



1. Introducción

- 1.1.** La misión de BBC es proporcionar a los clientes aditivos para el procesamiento de termoplásticos y termofijos en diversos segmentos como calzados, juguetes, perfiles rígidos, forros, películas, lonas, hilos y cables, entre otros, con una calidad y un rendimiento superiores, entablando así sólidas relaciones de largo plazo.
- 1.2.** BBC entiende que la información corporativa es un bien esencial para sus actividades y para proteger la calidad y garantía de los productos que ofrece a sus clientes.
- 1.3.** BBC entiende que la manipulación de la información pasa por diferentes medios de soporte, almacenamiento y comunicación, los cuales son vulnerables a factores externos e internos que pueden afectar la seguridad de la información corporativa.
- 1.4.** De esta forma, BBC establece su Política General de Seguridad de la Información, como parte integrante de su sistema de gestión corporativa, en sintonía con las buenas prácticas y las normas internacionalmente aceptadas, con el objetivo de garantizar niveles adecuados de protección a la información de la organización o bajo su responsabilidad.

2. Objetivo

- 2.1.** El objetivo de esta política es establecer directrices y normas de seguridad de la información que permitan a los colaboradores de BBC adoptar pautas de comportamiento seguro, adecuadas a las metas y necesidades de BBC;
- 2.2.** Orientar en cuanto a la adopción de controles y procesos para cumplir los requisitos relativos a la seguridad de la información;
- 2.3.** Proteger la información de BBC, garantizando requisitos básicos de confidencialidad, integridad y disponibilidad;
- 2.4.** Prevenir posibles causas de incidentes y responsabilidad legal de la institución, así como de sus empleados, clientes y socios;
- 2.5.** Minimizar los riesgos de pérdidas financieras, de participación en el mercado, de la confianza de los clientes o de cualquier otro impacto negativo en el negocio de BBC como resultado de fallos de seguridad.

3. Alcance

- 3.1.** Esta política se aplica a todos los usuarios de la información de BBC, incluida cualquier persona u organización que tenga o haya tenido vínculos con BBC, como empleados, exempleados, prestadores de servicios, exprestadores de servicios, colaboradores, excolaboradores, que hayan tenido, tengan o vayan a tener acceso a la información de BBC y/o hayan hecho, hagan o vayan a hacer uso de recursos informáticos contenidos en la infraestructura de BBC.

4. Directrices

4.1. El objetivo de la gestión de seguridad de la información de BBC es garantizar la gestión sistemática y efectiva de todos los aspectos relacionados con la seguridad de la información, respaldando las operaciones críticas del negocio y minimizando los riesgos identificados y sus eventuales impactos en la institución.

4.2. La Presidencia, la Dirección Ejecutiva y el Comité Gestor de Seguridad de la Información están comprometidos con una gestión efectiva de la seguridad de la información de BBC. De esta forma, adoptan todas las medidas pertinentes para garantizar que esta política se comunique, entienda y observe adecuadamente, en todos los niveles de la organización. Se harán revisiones periódicas para garantizar su continua pertinencia y adecuación a las necesidades de BBC.

4.3. Es política de BBC:

- 4.3.1. Elaborar, implantar y observar en su totalidad políticas, normas y procedimientos de seguridad de la información, a fin de garantizar que los requisitos básicos de confidencialidad, integridad y disponibilidad de la información de BBC se cumplan mediante la adopción de controles contra amenazas provenientes de fuentes tanto externas como internas;
- 4.3.2. Poner políticas, normas y procedimientos de seguridad a disposición de todas las partes interesadas y autorizadas, como empleados, terceros contratados y, cuando corresponda, clientes.
- 4.3.3. Garantizar la educación y concienciación respecto a las prácticas de seguridad de la información adoptadas por BBC para empleados, terceros contratados y, cuando corresponda, clientes.
- 4.3.4. Cumplir integralmente los requisitos de seguridad de la información aplicables o exigidos por reglamentos, leyes y/o cláusulas contractuales;
- 4.3.5. Tratar integralmente incidentes de seguridad de la información, garantizando que estos sean adecuadamente registrados, clasificados, investigados, corregidos, documentados y, cuando corresponda, comunicados a las autoridades pertinentes;
- 4.3.6. Asegurar la continuidad del negocio mediante la adopción, implementación, pruebas y mejora continua de planes de continuidad y recuperación ante desastres;
- 4.3.7. Mejorar continuamente la gestión de la seguridad de la información mediante la definición y revisión sistemática de los objetivos de seguridad en todos los niveles de la organización.

