POLÍTICA DE SEGURIDAD Y MANEJO DE LA INFORMACIÓN

APROBADO POR JUNTA DIRECTIVA EL 25 DEL MES DE JULIO DEL AÑO 2023

Bogotá D.C., COLOMBIA

CONTENIDO

TÍTULO I.

PARTE GENERAL

CAPÍTULO I OBJETIVO

Artículo 1 **Objeto de esta Política.**

La Política de Seguridad de manejo de la información de **LOOPAY S.A.S** ("La Compañía") es una herramienta a través de la cual se busca establecer los lineamientos que deban cumplirse sobre el manejo y la seguridad de la información en la organización.

Las disposiciones contenidas en este programa son una clara e inequívoca expresión de la voluntad que tiene la compañía de adoptar como política interna y como principio rector de su gobierno corporativo, la prestación de una colaboración eficaz, eficiente, incondicional e irrestricta a todas las autoridades públicas en su lucha por prevenir y combatir cualquier comportamiento que pueda ser constitutivo de infracciones a la ley penal y disposiciones administrativas, específicamente la corrupción, el soborno, el lavado de activos y todas sus manifestaciones.

Esta política de seguridad en el manejo de la información de la organización es la manifestación del compromiso que ha adquirido la compañía con los más altos estándares de honestidad en sus prácticas comerciales, para asegurar la confiabilidad en el manejo de la información que pueda afectar a la empresa o a aquellos terceros con los que la empresa tiene una relación comercial.

Artículo 2 Alcance.

Esta política aplica para todos los procesos que se realicen en la compañia, en los que se maneje información que pueda comprometer el adecuado desarrollo de los negocios; asimismo, aplica en el manejo de toda aquella información que de acuerdo con la

normatividad colombiana tiene una especial protección y sobre aquella en donde la Junta Directiva, el Representante Legal, y/o Oficial de Cumplimiento haya considerado que debe ser tratada de acuerdo a los protocolos aquí definidos.

Está política debe ser cumplida por las contrapartes, los asociados, empleados, clientes, contratistas y proveedores de productos de la compañia o que tengan algún tipo de relación con la organización, aportando con su participación en la toma de medidas preventivas y correctivas, siendo esto un punto clave para el logro del objetivo de esta política.

Del mismo modo, todas las contrapartes e inversionistas con las que la compañía mantenga una relación contractual tienen la obligación de dar cumplimiento a la presente normatividad.

CAPÍTULO II PRINCIPIOS

Artículo 3 Habeas Data.

El titular de la información tiene la facultad de exigir el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de la información suministrada, así como limitar las posibilidades de divulgación, publicación o cesión de sus datos personales.

En virtud de este principio, toda la información que repose en las bases de datos de la compañía debe ser asegurada bajo los más estrictos protocolos de seguridad, teniendo especial cuidado con aquellos que se encuentren dentro de la categoría de datos sensibles, establecida por la ley 1581 de 2012.

Artículo 4 Principio de legalidad.

Esta política de Seguridad en el Manejo de la Información se ciñe al respeto por los derechos y obligaciones que emanan del ordenamiento jurídico colombiano; en este sentido, la aplicación de esta política se encuentra reglada y debe sujetarse a lo que en ella se desarrolle.

Artículo 5 Principio de Integridad.

Toda la información verbal, física o electrónica debe ser recibida, procesada y transmitida integral y exclusivamente a las personas correspondientes, a través de los medios idóneos y sin modificaciones o alteraciones salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

Las personas obligadas por esta política de seguridad deberán obrar con honestidad, rectitud y probidad en la ejecución de todas las funciones que les sean asignadas, además del ejercicio de las funciones propias de su cargo en la organización.

Artículo 6 Principio de Transparencia.

En el tratamiento de la información debe garantizarse el derecho del titular a obtener en cualquier momento y sin restricción, información acerca de la existencia de los datos que haya proporcionado.

Asimismo, en virtud de este principio, toda la información que sea almacenada en las bases de datos de la compañía no puede ser manipulada o alterada, por lo que en todo momento se debe procurar su indemnidad.

Artículo 7 Principio de eficacia.

