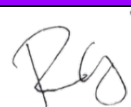
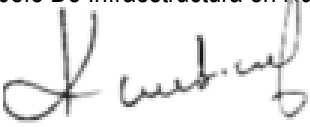
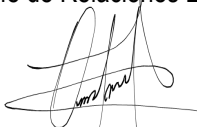
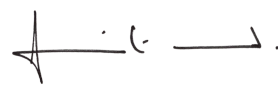


	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
		VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



06/08/2025

Elaboró	Revisó	Aprobó
 Linda P. Salgado Montes Abogada	 Rebeca González de León Directora de Asuntos Legales	
 Helbert López Jefe De Infraestructura en Nube	 Tatiana Martínez Jefe de Relaciones Laborales	
 Katherine Acendra Macareno Coordinadora de Gestión Documental	 Oscar Moreno Quiroga Director de Tecnología e Información	 Andrés Escobar Uribe Gerente Ejecutivo

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

CONTROL DE CAMBIOS

Versión	Causa del Cambio	Área y Responsable del Cambio	Fecha del Cambio
1.0.	Documento Nuevo	Dirección de asuntos legales – T.I	03/04/2024
2.0.	Cambio de tipo de documento, de dependencia, cambio de código, ajustes y adición de contenido de acuerdo a lo solicitado para certificación PCI.	Dirección Corporativa de TI	16/01/2025
3.0	Inclusión de contenido en el numeral 7.3.4. sobre las restricciones de los usuarios genéricos o compartidos. Así mismo se adiciona sobre la implementación de medidas de seguridad adecuadas en el numeral 7.3.7 y en el numeral 7.3.15.1. se adiciona información sobre el contenido del correo electrónico. Creación del numeral 8.6.6. sobre el tratamiento de datos de los titulares de las tarjetas. En el ítem 9 se adiciona la información relacionada al “incumplimiento”. En el ítem 10 se ajusta el deber de confidencialidad y se agrega un párrafo; en el mismo ítem se adiciona información sobre las “Obligaciones relacionadas con las medidas de seguridad implantadas”.	Dirección Corporativa de TI	06/08/2025

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	5
2. OBJETIVO.....	5
2.1. Objetivos Específicos:.....	5
3. ALCANCE.....	6
4. COMPROMISO DE LA ALTA DIRECCIÓN.....	6
5. REFERENCIAS NORMATIVAS.....	6
6. GLOSARIO.....	8
7. CONTENIDO.....	10
7.1. Conformación de Comité.....	10
7.1.1. Miembros del Comité de Seguridad de la Información.....	11
7.2. Matriz de Responsabilidades.....	11
7.2.1. Concientización y Capacitación en Seguridad de la Información.....	12
7.3. Lineamientos.....	13
7.3.1. Gestión de Activos.....	13
7.3.2. Uso de Dispositivos Móviles.....	14
7.3.3. Clasificación De La Información.....	15
7.3.4. Control de Accesos de Usuarios.....	15
7.3.5. Segregación de Ambientes.....	16
7.3.6. Creación de contraseñas.....	17
7.3.7. Responsabilidad del Usuario.....	18
7.3.8. Control de acceso físico a centros de datos.....	19
7.3.9. Uso De Los Controles Criptográficos.....	19
7.3.10. Pantalla Limpia y Bloqueo de Sesión Inactiva.....	20
7.3.11. Gestión de Cambios.....	20
7.3.12. Protección Contra Código Malicioso.....	21
7.3.13. Intercambio de Información.....	21
7.3.14. Uso de Mensajería Instantánea.....	22
7.3.15. Uso de Correo Electrónico.....	22
8. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.....	27
8.1. Seguridad Informática en las Relaciones con los Proveedores.....	27
8.2. Prestación de Servicio por Proveedores.....	28
8.3. Gestión de Continuidad de TI.....	28

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

8.4. Medidas de seguridad comunes.....	29
8.4.1. Control de acceso.....	29
8.4.2. Bases de datos temporales, copias y reproducciones.....	29
8.5. Medidas de seguridad para bases de datos no automatizadas.....	30
8.5.1. Archivo de documentos.....	30
8.5.2. Acceso a los documentos.....	31
8.6. Medidas de seguridad para bases de datos automatizadas.....	31
8.6.1. Identificación y autenticación.....	31
8.6.2. Control de acceso físico.....	32
8.6.3. Copias de respaldo y recuperación de datos.....	32
8.6.4. Registro de acceso.....	33
8.6.5. Redes de Comunicaciones.....	33
8.6.6. Tratamiento de Datos de Titulares de Tarjetas.....	33
9. CUMPLIMIENTO Y ACTUALIZACIÓN.....	34
10. FUNCIONES Y OBLIGACIONES DEL PERSONAL.....	34
11. DISPOSICIÓN FINAL.....	38

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

1. INTRODUCCIÓN

La siguiente política contiene el conjunto de medidas destinadas a preservar los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. Además, tiene como propósito establecer los requisitos para proteger los activos de información, dispositivos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de la compañía Plan B Investments S.A.S. ya que en la actualidad, las tecnologías de la información se enfrentan a un creciente número de amenazas, lo cual requiere de un esfuerzo constante por adaptarse y gestionar los riesgos introducidos por estas.

2. OBJETIVO

Establecer los lineamientos de seguridad informática, garantizando todas las acciones tendientes a mitigar los riesgos asociados a los procesos tecnológicos de la empresa, creando una cultura organizacional de los colaboradores de PLAN B INVESTMENTS en torno a la seguridad de la información basado en las mejores prácticas, haciéndolas extensivas a todos los terceros con los cuales se tenga un relacionamiento comercial o contractual.

2.1. Objetivos Específicos:

- Identificar riesgos de manera oportuna que permitan minimizar el impacto frente a posibles incidentes o problemas que comprometan la seguridad de la información de la compañía PLAN B INVESTMENTS S.A.S.
- Conocer los mecanismos de reporte de incidentes y finalmente ser replicadores de cultura al interior de La compañía.
- Mantener los sistemas de información y recursos tecnológicos adecuados, que fortalezcan la seguridad de la información.
- Establecer los fundamentos para el desarrollo y la implementación de un modelo de seguridad de la información, que defina la conducta a seguir en relación con el acceso, uso, manejo y administración de los recursos de información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

3. ALCANCE

Este documento aplica para todas las áreas administrativas y operativas de PLAN B INVESTMENTS S.A.S.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección de PLAN B INVESTMENTS S.A.S en cabeza de su Gerente Ejecutivo, reconoce la importancia de identificar y proteger los activos de información, así como la plataforma tecnológica que soporta los procesos de la compañía, razón por la cual resalta su compromiso con la Seguridad de la Información, apoyando el desarrollo, implementación, formalización, mantenimiento y mejora continua, que permita la mitigación de los riesgos que lleguen a afectar los datos, sistemas y aplicaciones esenciales para la operación.

En ese sentido, la Gerencia Ejecutiva garantiza y respalda la ejecución de las actividades que a continuación se indican:

- Proporcionar los recursos adecuados para el mantenimiento de la Seguridad de la Información.
- Promover la cultura de Seguridad de la Información.
- Apoyar la divulgación de las políticas y demás lineamientos de Seguridad de la Información.

5. REFERENCIAS NORMATIVAS

- Constitución política colombiana , Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 527, del 18 de agosto de 1999. Por medio de la cual se define y reglamenta el acceso y el uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y establecen las entidades de certificación y se dictan otras disposiciones.
- ISO 27001 2013: Es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

disponibilidad de la información.

