Política de uso y manejo de información reservada, confidencial, privilegiada, sensitiva y restringida

Marzo 2025
Santo Domingo de Guzmán, Distrito Nacional
República Dominicana

Contenido

1. Base legal

El presente documento se elabora en cumplimiento con la Ley núm. 249-17 del Mercado de Valores de la República Dominicana, del 19 de diciembre de 2017, el Reglamento de Información Privilegiada, Hechos Relevantes y Manipulación de Mercado (R-CNMV-2022-10-MV), y las demás normativas complementarias aplicables al mercado de valores dominicano.

2. Objetivo

El presente documento expone la Política de uso y manejo de información reservada, confidencial, privilegiada, sensitiva y restringida de Primma Valores, S. A., Puesto de Bolsa (en adelante, "Primma Valores") con el objetivo de establecer los estándares para salvaguardar la información y la documentación reservada, confidencial, privilegiada, sensitiva y/o restringida. En ese sentido, se establecen los lineamientos respecto al uso no autorizado, la divulgación o revelación, modificación, daño o pérdida de estos tipos de informaciones.

3. Ámbito de aplicación

Esta política podrá ser aplicable, según corresponda, a todas las partes interesadas de Primma Valores, incluyendo, pero no limitado a accionistas, miembros del Consejo de Administración, directores, empleados, relacionados comerciales, consultores, personal por tiempo definido y cualquier otro personal que se relacione o pueda relacionarse con información de carácter reservada, confidencial, privilegiada, sensitiva y/o restringida.

4. Clasificaciones

a) Toda información manejada por Primma Valores, corresponderá a una de cinco clasificaciones de sensibilidad:

- Información reservada
- Información confidencial
- Información privilegiada
- Información sensitiva
- Información restringida

5. Definiciones

b) *Hecho Relevante.* Hecho o evento respecto de un participante del mercado y de su grupo financiero, que pudiera afectar positiva o negativamente su posición jurídica, económica financiera, o el precio de los valores en el mercado.

c) *Información Confidencial.* El acceso a esta información debe ser fuertemente restringido basándose en el concepto de necesidad de saber. Su revelación requiere la aprobación del responsable de la información y, en caso de terceros, un acuerdo firmado de confidencialidad. Los ejemplos incluyen revisiones de rendimiento de empleados y planes de desarrollo de nuevos productos.

d) *Información Engañosa.* Es toda manifestación que, en forma dolosa, busque inducir a error a los inversionistas o afectar su comportamiento, incluyendo la omisión de datos fundamentales, siempre que dicha omisión pueda inducir a error a los destinatarios o cuando la persona supiera o debiera haber sabido que los informes o datos suministrados eran total o parcialmente falsos o erróneos.

e) *Información Privilegiada.* Información referida a uno o varios participantes del mercado, a sus negocios, a sus valores de oferta pública o al mercado que pudiera afectar su posición jurídica, económica o financiera, cuando no sea de dominio público.

f) *Información Pública*. Información de dominio público que ha sido difundida de manera indiscriminada al público en general o la Superintendencia considere que se encuentre a disposición del público por el nivel de accesibilidad para un inversionista común, aun cuando no haya sido publicada como Hecho Relevante.

g) *Información Reservada.* Información Privilegiada que se encuentra fuera del acceso público, debido a que su difusión puede poner en riesgo la estabilidad o seguridad financiera del mercado de valores o sus participantes.

h) *Información Restringida.* El acceso a esta información debe ser restringido basándose en el concepto de necesidad de saber. Su revelación se busca limitar a la Alta Gerencia y al Consejo de Administración. Requiere la aprobación del responsable de la información y, en caso de terceros, un acuerdo firmado de confidencialidad.

i) *Información Sensitiva (uso interno solamente).* Esta información debe ser revelada a terceros sólo si ha sido firmado un acuerdo de confidencialidad. Su revelación no debe provocar daños a la institución y se provee acceso libre a todos los empleados internos a través de la intranet de la organización.

j) *Instrumentos Financieros.* Son los valores de oferta pública y demás instrumentos ofrecidos y negociados en cualquier mecanismo centralizado de negociación o en el mercado OTC, conformados por activos financieros, instrumentos representativos de pasivos financieros o de patrimonio y los instrumentos derivados, incluyendo todo contrato que tenga como subyacente dichos valores o instrumentos.

