitoreo continuo a través del sistema antivirus, contratado también con DOCUXER, lo que asegura una vigilancia constante de nuestra infraestructura tecnológica y una respuesta rápida ante incidentes de seguridad. Además, se implementaron soluciones para optimizar la eficiencia operativa, como el sistema de impresión en red, que ha permitido simplificar los procesos de impresión, reducir costos operativos y mejorar la gestión de recursos tecnológicos dentro de la cooperativa. La firma BUCATONER es la encargada de este servicio.



La capacitación continua del personal en ciberseguridad ha sido un pilar esencial de nuestra estrategia. A través de simulaciones prácticas, como ejercicios de phishing y formación en ingeniería social, se ha reforzado la capacidad de respuesta frente a riesgos cibernéticos. Estos esfuerzos han sido cruciales para fomentar una cultura organizacional proactiva en seguridad de la información, asegurando que todos los niveles de la cooperativa estén alineados con las mejores prácticas en la protección de datos y activos críticos.

Nuestra colaboración con entidades especializadas, como el Centro Cibernético de la Policía Nacional y la inclusión de COOPRODECOL en los boletines de seguridad del Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT, ha sido clave para mantenernos actualizados sobre las nuevas amenazas y las mejores prácticas en ciberseguridad.

Simultáneamente, se lograron avances significativos en el cumplimiento de la Circular 036 de la Supersolidaria, especialmente en los aspectos clave de seguridad de la información. Se redujeron brechas de seguridad desde el punto de vista técnico, se implementaron planes estratégicos para alcanzar los objetivos, se optimizó la relación con proveedores de TI y se avanzó en la documentación de estrategias y planes para cumplir con las directrices de la circular. Además, se trabajó para garantizar la continuidad de la operación tecnológica, asegurando la estabilidad y disponibilidad de los sistemas. Estas acciones impactaron positivamente en la conformidad con las regulaciones vigentes, reduciendo riesgos y fortaleciendo nuestra postura de seguridad.

En cuanto al Sistema de Gestión de Seguridad de la Información (SGSI), se elaboraron y formalizaron documentos estratégicos clave, como planes, procedimientos y formatos, ante el Consejo de Administración. Se aprobó la metodología de gestión de riesgos de seguridad, que cubre la identificación de amenazas, vulnerabilidades y la implementación de controles adecuados. Esta metodología establece una base sólida para la integración y gestión continua de la seguridad de la información, permitiendo una respuesta efectiva ante riesgos emergentes.

Se mantuvo una relación estrecha con nuestros operadores tecnológicos y aliados estratégicos como S&H Soluciones Informáticas, desarrollando actividades conjuntas para implementar configuraciones de seguridad, realizar monitoreos y resolver alertas que pudieran poner en riesgo la integridad de nuestra red corporativa. Esto fue fundamental para garantizar la protección continua de los sistemas y la información de la cooperativa. También se logró mantener una contratación organizada con los proveedores de TI, enfocándose en salvaguardar los intereses y recursos financieros de la cooperativa, al tiempo que se obtuvieron beneficios adicionales, como capacitaciones y entrenamientos para el personal, reforzando las capacidades internas de seguridad.



Por último, se consolidó un proceso de planeación estratégica orientado a garantizar que todas estas iniciativas se integren dentro de un enfoque robusto y sostenible a largo plazo. Este proceso se fundamenta en tres pilares clave: procesos, tecnología y personas (empleados), y está siendo continuamente reforzado con el apoyo de la alta dirección para garantizar que la seguridad de la información siga siendo una prioridad estratégica para la cooperativa. Este enfoque permitirá avanzar en la creación de un proceso de seguridad integral y adaptable, garantizando la protección continua de nuestros recursos y datos críticos.

En resumen, las acciones emprendidas han sido fundamentales para alcanzar los objetivos de seguridad establecidos, reforzando nuestra infraestructura tecnológica y creando una base sólida para proteger los activos críticos de la cooperativa y asegurar la continuidad operativa. Se ha fomentado una cultura organizacional enfocada en la seguridad, respaldada por el apoyo constante de la gerencia y el Consejo de Administración. Las inversiones realizadas, junto con un enfoque integral en ciberseguridad y la capacitación continua del personal, han alineado nuestros esfuerzos con los objetivos estratégicos de la cooperativa, garantizando su preparación para afrontar futuros desafíos tecnológicos y cibernéticos.

Cordialmente;

Gabriel F. Anaya B
Ing. Gabriel Fernando Anaya Blanco
Director SGSI y Tecnología.