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 1377 de 2013: Reglamenta la Ley 1581 de 2012, estableciendo procedimientos para la implementación de políticas de tratamiento de datos personales.
- Ley 1273 de 2009 - Delitos Informáticos: Crea la protección de la información como bien jurídico y define delitos relacionados con ataques cibernéticos, acceso no autorizado y sabotaje informático.
- ISO/IEC 27002:2022: Ofrece un marco de referencia para la implementación de controles de seguridad de la información.
- Circular Externa 042 de 2020 (Superintendencia Financiera): Requiere a las entidades financieras fortalecer sus sistemas de seguridad cibernética.
- Marco de referencia de ciberseguridad para infraestructura crítica (ColCERT): Proporciona guías para proteger activos críticos contra ataques cibernéticos.
- Normativa de Comercio Electrónico (Decreto 2364 de 2012): Establece disposiciones sobre la validez jurídica de la información electrónica y seguridad en transacciones.
- Marco Nacional de Ciberseguridad (Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC): Un documento estratégico que guía la gestión de riesgos cibernéticos.
- NIST Cybersecurity Framework (NIST CSF) : marco de trabajo diseñado para identificar, evaluar y gestionar riesgos de ciberseguridad.
- Ley 256 de 1996 - Competencia Desleal: Incluye elementos relacionados con el manejo de la información empresarial y confidencialidad en el marco de la competencia.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

6. GLOSARIO

TÉRMINO	DESCRIPCIÓN
Activo	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Correo electrónico	Servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.
Claves, contraseñas o password	Forma de autenticación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.
Datos personales sensibles	Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos
Dato privado	Dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
Dato público	Dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas
Datos semiprivado	Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

	puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
Disponibilidad	Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
Gestión de riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos.
Habeas data	Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
Integridad	Propiedad de la información que busca preservar su exactitud y completitud.
Infraestructura tecnológica	Elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Internet	Corresponde a una interconexión de diferentes redes de computadoras, permitiendo la creación de una red única de alcance mundial.
Intranet	Red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

Responsable del tratamiento	Persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.
Seguridad de la información	Conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización, asegurando su confidencialidad, integridad y disponibilidad.
Titular de la información	Persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
Vulnerabilidad	Debilidad de un activo o control que pueda ser explotado por una o más amenazas

7. CONTENIDO

7.1. Conformación de Comité.

Se crea un comité denominado Comité de Seguridad de la Información  ACTA DE CONFORMACIÓN DE COMITÉ SEGURIDAD DE LA INFORMACIÓN.pdf , que se encargará de:

- Identificar e implementar mecanismos para lograr el cumplimiento de la normatividad y estándares en seguridad de la información.
- Presentar los lineamientos de seguridad que se aplican a los sistemas de información, redes de datos, así como, a todas las instalaciones en las que procesa, almacena o transmite información de los colaboradores, terceros y entes que tengan acceso a la información de PLAN B INVESTMENTS S.A.S garantizando su seguridad a través de los principios de confidencialidad, integridad y disponibilidad.
- Fortalecer la cultura y apropiación organizacional en materia de seguridad de la información para todos los colaboradores, terceros y entes que tengan acceso a la información de PLAN B INVESTMENTS S.A.S.
- Realizar una adecuada gestión de los riesgos e incidentes de seguridad de la información.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Proteger los activos de la información de la compañía mediante la implementación de políticas, procedimientos y controles.

7.1.1. Miembros del Comité de Seguridad de la Información.

- Abogada
- Arquitecto de Software
- Coordinadora de Gestión Documental
- Coordinador de Servicios de TI
- Jefe de Infraestructura en nube

7.2. Matriz de Responsabilidades.

ROL	ACTIVIDAD
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Aprobar los roles y responsabilidades del comité de seguridad de la información.
	Aprobar la Política General de Seguridad de la Información.
	Revisar mínimo una vez al año, o antes si surge la necesidad; la Política de Seguridad de la Información, con el fin de realizar las modificaciones y ajustes a que haya lugar.
	Revisar las modificaciones o ajustes de la Política de Seguridad de la Información y presentarlas para su aprobación.
	Facilitar la divulgación de la documentación relacionada a las políticas y procedimientos de Seguridad de la información.
	Velar por el cumplimiento de las políticas y procedimientos de seguridad de la información.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

	Analizar los incidentes de seguridad reportados y/o detectados y presentarlas al comité de seguridad informática los que considere críticos para la seguridad de los recursos informáticos.
	Participar activamente en la revisión y toma de decisiones relacionadas con los incidentes de seguridad que le sean escalados.
	Iniciar campañas de concientización y conocimiento de las políticas de seguridad de la información.
VISITANTES	- Cumplir las políticas de seguridad de la información institucionales cuando se les autorice acceso a los activos de información institucionales. - Utilizar únicamente la red local de invitados, la cual restringe el acceso solo a internet. - Solicitar al responsable del respectivo activo información la autorización de acceso a los mismos. - No interrumpir o deshabilitar los controles de seguridad dispuestos por la organización para la protección de sus activos de información.

7.2.1. Concientización y Capacitación en Seguridad de la Información.

- El comité de Seguridad de la Información, debe realizar campañas de concientización sobre sus responsabilidades en el buen uso de los recursos informáticos. Estas campañas deben ser realizadas semestralmente a través del canal de comunicaciones de la empresa.
- El comité de Seguridad de la Información, debe asegurar que la Política de Seguridad de la información se encuentre actualizada, divulgada, publicada y disponible en la intranet de la empresa.
- Todo colaborador debe recibir inducción y capacitación sobre la política de seguridad de la información, al momento de ser contratados y posteriormente, una vez cada año.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

7.3. Lineamientos.

7.3.1. Gestión de Activos.

- El área de Seguridad Informática debe identificar los activos de información relevantes para los procesos de negocio de la compañía y documentar su criticidad. Esta información debe plasmarse en un inventario y mantenerla actualizada.
- Todos los colaboradores deben usar de manera cuidadosa los recursos informáticos a los que cuenta tiene o le fueron asignados, promoviendo el uso responsable de los mismos.
- Cada colaborador es responsable de la información que usa y debe velar por la seguridad de la misma e informar cualquier violación de la que tenga conocimiento. Está prohibido el uso de cualquier recurso informático de la compañía para propósitos personales, o que violen cualquier ley local o global, guardar o transportar material ilegal, pornográfico, que haga crítica del crimen o violencia, ofensivo, lesivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general y adquisición de material sobre creaciones que violen la ley de propiedad intelectual.
- Está prohibido a todo el personal de la compañía la copia de cualquier software licenciado o de propiedad de la compañía. Las copias sólo podrán ser realizadas por el área de tecnología.
- Plan B Investments S.A.S prohíbe la instalación y el uso de programas, aplicativos, código de software, scripts, java-scripts, macros y cualquier tipo rutina informática que no esté licenciada y autorizada por la Dirección de Tecnología.
- Cualquier software no licenciado encontrado en los equipos de cómputo, será responsabilidad única y exclusiva del colaborador que tiene asignado el equipo, por lo que se considerará una falta grave al reglamento interno de trabajo esta conducta.
- Está prohibida la instalación de hardware y/o software por parte de colaboradores y usuarios externos vinculados a Plan B. Estas actividades sólo serán realizadas por el personal autorizado en el área de TI.
- Está prohibido alterar cualquier recurso informático así como cualquier mantenimiento que se practique a los equipos de cómputo debe ser autorizado por la Dirección de Tecnología.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Plan B Investments S.A.S. expresamente prohíbe el uso de los equipos de cómputo, periféricos (activos de la compañía) y/o de las aplicaciones de software (licenciadas para la compañía) para actividades diferentes a las relacionadas con las labores propias del negocio. En caso contrario debe ser autorizado por el Gerente o Director del área y por el Director de TI.
- Todos los equipos de cómputo y periféricos de la compañía que no sean portátiles o móviles deben ser utilizados dentro de las instalaciones de la compañía, excepto bajo expresa autorización de gerente, director, jefe de área o la dirección de tecnología.
- Está prohibido instalar software como “freeware”, “try-buy”. Si se requiere la instalación debe ser solicitado por Gerente, Dirección o Jefe de Área y autorizado por la Dirección de Tecnología.
- No está permitido la conexión a redes públicas que no sean debidamente autorizadas por la compañía y en su defecto por el Jefe directo del área.