En virtud del principio de eficacia, las personas obligadas a implementar esta política de seguridad encaminarán sus actividades laborales al cumplimiento de lo establecido en el

presente documento, de manera que este programa todos los objetivos que se han propuesto con su implementación.

Artículo 8 Principio de eficiencia.

Está política debe buscar un adecuado equilibrio entre el cumplimiento de los objetivos planteados con su implementación y la asignación de recursos al mismo, para asegurar de esta forma la competitividad y el buen desarrollo de las actividades de la empresa.

Artículo 9 Principio de seguridad.

La información sujeta a tratamiento se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar su seguridad, evitar su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

Artículo 10 Principio de reserva en el manejo de la información.

Todas las personas que intervengan en el tratamiento de la información están obligadas a garantizar su reserva, inclusive después de finalizada su relación laboral con la empresa.

CAPÍTULO III DEFINICIONES

Artículo 11 Sistema de información.

Es el conjunto de elementos y recursos informáticos de la compañía orientados a la captación, tratamiento y administración de datos e información, utilizados para cubrir una necesidad o un objetivo propio de la empresa.

Artículo 12 Incidente.

Es un evento o serie de eventos inesperados o no deseados que representan una probabilidad significativa de comprometer la seguridad de las operaciones de la empresa y amenazar la seguridad de la información.

Artículo 13 Riesgo.

Es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en la información.

Artículo 14 Email.

Es un sistema de correspondencia que permite el intercambio de mensajes a través de internet. Asimismo se le denomina al mensaje que es trasmitido por este medio.

Artículo 15 Contraseña.

Es un método de autenticación utilizado para superar una barrera de seguridad.

Artículo 16 Software.

Es un programa o conjunto de programas que atienden a unas pautas y procedimientos, con los cuales se pueden realizar distintas tareas en un sistema informático.

Artículo 17 Programa Ejecutable.

Es un programa compilado que se ha traducido a “código máquina”, para poder ejecutar uno o varios programas.

Artículo 18 Conexiones a Red.

Son los sistemas de enlace con que los dispositivos electrónicos (computadores, dispositivos móviles, etc.) cuentan para conectarse a internet.

Artículo 19 PDA (Personal Digital Assitant).

Actualmente cumplen esta función los teléfonos inteligentes, a través de estos se pueden realizar muchas de las funciones propias de una computadora, con la ventaja de poder contar con él constantemente.

Artículo 20 Código Malicioso.

Es un tipo de código informático dañino, diseñado para crear vulnerabilidades en el sistema que permitan el robo de datos e información, así como el daño de archivos y sistemas informáticos.

Artículo 21 Responsable de la Información.

Individuo o unidad organizacional que tiene la responsabilidad de controlar el uso de la información.

Artículo 22 Seguridad de la Información.

Protección de la información contra el acceso no autorizado, accidental o intencional, su modificación, destrucción o publicación.

Artículo 23 Seguridad Física.

Es la protección de los equipos de procesamiento de la información de daños físicos, destrucción o robo.

Artículo 24 Seguridad Informática.

Es la protección a la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, de las amenazas que puedan proceder de programas dañinos que sean instalados en los equipos o que provengan de internet.

TÍTULO II. NORMAS DE SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN

CAPÍTULO I CUMPLIMIENTO DE LAS NORMAS DE SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN

Artículo 25 **Cumplimiento de las Normas de Seguridad.**

Todo el personal de la compañía, proveedores y clientes que tengan acceso a información restringida o que accedan a la red informática de la organización, deben cumplir las normas de seguridad recogidas en este documento.

Artículo 26 Sanciones.

En caso de incumplimiento, la compañía se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como la ejecución de medidas sancionatorias que se consideren pertinentes, sin perjuicio de la responsabilidad civil y/o penal a que haya lugar.

CAPÍTULO II SEGURIDAD DEL MANEJO DE LA INFORMACIÓN PARA CLIENTES Y PROVEEDORES

Artículo 27 Seguridad de la Información.