Elaboración: Renata Brostel Gerente de Desarrollo	Aprovación: Jose Antonio Ramos da Silva Director Superintendente	Date: 01/08/2022
--	---	----------------------------

Roles y responsabilidades

4.4. COMITÉ GESTOR DE SEGURIDAD DE LA INFORMACIÓN - CGSI

4.4.1. Queda constituido el COMITÉ GESTOR DE SEGURIDAD DE LA INFORMACIÓN, que cuenta con la participación de como mínimo un representante de la Dirección y un miembro sénior de las siguientes áreas: Tecnología y Seguridad de la Información (GreenTec), Recursos Humanos, Compras, Ventas, Contabilidad, Seguridad Laboral y Desarrollo de Productos / Laboratorio.

4.4.2. Es responsabilidad del CGSI:

- 4.4.2.1. Analizar, revisar y proponer la aprobación de políticas y normas relacionadas con la seguridad de la información;
- 4.4.2.2. Garantizar la disponibilidad de los recursos necesarios para una eficaz gestión de la seguridad de la información;
- 4.4.2.3. Garantizar que las actividades de seguridad de la información se lleven a cabo de conformidad con la PGSI;
- 4.4.2.4. Promover la divulgación de la PGSI y tomar las medidas necesarias para difundir una cultura de seguridad de la información en el entorno de BBC.

4.5. GERENCIA DE SEGURIDAD DE LA INFORMACIÓN

4.5.1. Es responsabilidad de la Gerencia de Seguridad de la Información:

- 4.5.1.1. Llevar a cabo la gestión y operación de la seguridad de la información, teniendo como base esta política y demás resoluciones del CGSI;
- 4.5.1.2. Apoyar al CGSI en sus deliberaciones;
- 4.5.1.3. Elaborar y proponer al CGSI las normas y procedimientos de seguridad de la información, necesarios para hacer cumplir la PGSI;
- 4.5.1.4. Identificar y evaluar las principales amenazas contra la seguridad de la información, así como proponer y, cuando se apruebe, implementar medidas correctivas para reducir el riesgo;
- 4.5.1.5. Tomar las medidas pertinentes para hacer cumplir los términos de esta política;



- 4.5.1.6.** Gestionar los incidentes de seguridad de la información, garantizando un tratamiento adecuado.

4.6. GESTORES DE LA INFORMACIÓN

4.6.1. Es responsabilidad de los gestores de la información:

- 4.6.1.1. Gestionar la información generada o bajo responsabilidad de su área de negocio durante todo su ciclo de vida, incluidas su creación, manipulación y eliminación de acuerdo con las normas establecidas por BBC;
- 4.6.1.2. Identificar, clasificar y etiquetar la información generada o bajo responsabilidad de su área de negocio de acuerdo con las normas, criterios y procedimientos adoptados por BBC;
- 4.6.1.3. Revisar periódicamente la información generada o bajo responsabilidad de su área de negocio, ajustando su clasificación y etiquetado según sea necesario;
- 4.6.1.4. Autorizar y revisar los accesos a la información y sistemas de información bajo su responsabilidad;
- 4.6.1.5. Solicitar la concesión o revocación de acceso a la información o sistemas de información de acuerdo con los procedimientos adoptados por BBC.

4.7. USUARIOS DE LA INFORMACIÓN

4.7.1. Es responsabilidad de los usuarios de la información:

- 4.7.1.1. Leer, comprender y cumplir integralmente los términos de la Política General de Seguridad de la Información, así como las demás normas y procedimientos de seguridad aplicables;
- 4.7.1.2. Remitir cualquier duda y/o pedido de aclaración sobre la Política General de Seguridad de la Información, sus normas y procedimientos a la Gerencia de Seguridad de la Información o, cuando corresponda, al Comité Gestor de Seguridad de la Información;
- 4.7.1.3. Comunicar a la Gerencia de Seguridad de la Información cualquier evento que infrinja esta Política o que ponga/pueda poner en riesgo la seguridad de la información o de los recursos computacionales de BBC;



- 4.7.1.4. Firmar el Término de Uso de Sistemas de Información de BBC, formalizando la concienciación y la aceptación integral de las disposiciones de la Política General de Seguridad de la Información, así como de las demás normas y procedimientos de seguridad, asumiendo la responsabilidad de su cumplimiento;
- 4.7.1.5. Responder de la inobservancia de la Política General de Seguridad de la Información, normas y procedimientos de seguridad, como se define en el apartado Sanciones y castigos.