7.3.2. Uso de Dispositivos Móviles.

- El uso de los dispositivos móviles fuera de las instalaciones de la compañía es responsabilidad del colaborador que tiene asignado el equipo. Todo dispositivo móvil suministrado por Plan B Investments S.A.S, debe estar protegido con contraseña para el encendido y debe tener contraseña de bloqueo después de máximo 5 minutos de inactividad.
- Los colaboradores no deben cambiar la configuración de seguridad de los dispositivos suministrados por Plan B Investments S.A.S y que estén bajo su responsabilidad.
- Los colaboradores no deben instalar ningún software en estos dispositivos, solo el área de TI está autorizada para realizar esta labor. Se prohíbe el uso de celulares, pc, portátiles o cualquier dispositivo móvil con cámara fotográfica en los puntos de pago; excepto las PDA gestionadas por TI cuando la estación se encuentre en uso.
- Se prohíbe la transmisión de datos personales por medio de tecnologías de colaboradores y colaboradores externos vinculados a Plan B; tales como correo electrónico, redes sociales, SMS sin la debida seguridad, autorización y justificación.
- Se prohíbe el uso de la red de internet interna para realizar actividades que no sean acorde a las estipuladas en las funciones del personal.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Se restringe la conexión de dispositivos personales a la red corporativa. Las PDA que se utilicen en el punto de pago deben gestionarse desde TI con un software de tipo Mobile Device Management, el cual tendrá controles de seguridad para prevenir la salida de información sensible fuera de la organización.

7.3.3. Clasificación De La Información.

- **Pública:** Información que puede ser conocida por todos los miembros enmarcados en el alcance y el público en general.
- **Clasificada:** Información que requiere la organización para la ejecución de su objeto social y puede ser accedida por el personal de PLAN B INVESTMENTS S.A.S. exclusivamente para el cumplimiento de las actividades diarias, alineadas a las funciones y responsabilidades del cargo, por lo que su divulgación a terceros se encuentra prohibido.
- **Confidencial:** Información que solo debe tener acceso personal específico y la revelación al público puede causar daño a la reputación, marca o estrategias de organización.
 - La Dirección de TI colocará a disposición de los líderes de las áreas de la compañía, los medios para resguardar la información confidencial.
 - Los Jefes de cada área deben clasificar la información de acuerdo a los tipos de información que ha definido la compañía y de esta forma darle el tratamiento y protección correspondiente.
 - Los jefes de cada área son los responsables de hacer la clasificación y resguardar la información que maneja su área.
 - El Jefe de cada área es el único que puede difundir, enviar y dirigir a las personas que considere adecuadas la información confidencial. El tratamiento de esta información se puede enviar a un colaborador con el mismo rango o superior y por debajo de este.

7.3.4. Control de Accesos de Usuarios.

- Cada colaborador, tercero y/o contratista que necesite ingresar a un sistema de información, equipo o servidor de Plan B Investments S.A.S debe contar con un usuario único e intransferible.
- Toda creación de usuario en cada sistema de información, equipo, servidor o servicio debe realizarse siguiendo lo establecido en el

 GFA-DCTI-PRC02 Procedimiento de creación, modificación o inactivación de accesos V1 ...

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- En cada sistema de información debe poderse identificar qué usuarios pertenecen a colaboradores de la compañía y cuáles pertenecen a terceros.
- Para los usuarios que pertenecen a colaboradores, todo sistema de información debe permitir asociar la cédula del colaborador a la cuenta de usuario que éste utilizará. No se debe permitir el ingreso al sistema de información si no se ha realizado la asociación de la cédula del colaborador.
- Para los usuarios que pertenecen a terceros, todo sistema debe controlar el acceso de los mismos por periodos de tiempo definidos. Para los sistemas de información, el acceso a terceros se otorgará sólo por 3 meses. Este plazo se ampliará toda vez que el responsable de Plan B Investments S.A.S hacia el tercero (quien contrata con el tercero) solicite ampliación de este periodo, esta solicitud se hará mediante correo electrónico.
- Una vez un usuario alcance más de 3 meses sin ingreso al sistema, el usuario debe bloquearse o inhabilitarse automáticamente.
- Se debe ejecutar una tarea mensualmente, la cual tomará todos los usuarios bloqueados que tengan más de 4 meses sin ingresar al sistema y los inactivará automáticamente.
- Se debe definir quiénes son los responsables de los usuarios administradores de los sistemas y que cuentan con amplios privilegios de acuerdo a los roles determinados por la organización y en caso de requerir accesos adicionales se tramitarán mediante **+ DCTI-FO10 FORMATO DE SOLICITUD DE PERMISOS ESPECIALES V4**
- Los usuarios genéricos o compartidos se encuentran restringidos y solamente pueden ser utilizados en casos excepcionales aprobados por la dirección de tecnología para acceder a los sistemas de información, aplicaciones o sistemas operativos en equipos de puntos de venta, centros de distribución y zonas administrativas. Estos usuarios deben cumplir con todas las normativas de seguridad definidas en este documento.

7.3.5. Segregación de Ambientes.

- La Dirección Corporativa de TI establecerá entornos aislados, contando con la plataforma requerida para tener ambientes de desarrollo, pruebas y producción; esto con el fin de controlar las actividades y mitigar el riesgo del acceso al ambiente productivo donde se encuentra información sensible de la compañía.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- El acceso a los sistemas de información en los ambientes de producción se debe restringir para todos los responsables de realizar desarrollos en Plan B Investments S.A.S.
- El comité de Seguridad informática, realizará monitoreo 2 veces al año para validar los accesos, las autorizaciones y la ejecución por parte de los responsables.
- Los usuarios terceros que tengan accesos a los sistemas de información y/o aplicaciones, deben acogerse a los lineamientos definidos y garantizar que solo sean utilizados para la ejecución de sus labores autorizadas.
- Todos los responsables de realizar desarrollos deberán habilitar el acceso a servicios, recursos e información de las aplicaciones sólo a usuarios autorizados. Así como también garantizar que estos accesos se den de forma protegida y segura.
- Todos los responsables de realizar desarrollos no deben almacenar contraseñas, cadenas de conexión u otra información sensible en texto claro; deben implementar controles de integridad de dichas contraseñas.
- Todos los responsables de realizar desarrollos deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de forma segura, evitando indicar específicamente cuál fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

7.3.6. Creación de contraseñas.

- Todos los sistemas de información que se utilicen en la compañía deben adoptar como mínimo estas políticas de contraseñas
- Todos los sistemas de información deben generar una alerta que indique que la contraseña se encuentra próxima a vencerse y en lo posible indicar la cantidad de días que faltan para su vencimiento.
- Los sistemas de información, correos electrónicos y servidor de dominio deben garantizar que las contraseñas creadas por los usuarios contengan combinaciones alfanuméricas. (alternando las letras entre mayúsculas y minúsculas excepto para los servidores Iseries).

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Los sistemas de información, correos electrónicos y servidor de dominio deben garantizar que la contraseña tenga una longitud mínima de 8 caracteres.
- información.
- Los sistemas de información, correos electrónicos y servidor de dominio deben garantizar que al quinto intento de acceso fallido, el usuario sea bloqueado.
- Los sistemas de información, correos electrónicos y servidor de dominio deben garantizar que no se reutilicen las últimas 3 contraseñas.
- Las contraseñas creadas por los usuarios no deben utilizar números secuenciales ni repetitivos. Por ejemplo: 5555 o 9898
- Las contraseñas creadas por los usuarios no deben utilizar la secuencia básica del teclado. Por ejemplo: "qwerty" o "asdf". Los usuarios deben asignar contraseñas sencillas de recordar. El administrador que asigna la contraseña por primera vez, no debe asignarla igual que el usuario.

