POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Fecha de aprobación: Diciembre 20 de 2022

Contenido

INTRODUCCIÓN 4
DEFINICIONES 4
1. FUNDAMENTOS 7
1.1. PRINCIPIOS 7
1.2 OBJETIVO GENERAL 7
1.3 OBJETIVOS ESPECÍFICOS. 7
1.4 ORGANIZACIÓN DEL DOCUMENTO 8
1.5 ALCANCE 8
1.6. ORGANIZACIÓN Y RESPONSABILIDADES 9
1.6.1. Comité de Seguridad de la Información y Ciberseguridad 9
1.6.2. Seguridad de la Información y Ciberseguridad 10
1.6.3. Tics 10
1.6.4. Responsable de la Información 10
1.6.5. Comunidad (Usuarios de la Información) 11
1.6.6. Líneas de defensa. 11
1.6.6.1. Primera línea de defensa 11
1.6.6.2. Segunda línea de defensa 11
1.6.6.3. Tercera Línea de Defensa 12
1.7 CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA 12
1.8. ADMINISTRACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA 12
1.9. EXCEPCIONES A LA POLÍTICA 13
1.10. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA 13
2. POLÍTICAS INDIVIDUALES 13
2.1. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 13
2.2. PROPIEDAD INTELECTUAL 14
2.3. RESPONSABLES DE LA INFORMACIÓN 14
2.4. CUMPLIMIENTO DE REGULACIONES 14
2.5. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 15

2.6. CAPACITACIÓN Y CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 15

2.7. SEGURIDAD EN EL PERSONAL 16

2.8. TERCEROS QUE ACCEDEN INFORMACIÓN DE UNIPALMA S.A. LOCAL O REMOTAMENTE EN LOS APLICATIVOS LOCALES O EN EL CIBERESPACIO. 16

2.9. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL. 17

2.10. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN LOCAL O EN EL CIBERESPACIO. 17

2.11. CLASIFICACIÓN DE LA INFORMACIÓN. 18

2.12. CONTINUIDAD DEL NEGOCIO 18

2.13. SEGURIDAD FÍSICA 19

2.14. NO REPUDIO (RECONOCIMIENTO DE LAS TRANSACCIONES REALIZADAS) 20

2.15. ADMINISTRACIÓN DE ALERTAS 20

2.16. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD 20

2.17. CONECTIVIDAD 21

2.18. USO DE LOS RECURSOS INFORMÁTICOS DEL NEGOCIO LOCAL Y EN EL CIBERESPACIO, DE DISPOSITIVOS MÓVILES Y DE TRABAJO MÓVIL 21

3. SEGURIDAD EN NUEVAS TECNOLOGÍAS Y RIESGOS EMERGENTES 23

4. REGULACION 23

5. CAMBIOS POSTERIORES A LA CREACIÓN DE LA POLITICA. 24

INTRODUCCIÓN

El propósito de este documento es dar a conocer a los funcionarios de UNIPALMA S.A. la Política de Seguridad de la Información y Ciberseguridad establecida para la protección de la **información** y **sistemas de información**.
En el presente documento se incluyen los aspectos que deben tenerse en cuenta por parte de todos los funcionarios para que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (Confidencialidad); que esté protegida contra modificaciones no autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad) y que sea utilizada para los propósitos que fue obtenida (Privacidad) y que se deje el rastro de los eventos que ocurren al tener acceso a la información (Auditabilidad).

Por lo tanto, los funcionarios de UNIPALMA S.A. deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, ya que éstos soportan la Política de Seguridad de la Información y Ciberseguridad; en el entendido que la alta gerencia tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de seguridad de la información, de acuerdo con las responsabilidades asignadas dentro de la organización en relación con este tema.

