Anexo 31. Políticas de Seguridad de la Información y Ciberseguridad.

OBJETIVOS

Principal

Proteger la información de la Bolsa Mercantil de Colombia y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad, privacidad y confiabilidad de la información.

El objetivo principal se respalda en los siguientes objetivos específicos:

- Asegurar la implementación de las medidas de seguridad de la información y ciberseguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener la Política General de Seguridad, Ciberseguridad y Privacidad de la Información de la BOLSA MERCANTIL actualizada, a efectos de asegurar su vigencia y nivel de efectividad.
- Definir, implementar, operar y mejorar de forma continua un modelo de seguridad, ciberseguridad y privacidad de la información, soportado en lineamientos claros enfocados a las necesidades de sus partes interesadas.

ALCANCE/APLICABILIDAD

La presente Política General de Seguridad, Ciberseguridad y Privacidad de la Información se dicta en cumplimiento de las disposiciones legales vigentes y para atender la expectativa de las partes interesadas.

Aplica también en todo el ámbito de la Bolsa Mercantil, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la compañía a través de contratos o acuerdos con terceros.

La presente política debe ser cumplida por parte de la Junta Directiva, la Alta Gerencia y todos los colaboradores de la Bolsa, incluyendo pasantes y/o practicantes, así como colaboradores contratados bajo la modalidad de outsourcing, proveedores siempre y cuando el objeto de los bienes y/o servicios afecten los activos de información, sociedades comisionistas de bolsa, participantes de los mercados y entes de control externos, independiente de cual fuere su nivel jerárquico. De igual manera se pone a disposición de las personas vinculadas a las sociedades comisionistas miembros de la Bolsa para su cumplimiento.

DEFINICIONES

- **ADMINISTRACIÓN DE RIESGOS**

Se entiende por administración de riesgos el proceso de identificación, medición, control y mitigación, a un costo aceptable, de los riesgos de seguridad que pueden afectar a la información. Dicho proceso es cíclico y es llevado a cabo en forma periódica mediante la actividad de monitoreo.

- **AGENTE DE ANTIVIRUS**

Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos o maliciosos en sistemas informáticos.

- **BOLSA MERCANTIL**

BMC Bolsa Mercantil de Colombia S.A.

- **CIBERSEGURIDAD**

El desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la organización.

- **CLIENTE**

Equipo informático cuyo papel habitual es el de consumir servicios ofertados por otros equipos informáticos. Es el caso de los ordenadores personales situados en los puestos de trabajo.

- **CORREO ELECTRÓNICO:**

Servicio de red que permite a los clientes enviar y recibir mensajes electrónicos de textos, imágenes, videos, audio, u otros contenidos, mediante sistemas de comunicación electrónicos.

- **EVALUACIÓN DE RIESGOS**

Se entiende por evaluación de riesgos el análisis de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, para determinar la probabilidad de que ocurran y su potencial impacto en la operación de la BOLSA MERCANTIL.

- **IDENTIFICACIÓN Y AUTENTICACIÓN**

Corresponde al registro de un usuario en un sistema de información que permite identificarlo plenamente mediante el nombre de usuario y clave.

- **INCIDENTE DE SEGURIDAD**

Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la organización que son esenciales para el negocio.

- **INFORMACIÓN**

Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **INSTANCIA EN NUBE**

Es un servidor virtual en la nube, donde se instala y configura el sistema operativo, aplicaciones u otros servicios tecnológicos.

- **PROPIETARIO DE LA INFORMACIÓN**

Debe ser entendido desde su acepción técnica, no jurídica. Es decir, los usuarios definidos con esta responsabilidad en la matriz de activos de información o documento equivalente.

- **RESPONSABLE**

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la BOLSA MERCANTIL que así lo requieran.

- **RECURSO INFORMÁTICO**

Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

- **SEGURIDAD DE LA INFORMACIÓN**

El conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización.

- **SISTEMA DE INFORMACIÓN**

Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **SISTEMA MISIONAL**

Corresponde a los sistemas que soportan la operación CORE del negocio en la BOLSA MERCANTIL.

- **TECNOLOGÍA DE LA INFORMACIÓN**

Se refiere al hardware y software operados por la Bolsa Mercantil o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Bolsa Mercantil sin tener en cuenta la tecnología utilizada.