7.3.7. Responsabilidad del Usuario.

- Todo colaborador, tercero y/o contratista es responsable de salvaguardar la información manejada en los diferentes sistemas que Plan B Investments S.A.S le haya suministrado.
- Todo colaborador, tercero y/o contratista es responsable del uso de su usuario y contraseña; la contraseña es personal e intransferible, no deberá ser conocida por ningún otro colaborador, incluyendo su superior o jefe inmediato. En caso de sospecha de que la contraseña ha sido comprometida, el colaborador, tercero y/o contratista debe realizar el cambio de la contraseña en sus distintos sistemas de información. (Ver *"DCTI-INS02 Instructivo para el cambio de contraseñas en los sistemas de información"*).
- Todo contratista y/o tercero en general deberá implementar medidas de seguridad adecuadas, tales como la encriptación de datos, control de accesos, auditorías periódicas para proteger la confidencialidad e integridad de la información entregada por PLAN B y en ese sentido no permitirá el acceso a la información a terceras personas, salvo que sea necesario para cumplir con una obligación legal o regulatoria.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Todos los colaboradores de Plan B Investments S.A.S deben garantizar que las contraseñas usadas de carácter laboral sean diferentes de las usadas en su ambiente personal.
- Todos los colaboradores de Plan B Investments S.A.S deben evitar que las contraseñas estén escritas en papel, o en cualquier otro dispositivo o medio de trabajo que no esté debidamente protegido y probado de forma segura.
- Todos los colaboradores de Plan B Investments S.A.S deben cumplir con los lineamientos de seguridad para la creación de contraseñas.

7.3.8. Control de acceso físico a centros de datos.

- El acceso a los centros de datos y/o comunicaciones de las sedes de la compañía está restringido al personal autorizado previamente por el Director Corporativo de TI o el Jefe de Infraestructura en nube, para ello se deberá seguir el paso a paso registrado en el “*DCTI-INS01 Instructivo de Ingreso y/o Manipulación Cuarto de Comunicaciones*”.
- Todo personal que requiera acceder a centros de datos y/o comunicación de las sedes de Plan B Investments SAS debe contar con la tarjeta de acceso autorizada por el Director Corporativo de TI o el Jefe de Infraestructura en nube asignada para su uso.
- Todo ingreso y salida de personas a los centros de datos y/o comunicación de las sedes de Plan B Investments SAS debe ser registrado de acuerdo al Formato para bitácora de ingreso y/o manipulación cuarto de comunicaciones
- Todo personal (interno o externo) que requiera acceder centros de datos y/o comunicación de las sedes de Plan B Investments SAS, y no cuente con tarjeta de acceso asignada, debe estar siempre acompañado por personal del área de sistemas autorizado para ingresar, quien se encargará de controlar las actividades que dichos visitantes desarrollen. Estos visitantes deben registrarse en la Bitácora de Accesos del Centro de Datos.
- Las instrucciones de acceso a los Cuartos de Cableado de los Puntos de Venta se definen en el documento “*DCTI-INS01 Instructivo de Ingreso y/o Manipulación Cuarto de Comunicaciones*”.

7.3.9. Uso De Los Controles Criptográficos.

- La Dirección Corporativa de TI debe propender que los sistemas de información que contengan información sensible y/o confidencial tengan cifrado.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- La Dirección Corporativa de TI debe asegurar que los Sistemas de Información que sean publicados vía web tengan un certificado digital HTTPS actualizado.
- La Dirección Corporativa de TI debe garantizar que los Equipos/Portátiles que manejen información sensible o crítica deben estar protegidos utilizando métodos criptográficos.
- La Jefatura de Infraestructura en Nube es la responsable de administrar y almacenar de forma segura las llaves implementando técnicas criptográficas.

7.3.10. Pantalla Limpia y Bloqueo de Sesión Inactiva.

- Los cambios en las imágenes corporativas son definidos en el Área de Desarrollo Organizacional dependiendo a sus necesidades o las campañas que realicen. La frecuencia de actualización será determinada por dicha área.
- El Área de Desarrollo Organizacional es la responsable de diseñar y enviar a la Dirección Corporativa de TI el fondo de pantalla y el protector actualizado para colocar en todos los computadores de la compañía.
- La Jefatura de Infraestructura en Nube perteneciente a la Dirección Corporativa de TI es la encargada de habilitar las imágenes que haya enviado el Área de Desarrollo Organizacional. Se deberá definir el tiempo de publicación de estas imágenes.
- Toda sesión de usuario en los equipos de cómputo abierta que tenga treinta (30) minutos de inactividad será bloqueada automáticamente a excepción de los celulares.

7.3.11. Gestión de Cambios.

- La gestión del cambio estará a cargo de un comité de cambios, el cual estará regido bajo un reglamento.
- Para cada cambio o mejoras a realizar en los sistemas de información o servicios de red, se deben respetar los niveles de aprobación definidos en el Procedimiento de Control de Cambios.
- El colaborador responsable del cambio debe disponer de las pruebas documentadas por parte de los analistas de soporte. Así mismo debe contar con la aprobación del usuario dueño del proceso, en los casos que aplique.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- El colaborador responsable del cambio debe guardar el versionamiento de los diferentes cambios que se realicen en los sistemas de información, para el caso que sea necesario se pueda restituir a la última versión de los sistemas de información.
- El colaborador responsable del cambio debe documentar los cambios instalados en el ambiente de producción de los sistemas de información, registrando la fecha, responsable, los componentes, programas y/o librerías utilizadas.

7.3.12. Protección Contra Código Malicioso.

- La Jefatura de Infraestructura en Nube deberá velar por la instalación de software de Antivirus, EDR, Antispyware y Antimalware que reduzca el contagio de código malicioso como control mínimo en los recursos informáticos de la compañía donde aplique.
- La Jefatura de Infraestructura en Nube deberá asegurar que estas herramientas se encuentren con el licenciamiento autorizado y con las últimas actualizaciones.
- La Jefatura de Infraestructura en Nube debe implementar los parches de seguridad del software relacionado con la detección de código malicioso de manera periódica y efectiva.
- Ningún colaborador está autorizado para configurar los programas relacionados a antivirus, EDR, antispyware y antimalware en los PCs y/o Portátil, no deben ser alterados ni cambiados. Esta labor está estrictamente a cargo del personal de tecnología de la compañía.
- Los colaboradores deben estar al tanto sobre las actualizaciones y /o notificaciones que le muestre su portátil o PC relacionados al antivirus. Si detectan alguna situación de sospecha sobre el funcionamiento o ejecución de programas no reconocidos, deben reportar de manera inmediata a la mesa de servicios de TI.

7.3.13. Intercambio de Información.

- Los colaboradores son completamente responsables de todas las actividades realizadas con sus claves y buzón de correo proporcionado por la compañía.
- Las cuentas de correos corporativas nombradas y/o personalizadas asignadas a nombre del colaborador son de uso exclusivo e intransferible. En caso de presentarse incidentes con la cuenta, el único responsable es el colaborador designado.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- Ningún colaborador de la compañía está autorizado para realizar el envío del número de tarjetas de crédito, fecha de vencimiento y CVV (Código Valor de Validación) por medio del intercambio de mensajes.
- Al compartir información de la compañía con proveedores o personal externo, el usuario debe asegurarse que:
 - La información sea enviada exclusivamente al remitente interesado y tenga estricta pertinencia con lo que este haya solicitado.
 - En el mensaje enviado o en los archivos adjuntos no se remita información de carácter confidencial o sensible para la compañía.