La compañía protegerá y garantizará la confidencialidad, integridad, disponibilidad, auditabilidad y privacidad de la información que sea creada, almacenada o utilizada y que guarde relación con todo el proceso de selección, obtención de información, verificación, contratación y finalización de la relación comercial con el cliente o proveedor.

Artículo 28 Uso de la información.

Las áreas que procesan datos personales de clientes, beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la compañía.

Asimismo, se debe asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos y se deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de los mismos.

TÍTULO III. POLÍTICAS DE SEGURIDAD EN EL MANEJO DE LA INFORMACIÓN

CAPÍTULO I POLÍTICA DE INDICENTES DE SEGURIDAD

Artículo 29 Reporte de Incidentes de Seguridad.

Cualquier incidente que represente un riesgo para la seguridad de la información debe ser reportado inmediatamente al Área de Cumplimiento de la Compañía.

Artículo 30 Oficial de Protección en el Manejo de la Información.

La compañía contará con un oficial de protección de datos en el manejo de la información, quien será el responsable de velar permanentemente por el estricto cumplimiento de las normas establecidas en esta política. En desarrollo de esta función, el oficial de protección de datos en la información deberá:

1. Formular observaciones a la Junta Directiva y al representante de la Compañía acerca de la forma como se viene aplicando la ***política de seguridad en el manejo de la información***, así como de las dificultades que existan para su correcta implementación.

2. Evaluar permanentemente el desempeño de la ***política de seguridad en el manejo de la información*** y consignar sus conclusiones en informes anuales que deberán presentarse a la Asamblea de Accionistas.

3. Presentar a la junta directiva y al representante recomendaciones acerca de nuevos mecanismos o instrumentos que puedan adoptarse para mejorar la efectividad de la ***política de seguridad en el manejo de la información***.

5. Supervisar personalmente, o a través de un tercero especialista, las operaciones realizadas por los funcionarios de la Compañía, para identificar nuevos eventos de riesgo de seguridad.

6. Diseñar, programar y coordinar periódicamente planes de capacitación para los administradores y colaboradores de la compañía, relativos a la prevención de riesgos de seguridad en el manejo de la información.

7. Firmar con la Compañía el acuerdo de confidencialidad sobre la información que conoce, maneja y tramita.

Artículo 31 Procedimiento de Reporte de Incidentes de Seguridad.

Para asegurar que los incidentes de seguridad que se presenten con la información que maneja la compañía sean comunicados y atendidos oportunamente, se debe seguir el siguiente procedimiento:

1. Todo funcionario que tenga conocimiento de un incidente de seguridad debe reportarlo al Área de Cumplimiento y Protección de Datos, quien será el oficial de protección de datos en la información, para que este le dé el tratamiento pertinente.

2. El oficial de protección de datos deberá realizar una investigación sobre la alerta o sospecha que exista.

3. Culminada la labor investigativa, el oficial de protección de datos debe realizar un informe sobre los hechos, las actividades realizadas y los resultados obtenidos de la investigación. Dicho informe deberá además indicar si el incidente es producto de una amenaza externa o se debe a la acción o negligencia de uno o varios de los funcionarios de la compañía.

4. Si el oficial de protección de datos encuentra que la sospecha era cierta, presentará el caso ante el Área de Cumplimiento y Junta Directiva de la compañía, en donde pondrá en conocimiento los hechos, las alertas detectadas, las actuaciones e investigaciones adelantadas y la conclusión sobre las mismas.

5. Una vez se ha puesto en conocimiento del Oficial de Cumplimiento o la Junta Directiva los hechos objeto de investigación, se citará al funcionario o funcionarios involucrados para que manifiesten su versión de los hechos y aporten las pruebas necesarias que puedan servir para su defensa.

6. Frente al informe del oficial de protección de datos y las manifestaciones que en su defensa realice el funcionario o la Junta Directiva de la compañía dispondrá alguna de las siguientes decisiones:

Archivo de la investigación: La Junta Directiva dispondrá el archivo de la investigación cuando no se esté frente a la violación de alguna de las disposiciones de esta política.

Aplicación de una sanción disciplinaria: En caso de encontrar plenamente probado la violación a alguna de las disposiciones de esta política, la Junta Directiva procederá a imponer la sanción que considere pertinente teniendo en cuenta la gravedad de la violación.

