POLÍTICA CORPORATIVA DE CIBERSEGURIDAD

Versión	Descripción de cambios	Aprobación	Vigencia
1.0	Versión inicial	Comité de Ciberseguridad	Diciembre 2018
2.0	Actualización de conceptos y participantes del comité de ciberseguridad	Comité de Ciberseguridad	Julio 2021
3.0	Actualización de marcos normativos aplicables y principios generales	Comité de Ciberseguridad	Junio 2025

INDICE

1. Objetivo

La presente política corporativa proporciona un marco de actuación y compromiso, que permita definir procesos de gestión eficaces de seguridad a los activos de la Información de Andina, entendiéndose como tal, a todos aquellos elementos relevantes para la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para Andina independiente de su formato, medio o soporte que la contenga; y los equipos, redes y sistemas que soportan esta información y que permiten desarrollar las actividades comerciales y/o empresariales de Andina, incluyendo las versiones en producción, de desarrollo, test, pre-producción o cualesquiera otras que fueran utilizadas en las distintas fases de la prestación de los Servicios. Este marco referencial busca generar un modelo de control para el resguardo de la confidencialidad, integridad y disponibilidad de los activos de la Información, y cumplir con las leyes y reglamentos vigentes conforme con la normativa de los países en los que se tiene presencia, manteniendo un equilibrio entre los niveles de riesgo y el uso eficiente de los recursos.

2. Alcance

Esta política y los documentos que se desprendan de ella, son extensibles a todo el personal de Coca-Cola Andina, sus filiales y terceros que le presten servicios vinculados con las materias normadas, así como, a los grupos de interés que accedan a la información de Coca-Cola Andina. A menos que se especifique lo contrario, esta Política debe ser adoptada e integrada en el quehacer diario por todo el personal de Coca-Cola Andina y sus filiales. El manual de uso de activos de información digital establece las directrices aplicables a todo el personal.

3. Política de Ciberseguridad

La presente Política es el documento principal del marco normativo de ciberseguridad, de la cual se desprenden normas, estándares, procedimientos y/o manuales, que cubren ámbitos de Ciberseguridad asociada entre otros a:

- Recursos Humanos: Norma que establece la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad de la información que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de ciberseguridad.

- Seguridad Lógica: Norma que establece las directrices destinadas a garantizar la seguridad en el uso de los sistemas de información, con el fin de proteger la confidencialidad, integridad y disponibilidad de los recursos de información crítica de Coca-Cola Andina.
- Desarrollo digital seguro: Norma que define las directrices generales de seguridad de la información para el desarrollo, adquisición o mantención de los sistemas de información de Coca-Cola Andina conforme al ciclo de vida del desarrollo de software y al marco metodológico aplicado.
- Seguridad Física: Norma que define los lineamientos para la aplicación de controles que prevengan las amenazas físicas a las instalaciones y recursos críticos de la empresa, evitando accesos físicos no autorizados y daños a los equipos de procesamiento de información o interrupciones de sistemas.
- Uso de activos de información digital, aplicaciones y dispositivos tecnológicos: Manual que establece los lineamientos específicos de seguridad para el resguardo y uso aceptable que cada uno de los colaboradores es responsable de aplicar sobre los activos de información digital, aplicaciones y dispositivos tecnológicos entregados por la empresa, como las herramientas de colaboración, correo electrónico, video conferencia, mensajería instantánea, y los dispositivos digitales, computadores, notebook, celulares, equipos móviles, y sus accesos a internet para el intercambio digital de información, a fin de protegerlos de múltiples amenazas internas o externas, garantizando la integridad, confidencialidad y disponibilidad de los recursos que la empresa pone a disposición de los colaboradores para el cumplimiento de su tarea y para la utilización fundamentalmente para propósitos de negocio de la empresa y desarrollo de las funciones encomendadas.
- Gestión de riesgos de TI: Metodología que contiene los lineamientos necesarios para realizar un proceso adecuado para la evaluación, medición y gestión de los riesgos asociados a la tecnología.
- Monitoreo de Ciberseguridad: Norma asociada a la ejecución de análisis de riesgo y auditorías periódicas o bajo demanda, con el objeto de constatar el cumplimiento de las políticas de seguridad de la información, para detectar posibles brechas de seguridad las cuales requieran acciones correctivas y monitorear las actividades de usuarios o sistemas cuando se considere necesario.