7.3.14. Uso de Mensajería Instantánea.

- La Jefatura de Infraestructura en nube tiene como responsabilidad lo siguiente: Asignar el acceso a servicios de mensajería instantánea utilizando la aplicación autorizada en la compañía.
- Los usuarios de la aplicación de mensajería instantánea no pueden enviar información clasificada como confidencial por este medio. Esta aplicación solo está autorizada como herramienta de apoyo (chat) para las tareas relacionadas con las funciones asignadas.

7.3.15. Uso de Correo Electrónico.

- Todos los colaboradores que posean correo electrónico corporativo deben utilizarlo como herramienta de apoyo para la realización de sus labores, está prohibido utilizarlo para uso personal ya que se considera una falta al Reglamento Interno de Trabajo.
- Todos los colaboradores que posean cuenta de correo corporativo deben aceptar las políticas de seguridad y se comprometen a cumplirlas.
- El Comité de Seguridad Informática así como la Dirección Corporativa de TI debe promulgar a través de campañas de concientización el buen uso del correo electrónico para el intercambio de la información.
- Todos los colaboradores inscritos con correo electrónico del dominio de Plan B Investments S.A.S son responsables en caso de presentarse la violación de seguridad en el uso del correo y deben responder por las consecuencias ante las autoridades que así lo requieran. La compañía

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

colaborará al máximo de sus posibilidades para investigar este tipo de actos, incluyendo la cooperación con la Justicia.

- Toda información contenida en los buzones de correo que Plan B Investments S.A.S asigna, pueden ser usados para propósitos comerciales, legales, financieros o de cualquier otra índole que la compañía estime conveniente.

7.3.15.1. Contenido del Correo Electrónico.

- El asunto de los mensajes no debe sobrepasar el número de campos disponibles para su redacción.
- El contenido de los correos electrónicos deberá cumplir los fines corporativos, por lo tanto está prohibido que los colaboradores intercambien información de otra índole. Además el área de tecnología de la compañía deberá aplicar filtrado de contenido a manera de control de seguridad.
- Cada colaborador que envía el mensaje deberá garantizar que todos los correos lleven al final las firmas establecidas por el personal de TI, la cual debe contener la siguiente información Nombre, Apellidos, Cargo, Dirección, Ciudad y Teléfono
- Está prohibido descargar , extraer y/o ejecutar archivos con contenido que pueda ser malicioso o no apropiado para el buen uso de los sistemas informáticos de la Compañía tales como software (programas o instaladores), sitios web no autorizados, juegos, vídeos, música, presentaciones, imágenes o contenido multimedia.
- Todos los correos enviados a terceros deben tener la cláusula de confidencialidad que dice lo siguiente:

“Este mensaje y los archivos que contengan el mismo son confidenciales y podría contener información privilegiada y reservada de PLAN B INVESTMENTS S.A.S., para el uso exclusivo de su destinatario. Si usted llega a recibir por error un correo, por favor elimínelo y avise inmediatamente al remitente, absteniéndose de divulgarlo de cualquier forma. El presente correo electrónico solo refleja la opinión de su remitente y no representa necesariamente la opinión oficial de PLAN B INVESTMENTS S.A.S o de sus directivos y por tal razón no se hace responsable en ningún caso por daños derivados de la recepción del presente mensaje.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

En virtud de lo establecido por la disposición de Protección de Datos Personales usted tiene Derecho a solicitar al emisor de este mensaje la rectificación, actualización, inclusión o supresión de los datos personales incluidos en su base de contactos, listas o cadenas de mensajes en los cuales usted se encuentre, salvo estipulación legal. Si desea informar un fraude o conducta inapropiada cometida al interior de la Compañía o en situaciones externas que la involucren, puedes escribir al correo electrónico: datospersonales@tiendasisimo.com donde atenderemos tu consulta o reclamo.”

- Se entiende que la cuenta de correo electrónico asignada al colaborador, tienda o Centro de Distribución donde se presten los servicios, constituye una herramienta de trabajo destinada exclusivamente al desarrollo de actividades laborales. En consecuencia, su uso debe ser racional, estrictamente vinculado a propósitos laborales y conforme con las políticas internas de la Empresa.
- Toda la información que circule a través de dicho medio será considerada material clasificado y de propiedad exclusiva de la Empresa.
- Queda expresamente prohibido el uso de las herramientas tecnológicas de la Empresa (correo electrónico, red de internet, sistemas de comunicación, entre otros) para fines personales, incluso fuera del horario laboral. Esta prohibición incluye, pero no se limita a, el envío o recepción de correos ajenos a la actividad laboral, navegación en sitios no autorizados y uso de plataformas de mensajería para asuntos personales.
- Las credenciales de acceso (usuarios y contraseñas) asignadas al colaborador son de uso personal, confidencial e intransferible, por lo cual está prohibido suministrarlas a terceros, incluidos otros empleados de la Empresa, salvo que exista una autorización expresa para ello.
- Por tratarse de recursos informáticos de propiedad exclusiva de la Empresa, el colaborador reconoce y acepta expresamente que la Empresa podrá acceder, monitorear y revisar en cualquier momento la información contenida en los equipos, sistemas y cuentas asignadas, sin que ello constituya una vulneración de su derecho a la intimidad, en la medida en que dichas herramientas han sido otorgadas para el cumplimiento de fines laborales.

7.3.15.2. Clasificación de la Emisión de Correos de acuerdo con su Contenido.

Para el envío de comunicaciones masivas, las cuentas de correo electrónico autorizadas son: comunicaciones@tiendasisimo.com y así mismo la cuenta de correo que corresponda a la Gerencia Ejecutiva.

Los temas que se consideran, pueden ser objeto de una comunicación masiva se listan a continuación, así como las áreas desde las cuales se podrá generar dicho tipo contenido:

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

Contenido del correo	Área que Emite
Información de Ingresos, Retiros y Traslados de Personal	Gerencia de Talento Humano
Lanzamiento de marcas propias	Gerencia Comercial
Nuevos Punto de Venta	Gerencia de Operaciones
Procedimientos, Instructivos, Formatos y demás documentos vitales para la organización.	Gestión Documental, Grupo de Auditoría y Procesos.
Ofertas y Eventos Catálogo Plan B Investments S.A.S	Gerencia Comercial
Mensajes de días especiales dirigidos a Plan B Investments S.A.S u oficinas centrales (Amor y amistad, navidad, Día de la madre, día del padre, entre otros)	Gerencia Ejecutiva, Gerencia de Talento Humano.
Información de interés general para la comunidad Plan B Investments S.A.S	Comunicaciones Plan B Investments S.A.S
Aviso de mantenimientos preventivos, correctivos de los servicios tecnológicos	Dirección de Tecnología e Información
Campañas y tips de seguridad informática	Comité de Seguridad de la Información

7.3.15.3. Asignación de Espacio en el Buzón del Correo

- Las cuotas de almacenamiento asignadas a los usuarios permiten almacenamiento de archivos en la nube, así como almacenamiento de correo electrónico. Por esta razón para eficiencia en el almacenamiento y optimización de costos la Dirección Corporativa de TI dispone de una estructura documental organizacional en la cual todos los usuarios deberán almacenar los documentos y archivos relacionados con sus procesos. Este espacio será centralizado y la cuota de almacenamiento será la que determine la Dirección de TI, garantizando que este sea el espacio suficiente para la organización. Cualquier solicitud de ampliación debe gestionarse a través del jefe inmediato.
- Cada usuario es responsable de mantener espacio disponible en su buzón de correo electrónico, realizando revisiones periódicas para mantener información vigente que le sea útil, eliminando

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

mensajes y/o archivos adjuntos antiguos que le permitan liberar espacio. Además podrá acudir a la mesa de servicios de TI para realizar respaldos de información en caso de que así lo requiera.