k) *Manipulación de Mercado.* Acto realizado por una o varias personas, tanto físicas como jurídicas, a través del cual se interfiera o influya en la libre interacción entre oferta y demanda, haciendo variar artificialmente el volumen o precio de valores de oferta pública, con la finalidad de obtener un beneficio propio o de terceros, así como divulgar Información Engañosa al mercado con este propósito

6. Política de uso y manejo de información reservada, confidencial, privilegiada, sensitiva y restringida

a) Todo documento (físico o digital), carpeta o medio de almacenamiento que contenga información producida y generada en y/o para Primma Valores de carácter reservada, confidencial, privilegiada, sensitiva y/o restringida, debe ser ubicada en un área protegida donde solo sea accesible para las personas debidamente autorizadas.

b) Las informaciones reservadas, confidenciales, privilegiadas, sensitivas o restringidas deben clasificarse como tal. En ese sentido, el líder de área correspondiente a la información de que se trate deberá asegurarse de que la misma contenga la citada mención a través de uso del etiquetado adecuado (bien sea a través de "*watermarks"* o marcas de agua o cualquier otro distintivo donde se evidencie claramente la clasificación del documento).

- La ausencia de etiquetado no significará que la misma podrá ser compartida con terceros. Ante cualquier inquietud deberá consultarse al líder de área correspondiente a la información de que se trate o a la Presidencia Ejecutiva de Primma Valores.

c) Asimismo, debe velarse porque al cierre del día, no quede información reservada, privilegiada, confidencial, restringida o sensitiva sobre los escritorios de los colaboradores. La misma deberá guardarse oportunamente, según aplique, en los archivos de cada colaborador o, en su defecto, deberá cerrarse con llave las oficinas correspondientes. Igualmente, debe asegurarse que el material, la documentación o la información física que no se desee o no vaya a ser utilizada, sea triturada, destruida o desintegrada antes de ser desestimada.

d) Las computadoras portátiles ("laptops") y cualquier otro dispositivo portátil (tales como dispositivos móviles) que contengan información de Primma Valores, deberán tener instalado un software de cifrado ("*encryption*") o cualquier otro mecanismo o herramienta que se considere apropiada para los fines. En caso de que estos no estén siendo utilizados o no estén en la posesión directa del usuario asignado, deberán ser entregados oportunamente al encargado de tecnología.

e) En caso de activación de cifrado de las computadoras, se deberá asegurar que cada una esté configurada con una cuenta de control administrativa, independiente del usuario final, a fin de salvaguardar la información propiedad de Primma Valores.

6.1. Protección de la data

a) Los empleados no deben adquirir, poseer, intercambiar o utilizar equipos o programas que puedan ser utilizados para comprometer la seguridad de los sistemas de información y el eventual acceso a los datos almacenados por el sistema. Las herramientas prohibidas son aquellos con vencimiento a la protección contra copias de programas, que revelan contraseñas secretas, identifican vulnerabilidades del sistema o descifran archivos encriptadas, entre otros. Solamente el personal del proveedor de servicios tecnológicos utilizará este tipo de herramientas.

- En ese sentido, la participación de los empleados, en cualquier forma, en foros de discusión de versiones piratas de programas o sitios de internet relacionados a lo antes mencionado se encuentra prohibido, aún si la participación ocurre durante horas no laborables. Esta política se extiende a cualquier otra facilidad o sistema que intercambie copias ilegales de música, libros u otro tipo de material con derechos de reproducción a través de internet u otros medios de comunicación.

b) En todo caso, los programas, documentación y cualquier otro tipo de data (o información para estos fines) interna de la institución no puede ni debe ser vendida o transferida de ninguna manera a terceros para propósitos distintos a los negocios expresamente autorizados por la gerencia o del curso normal del negocio.