- **USUARIO**

Cualquier persona que utilice la infraestructura de red de la BOLSA MERCANTIL.

- **USUARIO INFORMACIÓN**

Se refiere tanto usuario interno (colaborador), como usuario externo (Firmas Comisionistas, Organismos de Control, proveedores), que haga uso de la información de la Bolsa Mercantil.

- **USUARIOS TERCEROS**

(Personal Temporal, personal de Órganos de Control): Todas aquellas personas naturales o jurídicas, que no son colaboradores de la BOLSA MERCANTIL, pero que por las actividades que realizan en la compañía, deban tener acceso a recursos informáticos.

- **ZONA DE SEGURIDAD**

Conjunto de nodos de una red que comparten finalidad, condiciones de conectividad, medidas de seguridad y modelo de asignación de ancho de banda.

POLÍTICA

Esta Política protege a la organización de una amplia gama de amenazas, a fin de garantizar la confidencialidad, integridad, disponibilidad, legalidad, privacidad y confiabilidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la BMC, Bolsa Mercantil S.A., en adelante, Bolsa Mercantil indistintamente o BMC.

Los principios de esta Política son parte de la cultura organizacional, ya que existe compromiso de la Alta Gerencia y de los Gerentes, Directores y Coordinadores para su difusión, consolidación y cumplimiento.

Esta Política incluye una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen:

- **Organización de la Seguridad:** Orientado a administrar la seguridad de la información dentro de la BOLSA MERCANTIL y establece un marco gerencial para controlar su implementación.

- **Seguridad de los recursos humanos:** Orientado a la adecuada aplicación de procesos de selección, contratación, desarrollo y retiro del personal.

- **Clasificación y Control de Activos:** Destinado a mantener una adecuada protección de los activos de información de la BOLSA MERCANTIL.

- **Control de accesos**: Asegurar el oportuno acceso a los sistemas de información de acuerdo con los perfiles definidos y los privilegios asignados, así como denegar los accesos no autorizados.

- **Cifrado**: Proteger la información clasificada como confidencial usando mecanismos que impidan su modificación y/o visualización por personas no autorizadas.

- **Seguridad Física:** Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información de la BOLSA MERCANTIL.

- **Gestión de las Comunicaciones y la Operatividad del negocio:** Dirigido a garantizar el funcionamiento correcto y seguro de los mecanismos y dispositivos de procesamiento de la información y medios de comunicación.

- **Desarrollo y Mantenimiento de los Sistemas:** Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

- **Relación con proveedores:** Destinado a establecer los riesgos de seguridad de la información asociados a la prestación de los servicios por parte de los proveedores de acuerdo con las directrices adoptadas por la compañía.

- **Incidentes o eventos:** Orientado a adoptar procedimientos que permitan reportar incidentes o eventos de seguridad de la información a la Bolsa de manera oportuna para una efectiva gestión de estos.

- **Administración de la continuidad de las actividades:** Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres, los cuales deberán ser concordantes y coordinados con los planes de contingencia y continuidad de la Bolsa Mercantil.

- **Cumplimiento:** Destinado a evitar infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos relacionados con la seguridad de información; y de los requisitos de seguridad establecidos en este documento.

La Gerencia Corporativa de Riesgos revisará anualmente la presente Política, a efectos de mantenerla actualizada. Así mismo, presentará cualquier modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad para la aprobación de la Junta Directiva. Podrá sufrir modificaciones futuras, de acuerdo con las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

El presente documento está basado en la norma ISO/IEC 27001:2013, como un marco de referencia para la gestión de la seguridad de la información en la compañía.

4.1. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación de la:

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. Es decir, hace referencia a la protección de información cuya divulgación no está autorizada.

- **Integridad:** La información precisa, coherente y completa desde su creación hasta su destrucción.

- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Adicionalmente, son considerados los siguientes conceptos:

- **Legalidad:** para garantizar el cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la BOLSA MERCANTIL en materia de seguridad de la información y ciberseguridad.

- **Confiabilidad de la Información:** La información debe ser la apropiada para la administración de la compañía y el cumplimiento de sus obligaciones.