5. Sanciones y castigos

- 5.1. Aunque sean resultado de mera omisión o intento no consumado, las infracciones de esta política, así como de las demás normas y procedimientos de seguridad, serán pasibles de sanciones tales como advertencia verbal, advertencia por escrito, suspensión no remunerada y el despido por justa causa, entre otras;
- 5.2. La aplicación de sanciones y castigos se realizará de acuerdo con el análisis del Comité Gestor de Seguridad de la Información, el cual deberá tener en cuenta la gravedad de la infracción, el efecto alcanzado, la recurrencia y las hipótesis previstas en el artículo 482 de la Consolidación de las Leyes del Trabajo, pudiendo el CGSI, en el uso del poder disciplinario que le es atribuido, aplicar la pena que considere conveniente cuando se tipifique falta grave.
- 5.3. En el caso de terceros contratados o prestadores de servicio, el CGSI debe analizar el incidente y deliberar sobre la aplicación de las sanciones y castigos de acuerdo con los términos previstos en el contrato;
- 5.4. En el caso de infracciones que supongan actividades ilegales, o que puedan causar daños a BBC, el infractor será responsable de los perjuicios, cabiendo la aplicación de las medidas judiciales pertinentes sin perjuicio de los términos estipulados en los puntos 6.1, 6.2 y 6.3 de esta política.

6. Casos Omisos

- 6.1. Los casos omisos serán evaluados por el Comité Gestor de Seguridad de la Información para su posterior deliberación.
- 6.2. Las directrices establecidas en esta política y en las demás normas y procedimientos de seguridad no se agotan en virtud de la continua evolución tecnológica y el constante surgimiento de nuevas amenazas. De esta forma, no se constituye una descripción enumerativa, siendo obligación del usuario de la información de BBC adoptar, siempre que sea posible, otras medidas de seguridad, además de las aquí previstas, con el objetivo de garantizar la protección de la información de BBC.

7. Glosario

- 7.1. Amenaza:** posible causa de un incidente, que podría perjudicar a BBC;
- 7.2. Activo:** todo lo que tiene valor para BBC;
- 7.3. Activo de información:** patrimonio intangible de BBC, constituido por información de cualquier naturaleza, ya sea de carácter estratégico, técnico, administrativo, financiero, mercadológico, de recursos humanos, legal, naturaleza, así como cualquier información creada o adquirida por medio de asociación, adquisición, licencia, compra, o confiada a BBC por socios, clientes, empleados y terceros, en formato escrito, verbal, físico o digitalizado, almacenada, que haya transitado o esté en tránsito por la infraestructura computacional de BBC o por una infraestructura externa contratada por la organización, además de los documentos en soporte físico, o medios electrónicos que hayan transitado dentro y fuera de su estructura física.
- 7.4. COMITÉ GESTOR DE SEGURIDAD DE LA INFORMACIÓN - CGSI:** grupo de trabajo multidisciplinario permanente, confirmado por la Dirección de BBC, que tiene por finalidad tratar cuestiones relacionadas con la seguridad de la información.
- 7.5. Confidencialidad:** propiedad de los activos de la información de BBC de no estar disponibles o ser divulgados a individuos, procesos o entidades no autorizadas.
- 7.6. Control:** medida de seguridad adoptada por BBC para tratar un riesgo específico.
- 7.7. Disponibilidad:** propiedad de los activos de la información de BBC de ser accesibles y utilizables a petición, por partes autorizadas.
- 7.8. Gestor de la información:** usuario de la información que ocupa un cargo específico, al que se atribuyó la responsabilidad de uno o más activos de información creados, adquiridos, manipulados o puestos bajo la responsabilidad de su área de actuación.
- 7.9. Incidente de seguridad de la información:** un evento o conjunto de eventos de seguridad de la información no deseados con una posibilidad significativa de afectar las operaciones o amenazar la información de BBC.
- 7.10. Integridad:** propiedad de los activos de información de BBC de ser exactos y completos.
- 7.11. Riesgo de seguridad de la información:** efecto de la incertidumbre sobre los objetivos de seguridad de la información de BBC.



7.12. Seguridad de la información: la preservación de las propiedades de confidencialidad, integridad y disponibilidad de la información de BBC.

7.13. Usuario de la información: empleados con un vínculo laboral, de cualquier área de BBC, o terceros asignados a la prestación de servicios a BBC, con independencia del régimen jurídico al que estén sometidos, así como otros individuos u organizaciones debidamente autorizados a utilizar y manipular cualquier activo de información de BBC para el desempeño de sus actividades profesionales.

7.14. Vulnerabilidad: causa potencial de un incidente de seguridad de la información, que podría perjudicar las operaciones o amenazar la información de BBC.

8. Revisiones

Esta política se revisa anualmente o de acuerdo con el parecer del Comité Gestor de Seguridad de la Información.