Política corporativa de seguridad de la información y ciberseguridad

Introducción

Los ciberataques son una de las principales amenazas mundiales en términos de impacto, tal y como lo ha informado el Foro Económico Mundial en enero de 2024, convirtiendo a la ciberseguridad en uno de los desafíos más importantes de la era digital. Los riesgos asociados con Ciberseguridad fueron ubicados dentro de los 5 principales riesgos que podrán afectar la humanidad en comparación con el año 2023 en donde los ciber riesgos se encontraban dentro de los 10 primeros lugares. Para el 2024 la probabilidad de ocurrencia de los ciber riesgos aumentó considerablemente.

Las nuevas tecnologías emergentes y en especial la inteligencia artificial (IA) se adoptará de forma masiva en 2024, marcando un cambio significativo en la forma en que se prestan servicios y cómo la sociedad interactúa con la tecnología. No obstante, pese a que este avance impulsará una nueva era tecnológica, también presentará nuevos riesgos en ciberseguridad, en donde los delincuentes aprovecharán la IA para encontrar vulnerabilidades y generar ataques cibernéticos complejos, incluyendo malware autónomo y phishing avanzado.

De acuerdo con lo anterior y teniendo en cuenta las constantes amenazas de ciberseguridad a las que la Corporación está expuesta, las cuales puedan vulnerar la seguridad de los sistemas, originando posibles pérdidas de la información y llevando a la Caja a la materialización de riesgos, los cuales a la vez pueden ocasionar impactos económicos, legales, reputacionales y la afectación en la operación de Colsubsidio; se genera la presente Política Corporativa de Seguridad de la Información, la cual es de obligatorio cumplimiento y en donde se describe el marco seguridad de la Información y ciberseguridad que involucra las unidades de servicio, áreas staff y áreas de apoyo de la corporación, con el objetivo de resguardar los activos de información con que cuenta la Caja.

Objetivo general

Garantizar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información de Colsubsidio. Así mismo, asegurar el cumplimiento normativo y la mitigación de riesgos a los cuales puedan estar expuestos.

Objetivos específicos

- Definir la seguridad de la información alineada con la Estrategia corporativa.
- Definir los estándares y procedimientos que regulan el uso de recursos tecnológicos, así como la conducta de los Trabajadores en relación con la seguridad de la información de Colsubsidio.
- Definir las responsabilidades y conductas aceptadas por Colsubsidio para mantener un ambiente seguro asociado con los activos de información.
- Minimizar los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información, en las etapas de modificación, transferencia y acceso no autorizados a los activos de información.
- Generar las directrices y los lineamientos relacionados con el manejo seguro de la información.
- Asegurar que los proyectos de negocio sigan los lineamientos de la política de Seguridad de la Información y las políticas específicas definidas por la Gerencia de tecnología.
- Garantizar la protección y confidencialidad de la información crítica y sensible de Colsubsidio, evitando accesos no autorizados y asegurando que la información solo esté disponible para aquellos que tienen los permisos necesarios.
- Asegurar la integridad de la información, tanto en almacenamiento (nube o Datacenter) como en tránsito, para prevenir modificaciones no autorizadas.
- Establecer planes y procedimientos para la detección temprana, respuesta rápida y recuperación efectiva frente a incidentes de seguridad, buscando disminuir el impacto que puedan generar.
- Crear un ciclo de mejora continuo para adaptarse a las amenazas cambiantes, las tecnologías emergentes y las lecciones aprendidas en incidentes de ciberseguridad.

Alcance

Aplica a todas las Unidades de Servicio (UES), áreas Staff y áreas de apoyo de Colsubsidio, que incluyen: Trabajadores, terceros (proveedores y contratistas), clientes y afiliados que de manera directa o indirecta interactúan con la infraestructura o los activos de información que hacen parte de los negocios o áreas transversales de la caja, quienes serán responsables por el conocimiento, la divulgación y el cumplimiento de la POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y LOS LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y CIBERSEGURIDAD.

Hace parte del alcance toda la información y recursos de valor (Tecnologías de información y de las comunicaciones -TICs-, Instalaciones, y Tecnologías operacionales -OTs-) asociados a ésta, propios de La Caja o gestionados por Terceros. Así mismo, la información generada, transmitida o resguardada por los procesos de la Caja y activos de información incluidos en dichos procesos.

Desarrollo de la política

1. Declaración de la política

1.1. Aspectos generales

- La Alta Dirección de Colsubsidio reconoce la importancia que tiene para la Caja la gestión adecuada de las amenazas de seguridad y ciberseguridad, las cuales pueden llegar a afectar la información, entendiendo que es un activo invaluable que actúa como fuente y soporte para el desarrollo de las operaciones y procesos de la Caja. Por lo anterior, se establece como una prioridad la gestión de la Seguridad de la Información, así como los riesgos asociados, a través de un conjunto de LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y CIBERSEGURIDAD, recursos, estructura tecnológica, controles de seguridad y modelo de gestión, con los cuales se fortalecen las capacidades para prevenir, detectar, responder y recuperar las operaciones de Colsubsidio, ante ataques y amenazas cibernéticas. En Colsubsidio, la protección de la información tiene como objetivo minimizar el impacto en los activos frente a riesgos identificados, buscando mantener un nivel de exposición que garantice la integridad, confidencialidad y disponibilidad, alineándose con las necesidades de los diversos grupos de interés.