Aviso a las autoridades competentes: En caso de que los hechos investigados revistan las características de un delito tipificado en la ley, la Junta Directiva de la compañía, además de la respectiva sanción disciplinaria interna, denunciara los hechos ante las autoridades públicas para iniciar las correspondientes investigaciones penales.

7. Si el incidente proviene de una amenaza externa, el oficial de protección de datos adelantará todas las acciones necesarias y pertinentes para contrarrestar la amenaza recibida. Igualmente presentará un informe al Oficial de Cumplimiento o a la Junta Directiva donde informe las investigaciones y acciones realizadas.

CAPÍTULO II POLÍTICA DE USO DE INTERNET

Artículo 32 Acceso a internet.

La compañía permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte del personal, evitando errores, perdidas, modificaciones no autorizadas o uso inadecuado de la información. El acceso a internet debe ser solicitado al personal encargado de tecnología y su uso está limitado para actividades de trabajo.

Artículo 33 Prohibiciones al Uso de Internet.

Está prohibido navegar en sitios de Internet que no estén relacionados con el desarrollo de las actividades laborales; igualmente, no se deben descargar software, música, videos o cualquier otro tipo de documento de Internet que no esté relacionado con las actividades de trabajo.

Está prohibido publicar en Internet información de la empresa sin contar con una autorización. Quien incumpla estas disposiciones se someterá a las responsabilidades disciplinarias internas, sin perjuicio de la responsabilidad civil y/ penal a que haya lugar.

CAPÍTULO III POLÍTICA DE USO DE EMAIL

Artículo 34 Acceso al Email.

La compañía otorgará bajo su criterio el acceso a los servicios de correo electrónico corporativo, para el desarrollo de las actividades empresariales. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos.

Cada funcionario de la compañía al que se le haya otorgado el acceso al correo, tendrá asignado un usuario y una clave personal.

El ingreso al correo electrónico de la compañía debe realizarse a través de los equipos informáticos que la organización haya dispuesto para ello y su acceso desde un terminal informático diferente debe ser autorizado.

Artículo 35 Uso del Email.

El correo electrónico corporativo es una herramienta para el intercambio de información entre personas y se debe utilizar únicamente para fines laborales; se debe evitar enviar cadenas de email, archivos de música, videos y programas ejecutables, salvo que estos estén relacionados con las actividades laborales de la compañía.

El contenido de los mensajes enviados a través del correo corporativo debe ser claro, conciso y respetuoso. No se deben utilizar expresiones difamatorias, groseras, racistas, ofensivas u obscenas en contra de individuos, proveedores, clientes o entidades públicas o estatales.

Artículo 36 Uso indebido del Email.

Se cataloga como uso indebido del Email intentar acceder a otras cuentas de correo electrónico corporativo sin tener autorización, enviar correos electrónicos con fines diferentes a los laborales, difundir "cadenas" o propaganda no relacionada con la organización, utilizar el usuario otorgado para crear cuentas en páginas de internet (Facebook, MercadoLibre, etc.), copiar o reenviar mensajes sin tener la autorización del remitente original, descargar archivos o software sin tener en cuenta medidas de precaución que eviten el acceso de virus informáticos, eliminar arbitrariamente la información que reposa en el email, dejar a la vista de terceras personas el usuario y contraseña del correo e intentar o modificar los parámetros de seguridad ya establecidos en el sistema de correo electrónico de la compañía.

CAPÍTULO IV POLÍTICA DE USO DE CONTRASEÑAS

Artículo 37 Usuario y la Contraseña Asignada.

Cada empleado será responsable de sus credenciales de acceso y todo lo que de él se derive, por lo que es imprescindible que esta información sea personal e intransferible.

Artículo 38 Responsabilidades.

Cuando se reciban las credenciales de acceso a los sistemas de la compañía, se considera que se acepta formalmente las normas de seguridad de la información dadas en este documento, y que asume las siguientes responsabilidades:

1. Se deben utilizar contraseñas seguras, que incluyan al menos un número y una letra.

2. Bajo ninguna circunstancia se debe compartir la contraseña a otras personas, ni mantenerlas por escrito, a la vista, ni al alcance de terceros.