- **Autenticidad:** Para asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantizar el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** Los eventos significativos de los sistemas de información son registrados para su control posterior (logs de los diferentes ambientes de producción).

- **Protección a la duplicación:** Para impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. Por lo anterior, una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

- **No repudio:** Para evitar que una compañía que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

4.2. RESPONSABILIDAD Y PRINCIPIOS ORIENTADORES

Esta Política es de aplicación a todos los grupos de interés de la BOLSA MERCANTIL, cualquiera sea su situación, en el proceso al cual se encuentre vinculado y cualquiera sea el nivel de las tareas que desempeñe; por tanto, estos deberán desplegar sus mejores esfuerzos para asegurar que su conducta se ajuste a los más altos niveles de disciplina, profesionalismo y seriedad en aras de preservar el buen funcionamiento de los sistemas y la información, su integridad, confidencialidad, y disponibilidad, así como la confiabilidad del público mismo.

Se consideran violaciones graves el robo, daño, divulgación, secuestro de información reservada o confidencial.

Los miembros de la Junta Directiva en el ejercicio de su cargo deben aplicar la presente Política y en especial preservarán la confidencialidad sobre aquella información que así lo requiera. Así mismo, aplicarán las medidas de seguridad respecto de los sistemas de información a los cuales se les de acceso para el desarrollo de sus funciones.

Si bien todos los colaboradores deben cumplir esta política, la presidencia, los vicepresidentes, gerentes, directores y coordinadores son responsables de la aplicación de esta Política dentro de sus procesos de responsabilidad, así como velar por el cumplimiento de dicha Política por parte de su equipo de trabajo.

La Gerencia Corporativa de Riesgos:

- Revisa y propone a la Junta Directiva políticas de seguridad de la información y las funciones generales en materia de seguridad de la información para su aprobación.

- Monitorea cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

- Toma conocimiento y supervisa la investigación y monitoreo de los incidentes relativos a la seguridad de la información y ciberseguridad.

- Da trámite para obtener la aprobación de las iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada proceso, así como acuerda y aprueba metodologías y procesos específicos relativos a seguridad de la información y ciberseguridad.

- Garantiza que la seguridad sea parte del ciclo de vida de la información.

- Evalúa y coordina la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios. Promueve la difusión y apoyo a la seguridad de la información y ciberseguridad dentro de la BOLSA MERCANTIL.

Teniendo en cuenta que la presente política no se refiere sólo a la seguridad, información tecnológica o ciberseguridad, la Vicepresidencia Financiera y Administrativa será responsable de la seguridad física de la información.

Adicionalmente, la Alta Gerencia, o a quien designe la misma, debe coordinar el proceso de administración de la continuidad de las actividades de la organización.
Los propietarios de la información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de esta, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios tienen permisos de acceso a la información de acuerdo con sus funciones y competencia.

El responsable de Formación y Entrenamiento debe velar porque todo el nuevo personal de la Bolsa, incluyendo los usuarios terceros, conozca sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

Así mismo, tiene a su cargo la notificación de la presente Política a todo el personal con el apoyo de la Gerencia Corporativa de Riesgos; de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad, cláusulas adicionales en los contratos laborales que sean requeridas, acuerdos u otra documentación de la BOLSA MERCANTIL con sus colaboradores y las tareas de capacitación periódica en materia de seguridad.

La Vicepresidencia de Tecnología tiene a su cargo la función de cubrir los requerimientos de seguridad informática y ciberseguridad establecidos para la operación que sean definidos en las directrices de seguridad de la información y por parte de la Gerencia Corporativa de Riesgos, así como la administración y comunicación de los sistemas y recursos de tecnología de la BOLSA MERCANTIL.

Por otra parte, tiene la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

La Vicepresidencia Jurídica y Secretaría General debe verificar la inclusión de cláusulas de cumplimiento de la presente Política y otras que en esta materia sean aplicables en la gestión de todos los contratos con terceros no laborales. Asimismo, asesora en materia legal a la BOLSA MERCANTIL, en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La Gerencia Corporativa de Auditoría Interna es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, y de informar sobre el cumplimiento de los controles establecidos en la presente Política.