7.3.15.4. Difusión de Información por correo electrónico.

- Está prohibido el envío de material o información a terceras personas sin tener la autorización para hacerlo, que bajo el criterio de la compañía, sea considerada información confidencial o lesione sus derechos, su patrimonio, recursos o afecte de cualquier manera su buen nombre, sus estrategias comerciales, su relación con los clientes y entidades gubernamentales.
- Toda información enviada por correo electrónico no debe violar la propiedad intelectual de cualquier persona u otros derechos personales, en los casos que aplique.
- Está prohibido la difusión masiva de E-mail No Solicitados por los Destinatarios (del término inglés “spamming”).
- Está prohibido alterar, omitir, o anular títulos del mensaje, información de retorno de envío y/o las direcciones del protocolo de Internet para ocultar o esconder la identidad del origen de un mensaje.
- Está prohibido el uso de los servicios para almacenar, publicar, desplegar, transmitir y anunciar la pornografía infantil y en general cualquier tipo de pornografía. Plan B Investments S.A.S., notificará a las instituciones que respaldan la ley en caso de detectar la presencia de pornografía infantil transmitiéndose a través de las cuentas de correo.
- Está prohibido la difusión de esquemas de pirámides, cadenas de mensajes, actividades financieras o comerciales diferentes a las aprobadas por la Compañía, cualquier tipo de información sospechosa de fraude con tarjetas de crédito u otro medio de pago, visualización de la información de tarjetas de crédito de terceras personas sin su debido consentimiento.
- Está prohibido el uso de lenguaje, material obsceno, difamatorio, abusivo o amenazante en las cuentas de correo determinadas por Plan B Investments S.A.S.
- Está prohibido la difusión de información a través de las cuentas de correo que difame la buena reputación e integridad de la compañía.
- Plan B Investments S.A.S., podrá mostrar cualquier información en su posesión, incluyendo, sin

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

limitarse la información contenida en las cuentas de correo de sus colaboradores con el objetivo de obedecer una orden judicial o administrativa, En este caso, Plan B Investments S.A.S. no tiene ninguna obligación de notificar a ninguna persona, incluso al colaborador, sobre quién ha visto la información, o a quien se ha proporcionado la información.

8. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Se debe garantizar el cumplimiento de los requisitos de seguridad establecidos para los cambios o nuevos desarrollos implementados en los sistemas de información de la compañía, con el fin de minimizar los riesgos y aumentar la confiabilidad en sus sistemas de forma anticipada. Por lo tanto:

- La Dirección Corporativa de TI es la encargada de establecer por medio de buenas prácticas de construcción de software, las especificaciones de seguridad en la adquisición o desarrollo de los sistemas de información.
- El Comité de Seguridad de la Información tiene como función promover la definición de requerimientos de seguridad de los sistemas de información, en temas relacionados a los controles de autenticación y accesos a los sistemas de información, cifrado y protección de la información y servicios a la red.
- Los Desarrolladores Internos y Externos son los responsables de certificar en los desarrollos o programas los requerimientos de seguridad documentando los cambios o modificaciones realizados.

8.1. Seguridad Informática en las Relaciones con los Proveedores.

- La Dirección Corporativa de TI se encarga de asegurar que los proveedores de TI conozcan y divulguen a su personal, las políticas y procedimientos de seguridad informática de la compañía.
- La Dirección Corporativa de TI apoyado con la Dirección de Asuntos Legales de la compañía, asegurará que los formatos y/o minutas que formalicen las relaciones comerciales con los proveedores contengan los niveles de acuerdo de servicio, la cobertura geográfica de los servicios en relación al soporte, penalización por incumplimiento de esos niveles de servicio, términos de pago y demás obligaciones a cargo del proveedor conforme al servicio contratado.
- La Dirección Corporativa de TI en conjunto con el área de Asuntos Legales modela y revisa los

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

acuerdos de confidencialidad, de intercambio de información con terceros, estos acuerdos deben especificar la responsabilidad de la parte receptora de la información y las sanciones respectivas en caso de incumplimiento.

8.2. Prestación de Servicio por Proveedores.

- La Dirección Corporativa de TI a través de sus jefaturas y líderes tiene la responsabilidad de hacer seguimiento del cumplimiento de los servicios de TI, así mismo al manejo de incidentes y revisar los informes generados por el proveedor.
- La Dirección Corporativa de TI a través de sus jefaturas y líderes tiene la responsabilidad de revisar el cumplimiento de los niveles de servicio acordados dentro de los contratos suscritos con proveedores.
- La Jefatura de Infraestructura en Nube debe tener un adecuado manejo de los cambios originados en los diferentes servicios de TI.
- La Jefatura de Infraestructura en Nube tiene la responsabilidad de proveer las conexiones adecuadas con los proveedores para los accesos requeridos a los recursos informáticos.
- La Jefatura de Infraestructura en Nube debe establecer las condiciones de forma segura para los accesos a los datos desde y hacia terceros.

8.3. Gestión de Continuidad de TI.

- La Dirección Corporativa de TI debe definir los requisitos y niveles de disponibilidad de los sistemas de información.
- La Jefatura de Infraestructura en Nube debe analizar y establecer los esquemas de redundancia y contingencia necesarios para el correcto funcionamiento de los sistemas de información y elementos de infraestructura de red críticos para la compañía.
- La Jefatura de Infraestructura en Nube debe realizar pruebas periódicas sobre las soluciones de contingencia de TI implementadas.
- La Jefatura de Infraestructura en Nube debe Implementar las estrategias y procedimientos (a su cargo).
- El Comité de Seguridad de la Información en conjunto con la Dirección Corporativa de TI debe

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

construir y mantener actualizado el Plan de Continuidad de negocio.

- El Comité de Seguridad de la Información en conjunto con la Dirección Corporativa de TI debe liderar las pruebas correspondientes de los procesos y procedimientos del Plan de Continuidad de negocio.
- El Comité de Seguridad de la Información en conjunto con la Dirección Corporativa de TI debe validar que los esquemas de redundancia y contingencia implementados sobre la plataforma tecnológica, incluyan las consideraciones de seguridad informática pertinentes.

8.4. Medidas de seguridad comunes

8.4.1. Control de acceso.

El personal de PLAN B INVESTMENTS S.A.S, únicamente podrá acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por la compañía, como responsable de la información, de acuerdo con su rol o por solicitud de su jefe inmediato. Estos permisos serán concedidos por el área de tecnología conforme al requerimiento interno.

PLAN B INVESTMENTS S.A.S se ocupa del almacenamiento actualizado de bases de datos de usuarios, perfiles de usuarios, y accesos autorizados para cada uno de ellos. Además, tiene mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de documentos electrónicos, consiste en la asignación de contraseñas y permisos, y en el caso de documentos físicos, en la entrega de llaves de apertura de dispositivos de almacenamiento donde se archiva la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios, corresponde de manera exclusiva al personal autorizado.

Cualquier personal ajeno a PLAN B INVESTMENTS S.A.S, que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

8.4.2. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias deben ser borradas o destruidas de acuerdo a lo establecido en la  GFA-DCTI-G01 GUÍA PARA LA ELIMINACIÓN DE DOCUMENTOS Y DEPURACIÓN DE ARCHIVOS.pdf.... , impidiendo así, el acceso o recuperación de la información que contienen.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

8.4.3. Revisión Periódica del Comité.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

PLAN B INVESTMENTS S.A.S, realizará una auditoría extraordinaria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe que contendrá:

- El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
- La identificación de las deficiencias halladas y la sugerencia de medidas correctivas o complementarias necesarias.
- La descripción de los datos, hechos y observaciones en que se basan los dictámenes y las recomendaciones propuestas.