  Formulario Ciberresiliencia proveedores Coca-Cola Andina: Formulario que se aplica para medir los indicadores del estado de madurez con las que determinan los niveles de resiliencia (para los objetivos: Anticipar, Resistir, Recuperar y Evolucionar) correspondientes a la provisión de los servicios de terceros en los ámbitos de IT (Information Technology) y de OT (Operation Technology).
- Seguridad de la Información: Política que tiene como objetivo establecer los lineamientos generales relativos a la responsabilidad, resguardo y gestión de riesgos de la información; así como también, entregar las directrices generales sobre el acceso, manipulación,

procesamiento, transmisión, protección, almacenamiento o cualquier otra actividad que se realice sobre los activos de información de Coca-Cola Andina.

- Plan de respuesta y recuperación ataque cibernético: Plan que asegura la aplicación de un procedimiento rápido y eficaz para actuar ante incidentes en materia de seguridad de la información, en particular los asociados a ataques de ciberseguridad. Este plan incluye además, las medidas para evitar que el daño se extienda, la comunicación de forma correcta del incidente a quien corresponda, tanto dentro como fuera de la empresa y los mecanismos para registrarlo con sus pruebas y evidencias, con objeto de estudiar su origen y evitar que ocurran en un futuro.

3.1 Estructura Normativa

La política de ciberseguridad y los documentos que emanen de ésta, constituyen el marco fundamental dentro del cual se deben insertar las actividades digitales de protección de los activos de la información. Estos lineamientos brindan un conjunto básico de reglas, para las que se deberán formular estándares, procedimientos y/o manuales detallados, que satisfagan los requisitos establecidos en las normas de los ámbitos detallados del punto 3.

3.2 Principios generales

Como directriz general, la ciberseguridad de Coca-Cola Andina:

Agrega valor a la compañía. La ciberseguridad se justifica porque agrega valor a la cadena de procesos y en suma a la empresa en su conjunto.

Es transversal a la compañía. La responsabilidad de la aplicación de controles de ciberseguridad en Coca-Cola Andina no se reduce exclusivamente a la gerencia de Tecnología. Sus principios deben aplicarse también a procesos, políticas y procedimientos comerciales, de negocio, de recursos humanos, financieros, etc. de cada operación y del corporativo. Esta visión integral es la que finalmente contribuye a cumplir los objetivos de ciberseguridad de la compañía.

La construimos todos en un esfuerzo permanente. La ciberseguridad se logra porque todos los colaboradores, en todas las actividades que realizan, piensan y actúan teniendo presente las condiciones de seguridad digital de la información.

Debe estar de acuerdo con las exigencias del medio. Todo esfuerzo por implementar ciberseguridad debe estar conforme a las leyes aplicables, regulaciones, exigencias y estándares de la industria y el mercado donde operamos.

Requiere un responsable y asignación de recursos. Considerando el grado de importancia que Coca-Cola Andina le está asignando a la ciberseguridad, se dedicarán los recursos humanos y financieros necesarios, con el objeto de lograr el nivel de ciberseguridad definido, incluyendo en el presupuesto anual un ítem especialmente dedicado a este objetivo.

Mejora continua. Compromiso en la revisión y actualización constante de las medidas de seguridad para adaptarse a las nuevas amenazas y tecnologías, incluyendo entre otros, la revisión de políticas, manuales, procedimientos, controles de seguridad y la capacitación del personal.

Identificar, Proteger, Detectar, Responder y Recuperar. Potenciar el desarrollo de capacidades de ciberseguridad en 5 pilares principales bajo un modelo de monitoreo continuo para dar respuesta proactiva a amenazas digitales y para asegurar la protección de los activos de la información, ciberactivos y la infraestructura crítica de tecnología, que se gestiona en Coca-Cola Andina y sus filiales en todos los países donde posee operaciones.

3.3 Lineamientos y conceptos claves:

Ciberseguridad, concepto que comprende el conjunto de acciones para la protección de la información presente en el ciberespacio, así como de la infraestructura que la soporta.

Ciberespacio, entorno virtual que engloba todos los sistemas de tecnología de la información, que se apoyan en la disponibilidad de una red privada o pública que permite la interacción digital de datos.