La Presidencia de la BOLSA MERCANTIL puede proponer modificaciones y actualizaciones a los términos de la presente Política en cualquier momento. El usuario tiene la responsabilidad de revisar periódicamente la versión más actualizada de estos términos a través del enlace proporcionado para la publicación de estos en la herramienta que para este fin disponga la BOLSA MERCANTIL.

4.3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Bolsa cuenta con un Sistema de Gestión de Seguridad de la Información - SGSI que tiene alcance a todos los productos, proyectos y procesos de la Bolsa toda vez que estos tienen implícitos el uso de activos de información que deben ser protegidos en función del nivel requerido de confidencialidad, integridad y disponibilidad.

Este sistema cuenta con una política general mencionada anteriormente y las siguientes directrices con sus respectivos objetivos:

- **DIRECTRIZ INTERNA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:**
    - Dar a conocer las directrices para la adquisición, desarrollo y mantenimiento de los sistemas de información de la organización, garantizando la seguridad de dichos sistemas.

- **DIRECTRIZ INTERNA DE CONTROL DE ACCESO:**

  Dar a conocer los lineamientos para:
    - Prevenir el acceso no autorizado a los sistemas de información.
    - Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
    - Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
    - Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
    - Restringir el acceso a los programas y archivos y establecer los niveles de acceso.
    - Asegurar que los datos, archivos y programas sean utilizados correctamente.

- **DIRECTRIZ INTERNA DE CONTROLES CRIPTOGRÁFICOS**
    - Establecer las directrices necesarias para proteger la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información de la Bolsa Mercantil de Colombia.

- **DIRECTRIZ INTERNA DE DISPOSITIVOS MÓVILES**
    - Establecer las condiciones para el manejo de los dispositivos móviles que acceden a información de la Bolsa Mercantil de Colombia (BMC), a fin de garantizar y velar por el uso responsable de estos por parte del personal.

- **DIRECTRIZ INTERNA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN**
    - Dar a conocer las directrices para que los activos de información reciban un adecuado manejo y protección.

- **DIRECTRIZ INTERNA DE GESTIÓN DE LAS OPERACIONES Y COMUNICACIONES**
    - Establecer las directrices para garantizar la documentación, mantenimiento y actualización de los procedimientos de operación y administración de la plataforma tecnológica.

- **DIRECTRIZ INTERNA DE RELACIÓN CON TERCEROS**
    - Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

- **DIRECTRIZ INTERNA DE SEGURIDAD DEL RECURSO HUMANO**
    - Establece la directriz general que cumple el proceso de Talento Humano para la selección, capacitación, permanencia y desvinculación de los colaboradores de la Organización.

- **DIRECTRIZ INTERNA DE SEGURIDAD FÍSICA Y DEL ENTORNO**
    - Definir las directrices para prevenir el acceso no autorizado a las instalaciones de la Bolsa y áreas de acceso Restringido, evitar la pérdida y/o daño de los activos de información y la interrupción del negocio.

En relación con estas directrices se ha establecido un plan de monitoreo del cumplimiento de estas y derivado de los resultados de este ejercicio se establecen las oportunidades de mejora en cuanto al fortalecimiento de las medidas de mitigación del riesgo.

Para el correcto funcionamiento del SGSI, la Bolsa aplica una metodología de gestión de los riesgos de seguridad de la información y ciberseguridad de la BOLSA para identificar, medir, controlar y monitorear los riesgos asociados a los activos de información de tal manera que se pueda asegurar la confidencialidad, integridad y disponibilidad de estos.

Para la adecuada articulación del SGSI se cuenta con:

- Una matriz RACI que establece las responsabilidades y segregación de funciones frente al sistema por parte de las distintas áreas y cargos relacionados con este.

- Una matriz de control de acceso en la que se lleva el control de acceso por cargo de los colaboradores a los diferentes sistemas y servicios de información.

- Gestión de vulnerabilidades – Hardening – Ethical Hacking mediante la cual se realiza el escaneo de vulnerabilidades a todos los sitios web expuestos a internet e internos Core del Negocio, sistema operativo de las instancias y servidores, certificados digitales, cumplimiento de línea base de seguridad Hardening, ejercicios de Ethical Hacking y vectores de ataques. Todo lo anterior para validar la exposición, impacto y prevención de ciberataques externos y/o internos.