DEFINICIONES

- **Activo de información**: Conjunto de datos con un contexto dato que vale la pena identificar, clasificar y proteger de acuerdo con su valor, criticidad y nivel de exposición.
- **Comunidad**: Son los usuarios de la información del negocio.
- **Confiabilidad**: La información debe ser la apropiada para la administración de la Entidad y el cumplimiento de obligaciones.
- **Colaborador:** Personal que maneja activos de información y presta sus servicios subordinados a Unipalma S.A.
- **Controles**: Salvaguardas basadas en dispositivos o mecanismos que se requieren para cumplir con los requisitos de una política.
- **Efectividad**: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
- **Eficiencia**: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
- **Información o Información del Negocio**: Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de soporte a las actividades de negocio y la toma de decisiones.
- **Internet**: Es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes.

- **Miembro de la Comunidad**: Un individuo que tiene autoridad limitada y específica del responsable de información para ver, modificar, adicionar, divulgar o eliminar información.
- **Modelo de Seguridad de la Información y Ciberseguridad**: Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.

- **Norma**: Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.
- **Organización de Seguridad de la Información y Ciberseguridad**: Estructura organizacional que soporta la Seguridad de la Información y Ciberseguridad, donde se definen roles y responsabilidades de cada uno de sus integrantes.
- **Perímetros o áreas seguras**: Un área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar activos de información con requisitos de seguridad y niveles de riesgo similares, para asegurar que cada zona se separa adecuadamente de las otras.
- **Política**: Es un conjunto de ordenamientos y lineamientos enmarcados, en los diferentes instrumentos jurídicos y administrativos que rigen una función, en este caso la Seguridad de la Información y Ciberseguridad.
- **Política de Seguridad de la Información y Ciberseguridad**: Documento donde se establecen las directrices y los lineamientos relacionados con el manejo seguro de la información en Unipalma S.A., que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.
- **Procedimiento**: Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.
- **Recursos de información**: Dispositivos o elementos que almacenan datos, tales como: registros, archivos, Bases de Datos, equipos y el software propietario o licenciado por Unipalma S.A.
- **Responsable de la información**: Un individuo o unidad organizacional que tiene responsabilidad por clasificar y tomar decisiones de control con respecto al uso de su información.
- **Riesgo**: La probabilidad de que ocurra un evento en seguridad de la información, que cause pérdida a Unipalma S.A.
- **Riesgo Inherente**: Aquel riesgo que puede existir de manera intrínseca en toda actividad. Puede generarse por factores internos o externos y afectar la rentabilidad y el capital de Unipalma S.A.
- **Seguridad de la información**: Protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.

- **Seguridad física**: Protección de los equipos de procesamiento de la información de daños físicos, destrucción o hurto; asimismo, se protege al personal de situaciones potencialmente dañinas.
- **NTC-ISO/IEC 27001**: Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos
- **NIST 800-53**: Proporciona un catálogo de controles de seguridad para todos los Sistemas federales de información de los Estados Unidos. Referenciado por la CE 007 de 2018 como uno de los marcos de referencia para tener en cuenta para la gestión de riesgos de Ciberseguridad.
- **Ciberseguridad**: Es el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger a los usuarios y los activos de la entidad en el ciberespacio.
- **Ciberespacio**: Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.
  Nota: Para el presente documento, se entenderá ciberespacio como el entorno donde se establezcan los servicios de la entidad y los prestados a través de terceros.
- **Ciberamenaza o amenaza cibernética**: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar un ciberataque contra la población, el territorio y la organización política del Estado.
- **Cibernética**: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnicas de funcionamiento de las conexiones de los seres vivos y de las máquinas.
- **Ciberataque o ataque cibernético**: Acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del ciberespacio.
- **Ciberiesgo o riesgo cibernético**: Posibles resultados negativos asociados a los ataques cibernéticos.
- **Evento de Ciberseguridad**: Ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.
- **Información en reposo**: Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, bases de datos, almacenes de datos, hojas de cálculo, archivos, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

- **Información en tránsito**: Información que fluye a través de la red pública o que no es de confianza, como Internet y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.
- **Terceros críticos:** Terceros con quien se vincula la entidad y que pueden tener incidencia directa en la seguridad de su información.
- **SGSI (Sistema de Gestion de Seguridad de la Información)**: Enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