Para ello, se definen los siguientes aspectos:

- La información es vital para Colsubsidio, siendo un activo crucial en las operaciones diarias y esencial para alcanzar los objetivos estratégicos. Todos aquellos con acceso autorizado son responsables de su uso adecuado y protección, reconociendo que la información es fundamental para el logro de los objetivos de la Caja.
- Todos los Trabajadores, contratistas vinculados a Colsubsidio tienen la obligación de conocer, comprender, cumplir y hacer cumplir la POLÍTICA CORPORATIVA Y LOS LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, sus principios y anexos técnico-asociados.

- La información personal de los clientes y afiliados, junto con los activos de información de Colsubsidio, deben ser protegidas conforme a la legislación colombiana vigente y según el nivel de clasificación y valoración definido internamente por Colsubsidio.
- La Gerencia de Tecnología y la Gerencia de Riesgos realizarán las evaluaciones periódicas de riesgos en todos los aspectos relacionados con la seguridad de la información. Estas revisiones se llevarán a cabo de manera sistemática, identificando amenazas potenciales, vulnerabilidades y evaluando el impacto asociado. La información recopilada, será utilizada para tomar decisiones informadas sobre la implementación de medidas de seguridad adecuadas.
- En casos donde se identifiquen riesgos que no puedan ser aceptados según los criterios establecidos, la Gerencia de Tecnología y la Gerencia de Riesgos se comprometen a tomar medidas inmediatas para mitigar dichos riesgos, revisando y aprobando los planes de mitigación propuestos, asegurando que sean efectivos y que estén alineados con los objetivos de seguridad de la organización.

1.2. Aspectos particulares

La política está diseñada para definir, implementar, operar y mejorar de forma continua un Modelo de Gestión de Seguridad de la Información, soportado en instrucciones claras, alineados con las necesidades del negocio y los requerimientos regulatorios que apliquen.

Proteger la información creada, procesada, transmitida o resguardada, con el fin de minimizar impactos financieros, operativos, legales y reputacionales debido a un uso incorrecto. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información.
Se parte de la operación de los procesos de negocio, velando por la seguridad de los recursos, las redes de datos, las aplicaciones, bases de datos, y demás componentes tecnológicos que hacen parte de la infraestructura tecnológica de Colsubsidio.

Asegurar la implementación de controles de acceso a la información, sistemas y recursos de red.
Contemplar a la seguridad parte integral del ciclo de vida de los sistemas de información.
La Caja protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Los siguientes LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y CIBERSEGURIDAD hacen parte integral de la presente POLÍTICA.

- Proceso de Adquisición de Tecnología y Desarrollo de Software
- Uso de dispositivos Móviles
- Acceso Remoto a la Red Corporativa
- Uso de los Activos de Información
- Acceso a los sistemas de Información
- Acceso y Uso del Correo Electrónico corporativo

- Uso de Internet Corporativo
- Uso de Redes Sociales
- Uso y Seguridad de los Equipos (Portátiles o Escritorio)
- Instalación y uso de software
- Manejo seguro de información por parte de Proveedores

A medida que se elaboren nuevos lineamientos específicos de seguridad de la información y ciberseguridad, se presentarán al comité de seguridad para la legalización. Así mismo, se publicarán en el Gestor documental de Colsubsidio (Isolucion), para conocimiento de todos los trabajadores.

2. Organización de la seguridad de la información

2.1. Organización interna

Como parte integral para el cumplimiento continuo de la Política, Colsubsidio establece el comité de Seguridad de la Información presidido por la Gerencia de Tecnología, para proveer el apoyo manifiesto en la investigación, gestión, construcción, implementación y mejora continua del modelo de Seguridad y ciberseguridad. El comité de seguridad y ciberseguridad es un órgano consultivo para la administración y el direccionamiento estratégico, conformado por representantes de las áreas relacionadas con la gestión integral de riesgos y seguridad. El Comité se encuentra constituido por:

- Gerencia de Tecnología
- Gerencia de Riesgo y Cumplimiento
- Auditoría Interna
- Como invitados, según necesidad y a demanda, un representante del área Seguridad física, jurídica de la caja, gestión humana, áreas de negocio o cualquier otra área de la organización requerida.

El Comité de Seguridad de la Información y ciberseguridad es el ente dentro de la organización responsable por proponer, definir y formalizar los Lineamientos específicos de seguridad de la Información y Ciberseguridad, así como de verificar su cumplimiento. Es responsable por el mantenimiento y mejora continua del sistema de gestión de Seguridad de la Información.