6.2. Privacidad de datos

a) Los mensajes enviados a través de los sistemas de computación y comunicaciones son propiedad de Primma Valores. La gerencia se reservará el derecho de examinar sin previo aviso toda información almacenada en los sistemas de información (correo electrónico

archivado, directorios de archivos personales, archivos en el disco duro, etc.), con el fin de velar por el cumplimiento de las políticas internas, dar soporte a la realización de investigaciones internas, cumplir con requerimientos legales, como orden judicial o citación, y dar asistencia a la administración de los sistemas de información.

b) El acceso a la información personal de clientes potenciales y entidades con la cuales Primma Valores realiza negocios debe ser estrictamente controlado y esta información debe ser utilizada únicamente para fines del negocio.

c) Toda sospecha de pérdida o divulgación de información sensitiva revelada a entidades no autorizadas deberá ser notificada inmediatamente al líder de la información que se trate, al proveedor de servicios tecnológicos y a la Dirección de Riesgos.

d) En ninguna circunstancia se revelará información acerca de debilidades de los sistemas a tercero alguno; los auditores internos no se considerarán como terceros para estos fines. Las excepciones a esta política deberán ser aprobadas por el Oficial de Ciberseguridad y Presidencia Ejecutiva.

6.3. Revelación de datos de terceros

a) La información vinculada a un cliente específico sea corporativo o personal, deberá ser compartida a terceros únicamente si: (1) el cliente ha provisto previamente su consentimiento por escrito o (2) Primma Valores recibe un requerimiento legal por escrito para revelar la información.

b) Todo empleado deberá abstenerse de discutir información privada de clientes en lugares públicos, aún la identidad del cliente sea mantenida bajo confidencialidad.

c) Los empleados deberán abstenerse de descubrir la identidad de clientes famosos cuando estén en su presencia, a excepción de que tales clientes expresen sus nombres abiertamente o por circunstancias de negocios en las que se requieran revelar la identidad del cliente para completar una orden o conducir alguna otra actividad legítima de negocios.

d) Las bitácoras que reflejen las actividades de usuarios de computadoras serán reveladas a terceros siempre que la institución: (1) esté obligado por una orden judicial, ley o reglamento o (2) tenga en su poder la autorización por escrito de los individuos involucrados.

e) Los empleados de Primma Valores no deberán permitir el acceso a personas de organismos de seguridad nacional a información de la entidad, sin la previa autorización de la gerencia Presidencia Ejecutiva; la violación en este sentido podrá ser considerará como una violación a esta Política.

6.4. Manejo de datos

a) La información recopilada sobre clientes o clientes potenciales, tal como números de teléfono y direcciones, deberá ser utilizada solamente para propósitos internos.

b) Los empleados no deberán utilizar el correo electrónico, sistemas de voz de automarcado o cualquier otro sistema de comunicaciones para la distribución de materiales de publicidad no solicitados, a menos que exista una campaña que lo autorice.

c) Los identificadores personales de los clientes, tales como números de identidad del cliente, no deberán estar accesibles públicamente. Esto incluye páginas de internet, sitios de comercio por internet, manuales de productos y publicidad en revistas. Puede realizarse una excepción para llaves públicas de encriptación y certificados digitales, los cuales están intencionados para estar ampliamente disponibles.

d) La información privada o sensitiva en custodia de la entidad no debe ser revelada a terceros a menos que estas entidades firmen antes un acuerdo explícito de cadena de confianza aprobado por el Oficial de Ciberseguridad.

e) Toda información interna de la institución deberá estar protegida de la revelación a terceros, y de ser divulgada a entidades externas, deberá contar con una autorización previa por parte del líder de área correspondiente a la información de que se trate.

f) Los empleados no deberán revelar a personas fuera de Primma Valores, los controles utilizados por los sistemas de información ni la manera en que estos controles son implantados. Las excepciones serán realizadas sólo si se ha obtenido antes la autorización del Oficial de Ciberseguridad y cuando ninguno de los técnicos asignados al Puesto de Bolsa estén capacitados en resolver el problema.

g) Toda información específica sobre debilidades de los sistemas de información deberá ser revelada únicamente con la aprobación del Oficial de Ciberseguridad o Presidencia Ejecutiva.

h) Se deberá revelar al Comité de Riesgos y Ciberseguridad sobre los individuos, organizaciones o sistemas específicos que hayan sido dañados por crímenes y abusos de computación, así como los métodos específicos utilizados para explotar ciertas debilidades de los sistemas. Esta revelación deberá seguir los protocolos definidos para la gestión de incidentes de ciberseguridad Ciberseguridad que deben incluir la creación de un informe que debe incluir las posibles mejoras para solventar las debilidades inidentificadas.

i) Los análisis técnicos y códigos fuentes para programación de virus de computación, gusanos, caballos de Troya y demás rutinas utilizadas para comprometer la seguridad de los sistemas, deberán ser revelados exclusivamente a personas autorizadas por el Oficial de Ciberseguridad.