- Un monitoreo de alertas de Ciberseguridad SOC que se tiene tercerizado, para el servicio de monitoreo de SOC 7x24, contemplando alertas, detección temprana de ciberataques, así como la ejecución de acciones predefinidas en caso de ataques de Ransomware, elevación de privilegios, denegación de servicios, entre otros.

- Monitoreos internos de seguridad de la información y ciberseguridad:
    - Control de instalación de software
    - Alertas antivirus y maliciosas
    - Conexiones remotas
    - Usuarios y perfiles de acceso
    - Actividades de los usuarios administradores

- Gestión de seguridad de la información en proyectos y terceros: Todo proyecto o iniciativa que tenga la compañía pasa por validaciones de seguridad de la información y ciberseguridad; se evalúa la adquisición de software, servicios o contratación de terceros que vayan a tratar información de clientes o de la compañía. Adicionalmente se lleva control y seguimiento a los proveedores críticos.

- Se cuenta con programas de capacitación y sensibilización hacia todos los colaboradores.

- Respecto de la gestión del sistema y de los riesgos de seguridad de la información se presentan informes a la Junta Directiva y el Comité de Riesgos para obtener su retroalimentación en aras de la mejora continua.

- Adicionalmente, la alta gerencia por medio de las auditorías internas y revisoría fiscal, valida el cumplimiento de las políticas y directrices de seguridad de la información de la compañía. El resultado de estas, se presentan al Comité de Auditoría para hacer seguimiento de los planes de acción acordados.

NIVEL DE CUMPLIMIENTO

El incumplimiento de esta Política traerá consigo consecuencias administrativas, disciplinarias, penales y/o las legales que apliquen de acuerdo con la normativa interna vigente e incluyendo aquellas que

competen al Gobierno Nacional en cuanto a Seguridad, Privacidad de la Información, Ciberseguridad y Gobierno Digital que sea referido.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cabal cumplimiento a la presente política.

La BMC Bolsa Mercantil de Colombia ha decidido definir, implementar, operar y mejorar de forma continua un modelo de seguridad, ciberseguridad y privacidad de la información, soportado en lineamientos claros enfocados a las necesidades de sus partes interesadas.

Los lineamientos internos que soportan el modelo de seguridad, ciberseguridad y privacidad de la información de la BMC Bolsa Mercantil de Colombia, deben ser revisados por la Gerencia Corporativa de Riesgos y aprobados por la Presidencia o instancia que esta designe mínimo anualmente, a través de los cuales la BMC Bolsa Mercantil de Colombia garantiza que:

- Las responsabilidades frente al modelo de seguridad, ciberseguridad y privacidad de la información sean definidas, compartidas, publicadas y aceptadas por los grupos de interés de la BMC Bolsa Mercantil de Colombia.
- Se proteja la información creada, procesada, transmitida y/o resguardada por los procesos que intervienen para alcanzar los objetivos estratégicos definidos por la BMC Bolsa Mercantil de Colombia, y en el cumplimiento de las funciones de la organización, con el fin de minimizar impactos financieros, operativos y/o legales debido a un uso incorrecto de ésta. Para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad y/o custodia.
- Se proteja su información frente a amenazas originadas por parte del personal custodio, responsable y/o usuarios de esta.
- Se proteja los centros de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Se controle la operación de sus procesos misionales, garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Se implemente mecanismos de control de acceso a la información, sistemas y recursos de red.
- Se garantice que la seguridad, ciberseguridad y privacidad de la Información sean parte integral del ciclo de vida de los sistemas de información.
- Se garantice, a través de una adecuada gestión de los eventos, la atención de los incidentes de seguridad, ciberseguridad y privacidad de la Información y las vulnerabilidades identificadas y asociadas con los sistemas de información proporcionando una mejora efectiva de su modelo de seguridad.
- Se garantice la continuidad de los procesos críticos de la organización ante eventos que puedan afectar su operación.
- Se garantice el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Todo el personal de la BMC Bolsa Mercantil de Colombia, incluyendo los grupos de interés con acceso a los sistemas de información y/o información de la organización, serán responsables de protegerla de acuerdo a los niveles de acceso, manejo, transferencia y/o destrucción, para garantizar esto, deberán conocer la política general de seguridad, ciberseguridad y privacidad de la información, así como sus

lineamientos internos y demás documentos que apoyen el desarrollo de la misma al interior de la organización, estando en la obligación de manifestar comportamientos incorrectos a nivel de seguridad, ciberseguridad y/o privacidad como parte de su trabajo diario.