Cada miembro de este comité deberá, contar con un suplente que esté en Capacidad de Cumplir y Tomar Decisiones en ausencia del titular responsable. De igual manera el comité de Seguridad de la información y ciberseguridad tendrá una periodicidad bimensual y será citado por la Jefatura de Seguridad Informática de la Gerencia de Tecnología. De igual forma podrán ser citadas sesiones extraordinarias según necesidad.

3. Roles y responsabilidades

Trabajadores

Cumplir con los lineamientos expuestos en la POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y LOS LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y CIBERSEGURIDAD en los cuales se describe el detalle de las obligaciones que los Trabajadores deben tener, respecto al manejo de los activos tecnológicos y la información de Colsubsidio.

Así mismo, es obligación de los Trabajadores, reportar incidentes de Seguridad de la información y Ciberseguridad al buzón de correo descrito para tal fin, o a la mesa de servicio.

Gerencia de Tecnología

- Identificar, evaluar, gestionar y reportar los riesgos e incidentes de Seguridad de la Información y Ciberseguridad inherentes a los productos, procesos y sistemas de seguridad que se identifiquen.
- Administrar las diferentes herramientas y plataformas de seguridad y ciberseguridad.
- Mantener las configuraciones seguras de la infraestructura tecnológica, los dispositivos, software actualizado y parches de seguridad.
- Configurar de forma segura la red, para administrar y proteger adecuadamente el acceso y tráfico de información.
- Mantener el inventario de dispositivos, activos tecnológicos y software relacionado.
- Gestionar el acceso a las aplicaciones y servicios de TI bajo el modelo de roles y perfiles.
- Mitigar los riesgos asociados a Seguridad de la Información y Ciberseguridad en los procesos e infraestructura tecnológica de Colsubsidio.
- Gestionar el cierre de vulnerabilidades detectadas sobre la infraestructura tecnológica del Colsubsidio.
- Monitorear correlacionar y alertar eventos inusuales, amenazas y posibles ataques cibernéticos o incidentes de seguridad o ciberseguridad.
- Implementar procesos y controles tecnológicos para Detectar, responder y recuperar ante amenazas y ataques cibernéticos identificados
- Asegurar la disponibilidad de los sistemas y datos esenciales para las operaciones comerciales de Colsubsidio. Para ello es necesario implementar medidas preventivas desde el frente técnico que mitiguen interrupciones no planificadas, ya sea por incidentes de seguridad, desastres naturales o fallos técnicos.
- Fomentar una cultura de seguridad de la información dentro de Colsubsidio, mediante programas de concientización y formación continua. De igual manera, trabajar para que los trabajadores comprendan los riesgos asociados con la seguridad de la información y adopten prácticas seguras en el uso diario de la tecnología.

Gerencia de Riesgos

- Realizar el análisis de riesgos de seguridad y Ciberseguridad de la infraestructura tecnológica de Colsubsidio, enfocado a la identificación y mitigación de estos. Lo anterior acompañado de la Gerencia de Tecnología.
- Hacer seguimiento al cumplimiento de la Política Corporativa y a los Lineamientos Específicos de seguridad y ciberseguridad.
- Definir en conjunto con la Gerencia de tecnología los controles que ayuden a optimizar el riesgo residual de seguridad.
- Definir y estructurar el plan de continuidad de negocio y el plan de DRP.
- Desarrollar e implementar un proceso estructurado para la identificación, evaluación y gestión de riesgos relacionados con la seguridad de la información, minimizando la exposición de amenazas y garantizando una respuesta efectiva en caso de incidentes.
- Certificar el cumplimiento de las leyes, regulaciones y normativas pertinentes en el manejo de la información. Esto incluye la protección de la privacidad, el respeto a las regulaciones de la industria y la respuesta adecuada a requisitos legales en caso de incidentes de seguridad.

4. Consecuencias

El incumplimiento de la presente POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y LOS LINEAMIENTOS EPECÍFICOS DE SEGURIDAD Y CIBERSEGURIDAD por parte de los Trabajadores independiente del tipo de contrato, son causales para que Colsubsidio pueda realizar acciones disciplinarias. Lo anterior, dando cumplimiento a los acuerdos contractuales establecidos.
Con respecto al incumplimiento por parte de los proveedores, se podrá generar:

- Sanciones a nivel contractual, a través de las cláusulas definidas para tal fin.
- Los casos de incumplimiento serán escalados con el área de compras y contratación para que evalúen la suspensión, cancelación o no renovación del contrato.

5. Entrada en vigencia de la política de seguridad de la información y ciberseguridad

La presente política aplica a partir de la fecha de firma por el Director Administrativo y se revisará de manera anual en el Comité de Seguridad y Ciberseguridad o antes si el comité lo decide. El monitoreo de cumplimiento a la presente política estará en cabeza del Comité de Seguridad de la Información o a quien este designe.