j) Los requerimientos de clientes que comprometan los mecanismos de seguridad deberán ser procesados previa aprobación la Presidencia Ejecutiva.

k) Toda información de identificación de clientes tal como números de tarjetas de crédito, referencias de crédito y número de cédula, deberá estar disponible sólo para el personal de Primma Valores que necesite de este acceso para poder realizar su labor.

l) El acceso a información sensitiva de datos, sistemas almacenamiento de datos y de inteligencia de negocios estará restringido únicamente por los usuarios y funcionarios designados por la institución.

m) La información sensitiva, que pudiera ser utilizada por adversarios, y que está fácilmente disponible en forma legible a través de canales públicos, debe ser ligeramente modificada para ocultar su verdadera naturaleza de alta integridad.

n) Los sistemas de computación que contengan información con varias clasificaciones de sensibilidad deberán utilizarse controles que reflejen la información más sensitiva en el sistema.

o) La información sensitiva confiada por terceros, incluidos clientes, deberá contar con su consentimiento expreso para su tratamiento y solo podrá utilizarse para los fines previstos en dicha autorización. No deberá revelarse a entidades externas, salvo que el tercero que originó la información haya aprobado expresamente su divulgación y la entidad receptora haya suscrito un acuerdo de confidencialidad debidamente aprobado.

6.5. Eliminación y destrucción de información

a) Toda información sensitiva deberá ser destruida u ocultada de acuerdo con los métodos aprobados por el Oficial de Ciberseguridad antes de que algún medio de almacenamiento magnético sea enviado a un proveedor para intercambio, mantenimiento o eliminación. Los medios de almacenamiento que contengan información secreta, antes de ser utilizados, deberán permanecer en los canales controlados hasta ser neutralizados (desmagnetizados) o llenados con ceros, conforme sea dispuesto en la Política de Seguridad Tecnológica y de la Información.

b) La destrucción de información sensitiva capturada en medios de almacenamiento (como CDs, carretes de cinta o discos floppy) deberá realizarse únicamente mediante métodos aprobados de destrucción, como el uso de trituradoras u otros equipos, aprobados por el Oficial de Ciberseguridad.

c) No deberán utilizarse trituradoras que generan tiras para la destrucción de información sensitiva debido a que las trituradoras que producen tiras de papel permiten que los documentos originales sean fácilmente reconstruidos. Sólo deberán emplearse trituradoras y demás equipo de destrucción de papel aprobados por el Oficial de Ciberseguridad.

d) Sin perjuicio de lo anterior, y siempre que no se trate de documentos o información cuya conservación sea indispensable para la integridad del expediente del cliente, requerido en la auditoría de la trazabilidad, la eliminación y/o destrucción de información sensible podrá ejecutarse tras cumplirse un período de diez (10) años posteriores a la fecha de finalización de la relación comercial, con el propósito de cumplir con lo requerido por el marco jurídico vigente sobre la conservación del rastro auditable inherente al expediente del cliente, ya sea en formato físico o digital. Dicho plazo podrá ser ajustado de conformidad a los cambios normativos aplicables.

6.6. Seguridad de datos

a) Todo empleado involucrado en representar a Primma Valores en un discurso, presentación, informe técnico, libro u otra comunicación a ser entregada al público deberá ser antes aprobada para publicación por la Presidencia Ejecutiva. La divulgación de nuevos productos, resultados de investigaciones, estrategias corporativas, informaciones sobre clientes o métodos de mercadeo, deberá obtener además la aprobación del Oficial de Ciberseguridad y del Director de Legal y Cumplimiento.

b) Los empleados podrán firmar acuerdos de confidencialidad provistos por entidades externas luego de recibir una autorización previa de la Dirección de Legal y Cumplimiento, área

designada para manejar asuntos de propiedad intelectual.