El framework de trabajo y control implementado en la organización, se basa en un subconjunto de recomendaciones y practicas extraídos de los estándares definidos en las normas CIS (CSC 7.1), COBIT 5, ISO (ISO 27001 / 27002:2013), NIST (NIST SP 800-53 Rev. 4 / NIST 800-82 rev2 y NIST CSF v1.1).

La información, procesos y sistemas de apoyo, son activos críticos para el negocio, debiendo ser resguardados cuidadosamente y en todo momento por todos los colaboradores y proveedores.

La obtención y mantención de niveles de ciberseguridad requeridos, tiene asociada inversiones y costos. Coca-Cola Andina se orienta a un equilibrio entre estándares de seguridad del mercado, de The Coca-Cola Company, del nivel de riesgo tolerable para el directorio y la inversión y costos que esto significa.

3.4 Estructura, Roles y responsabilidades

Para la gestión estratégica de la ciberseguridad se ha definido un Comité cuyo rol es revisar y aprobar la dirección y estrategia en los temas de ciberseguridad y contingencia que presente la Gerencia de Seguridad de Tecnología, así como, definir el nivel de ciberseguridad que debe tener la compañía, como también las normas y/o procedimientos que se publiquen. El comité de ciberseguridad será coordinado por la Gerencia de Seguridad de Tecnología. Este comité de ciberseguridad sesionará anualmente o cada vez que se necesite por temas contingentes o toma de decisiones y está formado por el Gerente Corporativo de Recursos Humanos, Gerente Corporativo de Legales, Gerente Corporativo de Tecnología, Gerente Corporativo de Control de Gestión, Riesgo y Sustentabilidad, Representante Gerencia Corporativa de Auditoría Interna y Gerente de Seguridad de Tecnología.

La Gerencia de Seguridad TI es responsable de elaborar, promover y coordinar la implementación de acciones e iniciativas de seguridad y contingencia tecnológica a nivel corporativo.

Los equipos de tecnología, representados por los gerentes, líderes técnicos, arquitectos y especialistas, son los principales responsables de que al interior de sus células y áreas de trabajo de su respectivo ámbito, se respeten las políticas, normas, estándares y los procedimientos de seguridad asociados.

Es responsabilidad de todo el personal de Coca-Cola Andina trabajar respetando las políticas, normas y procedimientos de seguridad definidos, en especial, realizando los controles, capacitaciones y procesos de concientización definidos, para minimizar los riesgos en el manejo de la información digital que necesita para cumplir sus funciones. En ninguna circunstancia ni pretexto, las personas enunciadas en el Alcance, podrán incurrir en conductas ilícitas a través de, o en relación con, los activos de información de la Compañía; ni siquiera bajo pretexto de estar cumpliendo instrucciones superiores o que el resultado del delito fuere en beneficio de Coca-Cola Andina. El no cumplimiento de las políticas, normas, procedimientos y manuales relacionados con la presente política y las que se desprenden de esta, como también, el uso impropio y/o ilegal de los activos de la información puede llevar a una acción disciplinaria e incluso al despido o desvinculación del trabajador y demás acciones legales que procedan según se describen y se identifican en los Reglamentos Internos de Orden, Higiene y Seguridad de cada operación.

Todo colaborador tiene la obligación de notificar por lo medios dispuestos para tal efecto cualquier incidente, vulnerabilidad, actividad o situación que afecte la seguridad de los activos de información de la empresa.

El rol de auditoría interna es entregar una mirada independiente de los modelos de control que se implementen, para cumplir con las directrices que se aprueben, comuniquen y publiquen como

resultado de las sesiones del comité y por lo tanto, su participación en el mismo está exenta de aprobación o rechazo de los temas que se sometan a consulta.

4. Plazo de transición

Esta nueva versión de la política no posee plazo de transición y será aplicada en forma inmediata a partir de su publicación.

5. Control de cambios

Versión	Descripción de los principales cambios (para mayores antecedentes, escribir a politicascorporativas@koandina.com)	Aprobación	Vigencia
1.0	Versión inicial	Comité de Ciberseguridad	Diciembre 2018
2.0	Actualización de conceptos y participantes del comité de ciberseguridad	Comité de Ciberseguridad	Julio 2021
3.0	Actualización de marcos normativos aplicables y principios generales	Comité de Ciberseguridad	Junio 2025