El comité de seguridad de la información, estudiará el informe y trasladará las conclusiones al responsable de administrar las bases de datos para que implemente las medidas correctivas.

8.5. Medidas de seguridad para bases de datos no automatizadas.

8.5.1. Archivo de documentos.

PLAN B INVESTMENTS S.A.S, fija los criterios y procedimientos de actuación establecidos por el área de Gestión Documental, que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los titulares.

Los documentos deben ser archivados considerando, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los sitios de almacenamiento de documentos deben disponer de llaves que controlen su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso PLAN B INVESTMENTS S.A.S., adoptará medidas alternas para impedir el acceso de personas no autorizadas.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir, en todo caso, que personas no autorizadas puedan acceder a ellos. La destrucción de documentos se debe hacer de acuerdo a lo establecido en la [PDF GFA-DCTI-G01 GUÍA PARA LA ELIMINACIÓN DE DOCUMENTOS Y DEPURACIÓN DE ARCHIVOS.pdf....](#) , para que se garantice que el documento no se pueda restaurar.

Los dispositivos de almacenamiento que contengan documentos con datos personales catalogados como “Sensibles” deben encontrarse en áreas protegidas con puertas de acceso con sistemas de apertura de llave. Estas áreas deben permanecer cerradas cuando no sea necesario el uso de dichos documentos. Si no fuera posible cumplir con lo anterior, PLAN B INVESTMENTS S.A.S., podrá adoptar medidas alternativas debidamente motivadas.

8.5.2. Acceso a los documentos.

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado, siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación catalogada como Sensible, tanto por usuarios autorizados como por personas no autorizadas de manera permanente, tal y como se refleja en el numeral referido anteriormente.

El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el Responsable de administrar la base de datos.

8.6. Medidas de seguridad para bases de datos automatizadas.

8.6.1. Identificación y autenticación.

PLAN B INVESTMENTS S.A.S debe garantizar que sus sistemas de información cuenten con métodos de autenticación segura que permitan identificar y autenticar de forma correcta a los usuarios, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos y demás información que estos alojen.

También ha de establecer mecanismos de doble factor de autenticación¹ que permita la identificación personalizada e inequívoca de todo usuario que intente acceder a los sistemas de información

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un

¹

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

procedimiento de asignación, distribución y almacenamiento de contraseñas. Para garantizar la integridad y confidencialidad de estas últimas, deben tener un mínimo de ocho caracteres entre ellos: contener mayúsculas, minúsculas, números, letras y carácter alfanumérico.

Por otra parte, PLAN B INVESTMENTS S.A.S., debe implementar parámetros de seguridad en sus sistemas de información que conlleven a sus colaboradores a realizar cambios de contraseñas de forma periódica, nunca por un tiempo superior a 30 días.

PLAN B INVESTMENTS S.A.S, también garantiza el almacenamiento automatizado, interno y cifrado de las contraseñas, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados y bloquear el acceso tras tres intentos.

8.6.2. Control de acceso físico.

Los lugares que son sede de los sistemas de información que contienen información de tipo Clasificada, confidencial o que contenga datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; asimismo, han de cumplir con las medidas de seguridad, correspondientes al documento o soporte acorde con la clasificación de la información que contiene. PLAN B INVESTMENTS S.A.S. tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas.

8.6.3. Copias de respaldo y recuperación de datos.

PLAN B INVESTMENTS S.A.S. debe llevar a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez al mes, excepto cuando no se haya producido ninguna actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, se deben establecer los procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán o complementarán manualmente los datos. PLAN B INVESTMENTS S.A.S., se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos. PLAN B INVESTMENTS COLOMBIA S.A.S., debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir las mismas medidas de seguridad exigidas para los datos originales.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

8.6.4. Registro de acceso.

De los intentos de acceso a los sistemas de información, PLAN B INVESTMENTS S.A.S, guarda, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

Los Responsables de administrar las bases de datos automatizadas se encargan de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, deben impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso. Los datos que contiene el registro de acceso deben conservarse por el tiempo que legalmente se encuentre establecido.

8.6.5. Redes de Comunicaciones.

El acceso a información a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso que se tiene dentro de las instalaciones de Plan B Investments.

8.6.6. Tratamiento de Datos de Titulares de Tarjetas

PLAN B INVESTMENTS SAS establece un compromiso firme con la seguridad de la información y el cumplimiento de los estándares internacionales, incluyendo el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS)

Teniendo en cuenta lo anterior, PLAN B INVESTMENTS SAS no almacena, procesa o transmite datos del titular de la tarjeta (Cardholder Data, CHD) ni datos confidenciales de autenticación (Sensitive Authentication Data, SAD) en ninguno de sus sistemas internos, incluyendo servidores, bases de datos, aplicaciones, archivos físicos o electrónicos, ni ningún otro medio. Todas las transacciones con tarjetas se realizan exclusivamente a través de datafonos administrados por terceros autorizados (proveedores de servicios de pago que cumplen con la norma PCI DSS), garantizando que la información de pago:

- Se transmite de forma segura y encriptada
- No es visible, accesible ni retenida por ningún componente de la infraestructura de PLAN B INVESTMENTS SAS
- Se transfiere directamente al procesador de pagos, quien es responsable del procesamiento y almacenamiento de los datos de la tarjeta conforme a su propia certificación PCI DSS.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

9. CUMPLIMIENTO Y ACTUALIZACIÓN

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Cada colaborador de planta, colaborador temporal, practicante, aprendiz y terceros en general que tenga algún vínculo con los procesos o que acceda a la información o plataformas tecnológicas de PLAN B, entenderá su rol y asumirá su responsabilidad respecto a los riesgos en Seguridad de la Información y de acuerdo con las políticas definidas. Este documento debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas, así mismo, debe adaptarse en todo momento a la normativa legal en materia de seguridad de la información incluyendo datos personales.

Incumplimiento. - El desconocimiento de la presente Política, así como su incumplimiento o la realización de cualquiera de las conductas expresamente prohibidas en ella, será considerado una falta grave y podrá constituir causal para la terminación del contrato de trabajo con justa causa, conforme con lo dispuesto en el numeral 6 del literal A) del artículo 7 del Decreto Ley 2351 de 1965, que modificó el artículo 62 del Código Sustantivo del Trabajo, lo que no obsta para que la Empresa pueda demandar la indemnización de los perjuicios de carácter intelectual, material, técnico, profesional e industrial que se le hayan ocasionado por parte del colaborador.

10. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los sistemas de información de PLAN B INVESTMENTS S.A.S., deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

PLAN B INVESTMENTS S.A.S, debe informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, cartelera de anuncios, etc.). De igual modo, debe poner a disposición del personal el presente documento para que puedan conocer la normativa de seguridad y sus obligaciones en esta materia en función del cargo que ocupan.

PLAN B INVESTMENTS S.A.S. cumple con el deber de informar con la inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, las funciones y obligaciones de su personal, las cuales, se definen, con carácter general, según el tipo de actividad que desarrollan y, específicamente, por el contenido de este documento. Cuando un colaborador trate documentos o soportes que contienen información clasificada, confidencial o que contengan datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

Las funciones y obligaciones de los usuarios de la información bajo responsabilidad de PLAN B INVESTMENTS S.A.S., son las siguientes:

Deber de Confidencialidad: Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a información de la Empresa y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los colaboradores de PLAN B INVESTMENTS S.A.S no pueden comunicar o revelar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

Parágrafo: El colaborador que, en desarrollo de la prestación de sus servicios, tenga acceso a información confidencial, está en la obligación de mantenerla en estricta reserva, con el fin de evitar perjuicios a la Empresa y a sus accionistas. Esta información confidencial incluye, pero no se limita a: documentos relacionados con productos, servicios, equipos, maquinaria, formulaciones, canales de venta, estrategias de mercadeo, publicidad, ventas y comercialización; análisis de la competencia; infraestructura; sistemas de información; archivos y bases de datos; información sobre proveedores y clientes; condiciones comerciales; volúmenes de negocio; costos de adquisición de materias primas; precios de venta; márgenes de utilidad; información fiscal, tributaria y de comercio nacional e internacional; proyectos de desarrollo de productos; conocimientos técnicos (*know-how*); así como cualquier otro aspecto relacionado con las actividades desarrolladas por la Empresa incluso si no se encuentra expresamente marcado como confidencial.