6.7. Prácticas en las áreas de oficina

a) Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida.

b) Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información reservada, confidencial, privilegiada, sensitiva o restringida que esta esté ubicada en gavetas o archivos con llave.

c) Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible. Igualmente, las mismas no podrán ser compartidas con otro usuario ni con otra persona externa a Primma Valores.

d) Las impresoras y trituradoras deben ser localizadas en áreas donde el público general no pueda ver la información reservada, confidencial, privilegiada, sensitiva o restringida.

e) La información confidencial que se desee compartir en papel deberá ser enviada solamente a través de un servicio de mensajería de Primma Valores o correo registrado.

f) La información confidencial podrá ser discutida por teléfonos inalámbricos o celulares siempre y cuando se utilicen equipos de encriptación de voz aprobados por el relacionado comercial de servicios tecnológicos; y en teléfonos con bocinas (speaker) luego de verificar que todas las personas participantes sean empleados o personas autorizadas a escuchar la misma. En todo caso, los empleados deberán utilizar términos cautelosos y abstenerse de mencionar detalles sensitivos más allá de los necesarios para realizar el trabajo cuando la divulgación de información sensitiva por teléfono sea absolutamente requerida.

g) Ante la eventualidad de pérdida o extravío de información reservada, confidencial, privilegiada, sensitiva o restringida, así como en caso de que la misma haya sido divulgada a personas o entidades no autorizadas, o si este acontecimiento incluye pérdida de cualquier equipo, medio electrónico de almacenamiento o componente o herramienta tecnológicos, se debe notificar inmediatamente a la Presidencia Ejecutiva y al Oficial de Ciberseguridad.

h) En toda reunión, conferencia o presentación donde se revele información confidencial, el orador deberá comunicar claramente la sensibilidad de la información y le solicitará a la audiencia no revelar la información a terceros. El apoyo visual, como diapositivas y transparencias, deberá incluir las etiquetas de confidencialidad adecuadas.

i) Los empleados deberán utilizar términos cautelosos y abstenerse de mencionar detalles sensitivos más allá de los necesarios para realizar el trabajo cuando la divulgación de información sensitiva por teléfono sea absolutamente requerida.

j) La información confidencial de nuestra institución podrá ser discutida por teléfonos inalámbricos o celulares siempre y cuando se utilicen equipos de encriptación de voz aprobados por el proveedor de servicios tecnológicos.

k) La información reservada, confidencial, privilegiada, restringida y/o sensitiva no debe ser leída, discutida o de alguna manera expuesta en aviones, restaurantes, transporte público, u otros lugares públicos.

l) Los empleados en posesión de laptops, notebooks, teléfonos inteligentes y demás equipos que contengan información confidencial no deberán dejar esos equipos sin atención en momento alguno y dicha información deberá estar encriptada.

m) Todas las laptops, notebooks y demás computadoras portátiles que contengan información sensitiva de deberán emplear consistentemente tanto encriptación de todos los archivos en el disco duro como protección de inicio.

n) Toda información confidencial podrá ser enviada por un sistema de correo electrónico luego de ser encriptada mediante un método aprobado por el proveedor de servicios tecnológicos.

o) Toda información sensitiva guardada en el Disco Duro o en otros componentes internos o externo de una computadora personal, deberá ser protegida por un control de acceso o por encriptación.

6.8. Otras medidas de seguridad de la información

a) Toda computadora personal, computadora portátil, asistente personal digital (pda), teléfono inteligente, o cualquier otra computadora que se utilice para actividades de negocios y que contenga información sensitiva, deberá ser de uso exclusivo del propietario por lo que su préstamo a otros estará totalmente prohibido.

b) Primma Valores proveerá gabinetes de archivo con cerradura, de modo que estos sean utilizados por todos los empleados para guardar todo material sensitivo bajo llave en estos gabinetes cuando se alejen de sus escritorios, y deberán proveer una copia de respaldo de la(s) llave(s) al Director de la Unidad correspondiente.

c) En ninguna circunstancia los servidores de la página web deberán ser utilizados para el almacenamiento de información crítica de negocios.

d) El proveedor de servicios tecnológicos será el responsable de establecer y mantener un sistema de comunicaciones que permita a los empleados notificar rápidamente al personal adecuado sobre sospechas de problemas con la seguridad de la información. Estos problemas incluyen infestación con virus de computación, intrusiones de hackers, revelación inadecuada de información interna a personas externas, interrupciones del servicio del sistema y otros eventos con serias implicaciones de seguridad de la información. Los usuarios deberán notificar al proveedor de servicios tecnológicos y al Oficial de Ciberseguridad sobre todos los problemas en sistemas de producción. Todos los errores significativos, procesamiento incompleto y procesamiento inapropiado de aplicaciones de producción deberán ser prontamente reportados al proveedor de servicios tecnológicos y al Oficial de Ciberseguridad.