3. No se debe utilizar la misma contraseña en todos los sistemas o servicios.

4. Toda persona será responsable de las acciones registradas en los sistemas informáticos de compañía ejecutadas con su usuario.

5. El personal debe asegurarse que los equipos queden protegidos cuando estén desatendidos, es decir, deben bloquearse al ausentarse del puesto de trabajo.

Artículo 39 Prohibiciones en el Uso de Contraseñas.

Está prohibido descifrar claves o intentar obtener otros derechos o accesos distintos a aquellos que hayan sido asignados por la empresa. La persona que incumpla esta disposición se sujetara a la responsabilidad disciplinaria interna, sin perjuicio de la responsabilidad civil y/o penal a que haya lugar.

CAPÍTULO V POLÍTICA DE USO DE INSTALACIÓN DE SOFTWARE

Artículo 40 Instalación de Software.

Está prohibido instalar un software no autorizado o un software gratuito no relacionado con actividades laborales, en los equipos de la empresa. Asimismo, no se podrá descargar, ni cargar programas informáticos no autorizados a través de internet.

Artículo 41 Uso de Software.

El software que se utilice durante la ejecución de las actividades laborales debe ser el autorizado por la compañía; el uso inadecuado de los programas informáticos deberá ser informado al personal encargado.

Está prohibida la realización, adquisición o utilización de copias no autorizadas de los programas informáticos de la compañía. El colaborador que incumpla estas disposiciones se someterá a las responsabilidades disciplinarias internas, sin perjuicio de la responsabilidad civil y/o penal a que haya lugar.

Artículo 42 Procedimiento de Reporte Inadecuado de Programas Informáticos.

El oficial de protección de datos hará revisiones periódicas para verificar el manejo y estado de los sistemas informáticos de la compañía. En caso de encontrar anomalías en su uso, hará las investigaciones pertinentes.

Asimismo, todo funcionario que tenga conocimiento del mal manejo de los programas informáticos que le esté dando algún miembro de la compañía, deberá reportarlo al oficial de protección de datos en el manejo de la información, para que este le dé el tratamiento que se describe a continuación:

1. El oficial de protección de datos deberá realizar una investigación sobre la alerta o sospecha que exista.

2. Culminada la labor investigativa, el oficial de protección de datos debe realizar un informe de las actividades realizadas y de los resultados obtenidos de la investigación.

3. Si el oficial de protección de datos encuentra que algún funcionario está utilizando indebidamente los sistemas informáticos de la compañía, le informará a la Junta directiva para que estos tomen alguna de las medidas establecidas en el artículo 31 de esta política.

CAPÍTULO VI POLÍTICA DE USO DE REDES INALÁMBRICAS

Artículo 43 Uso de Redes Inalámbricas.

El uso de cualquier tecnología inalámbrica (redes Wireless, bluetooth u otras) en la empresa debe ser autorizado por el personal encargado. La compañía se reserva el derecho de bloquear, suspender, alterar, o monitorear los servicios soportados en su red informática, cuando se detecten actividades que contravengan los principios y normas expresados en el presente documento.

Artículo 44 Prohibiciones al Uso de Redes Inalámbricas.

Está prohibido modificar las conexiones de red en las computadoras sin autorización del personal encargado.

No se debe conectar a redes inalámbricas que no hagan parte de la red de la organización; si se requiere conectar un equipo de la empresa a redes inalámbricas que no forman parte de la misma, se debe comunicar al personal encargado.

CAPÍTULO VII POLÍTICA DE USO Y CUIDADO DE EQUIPOS INFORMÁTICOS

Artículo 45 Uso y Cuidado de los Equipos Informáticos.

Los equipos informáticos (sistemas, computadoras, impresoras, scanner y otros dispositivos) asignados al personal de la compañía, deben ser utilizados para realizar actividades laborales. El personal debe ser responsable y garantizar un uso seguro del equipo que le ha sido asignado.