También se considera confidencial toda información relativa a nuevos negocios de la Empresa y/o de sus accionistas, así como cualquier documento o dato que el colaborador tenga en su poder, o que haya recibido, para la adecuada ejecución de sus funciones

Uso de recursos y materiales de trabajo: Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al jefe inmediato o a los responsables del área de Tecnología de la compañía, según corresponda.

Uso de impresoras, escáneres y otros dispositivos de copia: Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos. En caso de tratarse de documentos que ya no se requieren y en el caso explícito que contengan información sensible, deberán ser destruidos y no reutilizados como reciclaje para nuevas impresiones.

Obligación de notificar incidentes: Los colaboradores tienen la obligación de notificar los incidentes de las que tengan conocimiento a los responsables de administrar los sistemas de información, quienes se encargarán de

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

su gestión y resolución. (Ver “DCT-PRC03 Procedimiento de Gestión de Incidentes de Seguridad Informática”).

Responsabilidad sobre los terminales de trabajo y portátiles: Cada colaborador es responsable de las herramientas tecnológicas proporcionadas por PLAN B INVESTMENTS S.A.S. Cuando esté ausente de su puesto, debe bloquear su sesión en su equipo de cómputo para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el equipo al finalizar la jornada laboral, exceptuando aquellos donde el área de tecnología indique lo contrario. Asimismo, los colaboradores serán responsables de la custodia y buen uso de los equipos de cómputo que le sean asignados, y los mantendrán controlados con el fin de evitar su pérdida, daño o sustracción.

Uso limitado de Internet y correo electrónico: El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desarrollo de las actividades a su cargo en PLAN B INVESTMENTS S.A.S.

Salvaguarda y protección de contraseñas: Las contraseñas proporcionadas a los colaboradores son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar o recuperar la contraseña y el colaborador no pueda hacerlo por sí mismo deberá comunicarlo a los administradores de los sistemas de información.

Copias de respaldo y recuperación de datos: La Dirección de Tecnología de la compañía tendrá la responsabilidad de salvaguardar la información propia de los sistemas de información mediante copias y respaldos de información debidamente custodiados.

Archivo y gestión de documentos y soportes: Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas en el

 [GFA-DCTI-PG01 PROGRAMA DE GESTIÓN DOCUMENTAL.pdf](#)

Obligaciones relacionadas con las medidas de seguridad implantadas:

- Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
- No revelar información a terceras personas ni a usuarios no autorizados.
- Observar las normas de seguridad y trabajar para mejorarlas.
- No realizar acciones que supongan un peligro para la seguridad de la información.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- No extraer información de las instalaciones de la organización sin la debida autorización.
- No utilizar para ningún efecto, ni divulgar a terceras personas, naturales o jurídicas (i) los secretos comerciales, administrativos e industriales de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, (ii) este Acuerdo de Confidencialidad, (iii) las conversaciones previas a su aceptación, (iv) la información técnica o tecnológica o de diseño industrial de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, (v) los manuales, reglamentos, políticas, guías, lineamientos, circulares, memorandos de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, (vi) la información sobre los equipos, productos, formulaciones, materias primas, mantenimiento y fuentes de suministros de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, (vii) los costos, precios y presupuestos de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, (viii) la información sobre fórmulas de PLAN B INVESTMENTS S.A.S , (ix) los sistemas, operaciones, prácticas y políticas de seguridad de PLAN B INVESTMENTS S.A.S y/o de sus Accionistas, y (x) en general, cualquier clase de información que le haya sido entregada por PLAN B INVESTMENTS S.A.S y/o sus Accionistas con carácter de confidencial.
- No revelar los secretos o datos reservados de PLAN B INVESTMENTS S.A.S A y/o sus vinculadas y/o clientes y/o proveedores, así como la utilización para su beneficio o de terceros de cualquier información de PLAN B INVESTMENTS S.A.S a los que hubiere accedido debido a la prestación del servicio;
- No divulgar ni dar a conocer de ninguna forma y por ningún motivo la Información Confidencial, a menos que ello sea solicitado por autoridad competente, en cuyo caso, de todos modos, antes de proceder a entregar la información solicitada, deberá enviar copia de la solicitud en cuestión a PLAN B INVESTMENTS S.A.S junto con los antecedentes del caso.
- No utilizar la Información Confidencial recibida de PLAN B INVESTMENTS S.A.S y/o sus Accionistas para el beneficio de terceros o para sí mismo.
- Entregar a PLAN B INVESTMENTS S.A.S al momento de la terminación del contrato, o antes, toda la Información Confidencial que se encuentre en su poder, ya sea en medio escrito, magnético, digital y en general por cualquier otro sistema tecnológico con capacidad para almacenar información en cualquiera de sus formas. Si por alguna razón el colaborador descubre con posterioridad a la terminación de la misión que aún conserva Información Confidencial, así deberá informarlo a PLAN B INVESTMENTS S.A.S y a sus Accionistas y realizar la devolución en forma inmediata.

	PLAN B INVESTMENTS S.A.S. DIRECCIÓN CORPORATIVA DE TECNOLOGÍA E INFORMACIÓN	FECHA: 06/08/2025
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 3.0 CÓDIGO: DCTI-PO01

- No fotocopiar, copiar, grabar y en general no reproducir ninguna Información Confidencial y, en el evento de haberlo hecho, se compromete a la terminación de su misión, o antes, a devolver a PLAN B INVESTMENTS S.A.S las copias o reproducciones que haya realizado de la Información Confidencial obtenida en desarrollo de su prestación de servicios en misión.
- Utilizar la Información Confidencial única y exclusivamente para los propósitos propios del trabajo contratado.
- A tomar todas las medidas conducentes para evitar el uso inadecuado de la Información Confidencial o su filtración.
- Responder por la discreción y no divulgación o uso no autorizado de la Información Confidencial hasta después de la terminación de su contrato, en forma ilimitada, salvo autorización expresa por escrito del representante legal de PLAN B INVESTMENTS S.A.S.
- Dar estricto cumplimiento a lo dispuesto en las cláusulas de confidencialidad y tratamiento de datos personales –hábeas data– contenidas en el contrato de trabajo, así como a las obligaciones en este tema establecidas en la normativa legal vigente sobre la materia.

11. DISPOSICIÓN FINAL

- La presente Política forma parte integral de los contratos individuales de trabajo suscritos o que se lleguen a suscribir con los trabajadores de PLAN B INVESTMENTS S.A.S., salvo que se pacten estipulaciones en contrario, y siempre que dichas estipulaciones sean más favorables para el trabajador.
- Tanto la Empresa como sus trabajadores están sujetos al estricto cumplimiento de lo dispuesto en esta Política. Se presume, además, que todos los trabajadores conocen su contenido, por lo que, en ningún caso, podrá alegarse su desconocimiento.
- Esta Política ha sido aprobada por PLAN B INVESTMENTS S.A.S, como responsable del tratamiento de datos, aceptando su contenido, ordenando su ejecución y cumplimiento, con carácter general por todo el personal de la empresa, y en particular, por aquellos referidos en este documento.