e) La información crítica de negocios y los programas críticos archivados en medios de almacenamiento de computación por un período prolongado deberán ser probados para asegurar que la información es aún recuperable.

f) Los medios utilizados para almacenar datos sensitivos, críticos, o que contienen información

valiosa deberán ser de alta calidad y deberán ser probados cada tres meses, para asegurar que pueden grabar apropiadamente la información en cuestión. Los medios para almacenar datos que no puedan retener información de manera confiable no deberán ser utilizados para respaldo de información.

g) El desecho de los equipos de sistemas de información debe proceder de acuerdo con los procedimientos establecidos por el proveedor de servicios tecnológicos, incluyendo el retiro irreversible de la información y *software*.

h) Los empleados deberán contar con la aprobación escrita de la gerencia antes de destruir o desechar expedientes o fuentes de información potencialmente importantes.

i) La destrucción de expedientes está prohibida a menos que esta sea autorizada y esté documentada en el documento oficial de programación de destrucción y retención de la información. Los empleados no deberán destruir los expedientes de Primma Valores a menos que los mismos aparezcan en una lista de los expedientes autorizados para la destrucción, o porque aparecen en el documento oficial sobre la retención y disposición de expedientes de la firma. A los fines de esta Política, se entenderá como destrucción a cualquier acción que prevenga la recuperación de la información del medio de almacenamiento en el cual se registra (incluyendo encriptación, eliminación, y disposición del hardware necesario para recuperar la información).

j) Cuando se esté en un proceso de investigación de algún incidente de seguridad, y el Director de Legal y Cumplimiento genere una petición de investigación electrónica, las actividades de destrucción de datos electrónicos deberán ser suspendidas inmediatamente, hasta que la Dirección de Legal y Cumplimiento determine si estas actividades no comprometen evidencias para la investigación.

7. Prohibición del uso de información privilegiada

a) Conforme establecido en la normativa vigente, les queda prohibido el uso de información privilegiada en el mercado de valores a todos los colaboradores, accionistas, miembros del Consejo de Administración, y en general, a todas las personas físicas y jurídicas que actúen, se relacionen o que de cualquier forma tomen conocimiento de información privilegiada.

- Esta prohibición durará hasta tanto la información privilegiada sea publicada como Hecho Relevante, conforme a lo dispuesto en la normativa.

8. Comunicación de información privilegiada y reservada a reguladores

a) Primma Valores deberá comunicar a la Superintendencia del Mercado de Valores respecto al conocimiento o sospecha del uso de la información privilegiada de acuerdo con el procedimiento que fuere estipulado en el Reglamento de Información Privilegiada, Hechos Relevantes y Manipulación de Mercado aprobado por el Consejo Nacional del Mercado de Valores (CNMV). Lo anterior, sin detrimento del deber de información del Oficial de Ciberseguridad al Banco Central de la República Dominicana (BCRD), sobre hechos o situaciones que deben ser notificadas o reportadas en el marco del Reglamento de Seguridad Cibernética y de la Información emitida por la Junta Monetaria y su instructivo de aplicación.

b) Esta notificación a la Superintendencia del Mercado de Valores podrá ser realizada por el Director de Legal y Cumplimiento, el Oficial de Cumplimiento o el Oficial de Ciberseguridad. Ante la ausencia temporal o parcial de cualquier de estos funcionarios, deberán observarse las disposiciones y esquemas de suplencias previstos en el Manual Administrativo de Funciones de Primma Valores y el Manual de Cumplimiento para la Prevención del Lavado de Activos, del Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva.

c) La remisión de comunicaciones de Hechos Relevantes a la Superintendencia y a las entidades de autorregulación, según aplique, deberá realizarse a más tardar, el día hábil siguiente de producirse el hecho, la situación o la información. La remisión de la comunicación del Hecho Relevante deberá realizarse por escrito, en la modalidad y a través del canal que disponga la Superintendencia.

d) Según se disponga en el Reglamento correspondiente, Primma Valores deberá revelar cualquier otro evento que pudiera afectar positiva o negativamente su posición jurídica, económica o financiera o el precio de los valores en el mercado.