Todos los funcionarios que reciban un equipo tecnológico para el desarrollo de sus funciones, deberán firmar un acta de entrega y responsabilidad, en donde manifestarán asumir la responsabilidades derivadas de un inadecuado uso o pérdida del equipo que sea imputable al colaborador, igualmente, a la entrega del equipo corporativo, se realizará entrega de la política de seguridad en el manejo de la información y manifiestan su compromiso para cumplir la misma.

Artículo 46 Transparencia en la información.

Los colaboradores que reciban equipos tecnológicos para el desarrollo de sus funciones, deberán garantizar el estado, la fidelidad y veracidad de la información que en ellos se produzca, guarde y custodie, so pena de responsabilidad disciplinaria al interior de la compañía, sin perjuicio de la responsabilidad civil y/o penal a que haya lugar.

Artículo 47 Protección de la Información.

La información debe ser protegida contra el acceso no autorizado, modificación, divulgación, pérdida o destrucción, sin importar la fuente en donde esté almacenada (computadores, librerías, portátiles, medios extraíbles, contratos, documentos, etc.).

Para una efectiva protección de la información, se debe tener un especial cuidado en el manejo de los equipos informáticos, de manera que tanto en la recepción, como en el manejo y almacenamiento de la información esta sea custodiada.

Artículo 48 Información clasificada.

Es aquella información que al ser divulgada puede llegar a causar daño a algunos derechos individuales de las personas naturales o jurídicas. Su tratamiento debe estar encaminado a proteger la intimidad y privacidad del titular de la información. Se debe controlar su circulación la cual solo está autorizada para uso interno.

Artículo 49 Información reservada.

Es aquella información que con su divulgación puede causar daños a bienes o intereses públicos y su reserva está justificada por la ley.

Se debe garantizar su confidencialidad, y su distribución debe hacerse únicamente previa autorización. Asimismo, el responsable de la información debe asegurarse de que esta sea almacenada bajo llave o cifrada cuando no esté en uso.

Artículo 50 Prohibiciones al uso de equipos informáticos.

Está prohibido modificar la configuración de los equipos informáticos sin previa autorización y manipular comidas o bebidas cerca de los mismos. Quien incumpla esta disposición se someterá a las responsabilidades disciplinarias internas, sin perjuicio de la responsabilidad civil o legal a que haya lugar.

CAPÍTULO VIII POLÍTICA DE BACKUP Y RESPALDOS

Artículo 51 Copia de Seguridad.

Para asegurar que toda la información esencial y el software se pueda recuperar después de una falla, se debe realizar con regularidad el respaldo de los datos de la empresa en las carpetas, servidores y dispositivos autorizados para este fin.

Artículo 52 Prohibiciones al Respaldo de información.

Está prohibido respaldar datos personales (fotos, música, videos, imágenes y otros) en los servidores de respaldo de la empresa, así como respaldar los datos de la empresa en dispositivos externos sin autorización.

Si por la ejecución de sus labores requiere respaldar los datos de la empresa en dispositivos externos debe solicitar su autorización.

Artículo 53 Eliminación de información.

La información que vaya a ser eliminada o que cumpla el periodo de retención, debe surtir un proceso de borrado seguro y posteriormente será eliminada o destruida de forma adecuada.

CAPÍTULO IX **POLÍTICAS DE MEDIOS REMOVIBLES**

Artículo 54 Uso de Medios Removibles

Está prohibido copiar información corporativa de cualquier naturaleza en medios removibles, tales como USB, CD, Diskette, celulares o cualquier dispositivo móvil, sin previa autorización.

Artículo 55 Cuidado de Medios Removibles.

Si se está autorizado a utilizar medios removibles, estos no se pueden dejar expuestos a la utilización de terceros, y se debe asegurar su cuidado cuando no se estén usando.

CAPÍTULO X POLÍTICA DE USO DE LA NUBE

Artículo 56 Acceso

El acceso a la nube es otorgado personalmente a cada colaborador que cuente con una cuenta de correo corporativa. El único con acceso además de la administración IT es el funcionario a quien le fue asignado. En razón de ser un acceso con la cuenta de correo se recomienda al colaborador utilizar todos los controles de seguridad ofrecidos por el proveedor de la nube. Es muy importante que el usuario mantenga control del ingreso y egreso de la plataforma nube debido a los riesgos que representa dejar la sesión abierta.