La Política General de seguridad, ciberseguridad y privacidad de la Información se encuentra regida por los lineamientos de obligatorio cumplimiento definidos por la Superintendencia Financiera de Colombia - SFC, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y demás organizaciones de control, acorde a lo incorporado en el documento CONPES 3701 de 2011 y 3854 de 2016 para la implementación de dicha política.

ESTRUCTURA DE GOBIERNO.

Junta Directiva: Aprobar la política de seguridad, ciberseguridad y privacidad de la información y hacer seguimiento, pronunciándose sobre la gestión del modelo definido para el cumplimiento de esta y tomar las decisiones que considere pertinentes frente a seguridad de la información, a partir de los reportes que contengan los resultados de la gestión que se generen de las revisiones anuales, semestrales o cuando se requiera por cambios normativos o cuando la situación lo amerite.

Presidencia (CEO- Chief Executive Officer): Su función principal será la de supervisar y velar porque la estrategia definida para el desarrollo, implementación, gestión y seguimiento del modelo de seguridad, ciberseguridad y privacidad de la información en la organización cumpla con la consecución de los objetivos de esta, además de definir revisar y aprobar, directamente o a través de la instancia que esta designe, los principios a seguir dentro de la organización en el marco de la presente política.

Gerencia Corporativa de Riesgos (CISO – Chief Information Security Officer): El rol es ejecutado por el Gerente Corporativo de Riesgos y su función principal es ser el responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna[1] y es el responsable del programa de tratamiento de datos personales en la Organización.

Oficial de Seguridad (CSO - Chief Security Officer): Este rol es ejecutado por un Profesional Senior de la Gerencia Corporativa de Riesgos y su función principal es identificar qué activos de información necesitan protección y cómo deben protegerse emitiendo lineamientos y estrategias, así como liderar la implementación de esas medidas de protección en conjunto con los responsables de los controles.

Vicepresidencia de Tecnología (CTO - Chief Technology Officer): Se encarga de que las organización estén alineadas con la tecnología de la información para lograr los objetivos planificados, de mejorar los procesos de tecnologías de la información de la organización, gestionar los riesgos de TI y la continuidad de negocio en el componente del DRP, controlar el coste en infraestructura de tecnologías de la información, alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, establecer mejoras e innovaciones de soluciones y productos y gestiona del día a día de las tecnologías de la información.

[1] Numeral 3.2.6 Circular Externa 007 de 2018 expedida por la SFC.

Vicepresidencia Financiera y Administrativa (CFO – Chief Financial Officer) – Interacción con CTO: Su función a nivel de seguridad física es la de proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros.

Gerencia Corporativa de Talento Humano: Su rol es el de implementar los controles definidos que garanticen la seguridad de la información necesaria antes de la contratación, durante la ejecución del empleo y después de terminar el empleo o cambiar de rol dentro de la organización.

Vicepresidencia Jurídica y Secretaría General (CLO – Chief Legal Officer): Este rol es ejecutado por el Vicepresidente Jurídico y Secretario General. Su función es Identificar los requisitos legales, estatutarios, reglamentarios y contractuales (no laborales) pertinentes a seguridad, ciberseguridad y privacidad de la información.

Auditoría Interna – Informar al CEO: Este rol es ejecutado por el Gerente Corporativo de Auditoría Interna. Su función principal es planificar, establecer, implementar y mantener uno o varios programas de auditoría de seguridad, ciberseguridad y privacidad de la información que incluyan la frecuencia, métodos, responsabilidades, requisitos de planificación y elaboración de informes, asegurando la objetividad e imparcialidad en los procesos de auditoría e informar los resultados de estas a las instancias que corresponda.