9. Procedimiento de notificación por incumplimientos de la Política

a) Todo empleado que tenga o reciba información sobre, o constate por cualquier medio, algún incumplimiento relacionado a la presente Política deberá notificar de este hecho al Oficial de Ciberseguridad, debiendo entregar cualquier información o documentación que sea requerido por dicho funcionario.

b) El Oficial de Ciberseguridad procederá a levantar un informe del evento ante la Presidencia Ejecutiva y ante el Comité de Riesgos y Ciberseguridad de Primma Valores. En dicho Comité, se tomará la decisión que se considere oportuna y prudente respecto al evento, sus consecuencias, su impacto y el tratamiento de este (incluyendo del personal relacionado con el evento, si fuere el caso).

- El Comité levantará un acta de la sesión, la cual podrá omitir nombres específicos en caso de considerar que dicha mención afecta el deber de confidencialidad o la salvaguarda de información. Esta acta deberá, sin embargo, estar a disposición de la entidad reguladora cuando así lo solicite de forma expresa.

- Al considerarse de gran relevancia e importancia la aplicación, implementación y cumplimiento de la presente Política, el Oficial de Ciberseguridad queda facultado a convocar al Comité de Riesgos y Ciberseguridad con la mayor celeridad posible, siendo válida la convocatoria realizada por cualquier medio fehaciente (respectando las normas de quórum, validez de decisiones y demás disposiciones relacionadas contenidas en el Manual de Funcionamiento del Comité).

c) El Oficial de Ciberseguridad podrá contar con el apoyo del Oficial de Cumplimiento y/o del Director de Legal y Cumplimiento, quien podrá asistir (de ser así requerido), o quedar representado, ante la sesión en que se conozcan de estos eventos.

d) Una vez adoptada una decisión en el Comité de Riesgos y Ciberseguridad, el Oficial de Ciberseguridad procederá a emitir el informe final, con las recomendaciones y decisiones del citado Comité, para el conocimiento del Consejo de Administración.

10. Sanciones

a) Dado a la naturaleza de la información que se maneja en Primma Valores, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso. La pérdida o el mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad, incumplimientos contractuales, daños a las personas e incumplimiento de regulaciones y leyes aplicables a Primma Valores.

b) En ese sentido, cualquier violación a las disposiciones establecidas en la presente Política será considerada como una infracción grave, teniendo las repercusiones establecidas en el Reglamento Especial de Sanciones Disciplinarias de Primma Valores. No obstante, Primma Valores se reserva la facultad de aplicar la sanción más severa (muy grave).

11. Responsables

a) Corresponderá al Oficial de Ciberseguridad velar por el fiel cumplimiento de las disposiciones establecidas en el presente documento y realizar todas las gestiones que fueren necesarias para formar o capacitar al personal en las mejores prácticas y el adecuado manejo de la información. En dicho tenor, corresponde al Oficial de Ciberseguridad (con el apoyo del equipo que fuere designado) realizar las revisiones periódicas de la adecuada clasificación de la información, los controles y demás procesos relacionados con la presente Política.

b) En todo caso, los empleados, funcionarios y, en general, todo el personal de Primma Valores, deberá velar por el cumplimiento estricto del requerimiento de clasificar información, así como de manejar la información con la criticidad exigida.

12. Disposiciones misceláneas

a) En caso de que existiere contradicción entre lo dispuesto en esta Política y la Política de Seguridad Tecnológica y de la Información, prevalecerá lo dispuesto en la presente Política.

-

Historial de revisión

HISTORIAL DE REVISIÓN			
Fecha de aprobación:	Marzo 2025	**Aprobado por:**	Consejo de Administración
Descripción de cambios			
Versión	**Descripción**		
Enero 2020	Elaboración inicial.		
Octubre 2020	Cambios realizados en función de las observaciones presentadas por la SIMV.		
Abril 2023	Cambios realizados para adecuar de acuerdo con el Reglamento de Información Privilegiada, Hechos Relevantes y Manipulación de Mercado (R-CNMV-2022-10-MV).		

Marzo 2025	Actualización para incluir observaciones realizadas por la Superintendencia del Mercado de Valores mediante comunicación SL-2024-006782 de fecha 5 de diciembre de 2024.

Otto Obritzhauser Presidente	José Miguel Cuervo Vicepresidente
Rebeca García Secretaria	Luis Martí Vocal
J. Julio Cross Vocal	Susana Martínez Nadal Vocal

Javier Guerrero
Vocal