El producto de la nube se encuentra enlazado con todos los productos ofrecidos en el paquete del proveedor de correo electrónico, por lo tanto, todos los productos son accesibles desde la misma sesión.

Al ser una plataforma de almacenamiento de información es importante acatar el uso de las buenas prácticas de manejo y acceso, para no poner en riesgo la información del usuario y por ende de la organización

Artículo 57 Objetivo

El mayor objetivo del producto del almacenamiento en nube es que cada uno de los usuarios utilice este producto para almacenar toda la información del proceso a cargo, de manera organizada y estructurada. Puede dar la oportunidad de un trabajo colaborativo entre usuarios. Respaldo y control seguro de la información. Adicionalmente aportar en la protección de la información a posibles códigos maliciosos que puedan capturar o encriptar la misma. De esta manera la información no reposará en los dispositivos asignados al colaborador si no que siempre permanecerá en constante respaldo y actualización en servidores en la nube. Permitir la constante flexibilidad de acceso y manejo de la información desde cualquier estación de cómputo.

Artículo 58 Uso

El uso correcto de la nube corresponde a tener instalada una memoria de almacenamiento virtual en el dispositivo asignado, gestionando y alojando toda la información en está nube. Cumplir con el almacenamiento de la nube garantiza por defecto la copia de seguridad de la información con control de versiones y administración del área de tecnología.

La información que repose en el espacio en la nube de cada usuario debe corresponder única y exclusivamente a contenido de gestión, operación y administración del proceso

asignado al colaborador. El control de cambios y compartición de documentación con otros usuarios es responsabilidad y administración del colaborador. Se debe conservar y validar la configuración de seguridad de la nube para respaldo e integralidad de la información alojada en la nube.

El control de espacio o almacenamiento corresponderá también a la buena administración y gestión del colaborador que tenga una cuenta corporativa asignada.

Artículo 59 Uso Indebido

La nube no debe ser sincronizada en un dispositivo externo a la organización. Las credenciales de acceso deben ser únicas e intransferibles por cada uno de los colaboradores. No se debe almacenar contenidos de alta capacidad o de otra gestión ajena al proceso de cada colaborador. No se debe dar permisos públicos para acceso a la información desde otra entidad o público ajeno a la organización.

Artículo 60 **Alcance**

El alcance del producto de nube es para todos los colaboradores que cuenten con una cuenta de correo corporativa en la organización. El espacio del almacenamiento por defecto es de 1TB por usuario.

TÍTULO IV. SEGUIMIENTO Y CONTROL

CAPÍTULO ÚNICO

Artículo 61 Seguimiento y Control.

La compañía, a través del oficial de protección de datos, comprobará ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de los recursos informáticos de la compañía y la implementación de esta política de seguridad.

Artículo 62 Manejo incorrecto de la Información.

En caso de el oficial de protección de datos en el manejo de la información detecte que alguien utiliza incorrectamente la información, software o cualquier otro recurso informático de la empresa, se le comunicará tal circunstancia y se le facilitará en su caso la formación necesaria para el correcto uso de los recursos.

Artículo 63 Mala Fe en el Manejo de la Información.

En caso de apreciarse mala fe en la incorrecta utilización de la información, software o cualquier otro recurso informático de la empresa, la compañía ejercerá las acciones que legalmente le amparen para la protección de sus derechos y los de sus clientes.

TÍTULO V. DISPOSICIÓN FINAL.

CAPÍTULO ÚNICO

Artículo 64 Vigencia.

Esta política rige a partir de su promulgación y deroga las anteriores emitidas sobre el mismo tema.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DEL CAMBIO	ELABORACIÓN / MODIFICACIÓN	REVISIÓN Y APROBACIÓN
01	28-08-2024	• Versión Inicial	**Omar Alejandro Vera López (Oficial de Cumplimiento)**	**Omar Alejandro Vera López (Oficial de Cumplimiento)**