1. FUNDAMENTOS

1.1. PRINCIPIOS

UNIPALMA S.A. ha establecido como fundamentales los siguientes principios que soportan la Política de Seguridad de la Información y Ciberseguridad:

a) La Información es uno de los activos más importantes de UNIPALMA S.A. y por lo tanto debe ser utilizada acorde con los requerimientos del negocio y conservando criterios de calidad (Efectividad, Eficiencia y Confiabilidad).
b) La confidencialidad de la Información del Negocio, así como aquella perteneciente a terceros, debe ser mantenida, independientemente del medio o formato donde se encuentre.
c) La Información del Negocio debe ser preservada en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
d) La Información del Negocio debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla; asimismo, presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.
e) La privacidad de la información de UNIPALMA S.A. debe ser preservada.
f) Los eventos que ocurren al tener acceso a la información de Unipalma S.A. deben dejar rastro y permitir la reconstrucción, revisión y análisis de la secuencia de estos.

1.2 OBJETIVO GENERAL

Establecer las directrices y los lineamientos relacionados con el manejo seguro de la información y sistemas de información, enmarcado en estándares internacionales de seguridad ISO 27001 y en normas de entes reguladores.

La presente Política de Seguridad de la Información y ciberseguridad es una declaración de las políticas, responsabilidades y de la conducta aceptada para proteger la Información del Negocio en UNIPALMA S.A.

1.3 OBJETIVOS ESPECÍFICOS.

Los objetivos específicos que persigue La Política de Seguridad de la Información y Ciberseguridad son:

a. Establecer los fundamentos para el desarrollo y la implantación del Modelo de Seguridad de la Información y Ciberseguridad
b. Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información que se encuentra en los aplicativos locales como en los implementados en el ciberespacio.
c. Establecer y comunicar la responsabilidad en el uso de los activos de información y sistemas de Información, que soportan los procesos y sistemas del negocio que se ejecutan en la infraestructura tecnológica local y la establecida en el ciberespacio.
d. Administrar los riesgos en seguridad de la información y Ciberseguridad.
e. Establecer los canales de comunicación que le permitan a la Gerencia mantenerse informada de los riesgos y uso inadecuado de los activos de información y sistemas de Información que se puedan presentar en la infraestructura local y el ciberespacio, y las acciones tomadas para su mitigación y corrección.

f. Proteger la imagen, los intereses y el buen nombre de UNIPALMA S.A.

g. Establecer las condiciones en el manejo de la información y Sistemas de Información que permita a Unipalma S.A., el cumplimiento del marco normativo exigido de los entes de control que la vigilan.

1.4 ORGANIZACIÓN DEL DOCUMENTO

El documento está organizado fundamentalmente en dos partes:

En la primera, se describe el objetivo general de la Política de Seguridad de la Información y Ciberseguridad, sus características, los responsables y la forma en que debe ser desarrollada, implantada y mantenida.

En la segunda, se desarrollan políticas individuales, que especifican la conducta aceptada por UNIPALMA S.A. en el manejo de su información y las acciones que deben ser tomadas para lograr los objetivos de la presente Política.

1.5 ALCANCE

La Política de Seguridad de la Información y Ciberseguridad da las directrices requeridas para implantar un Modelo de Seguridad de la Información y Ciberseguridad confiable y flexible, y define el marco básico que guiará la implantación de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con la seguridad de la información y ciberseguridad.

Esta Política de Seguridad de la Información y Ciberseguridad aplica para todos los niveles de la organización: usuarios (que incluye empleados y accionistas), terceros (que incluye proveedores y contratistas), entes de control y entidades relacionadas; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación.

Adicionalmente, la presente política aplica a toda la información creada, procesada o utilizada en el soporte al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Declaración de Compromiso

Unipalma está comprometida con la política de seguridad de la información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de seguridad de la información y Ciberseguridad. Por lo anterior deben:

- ✓ Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la política de seguridad de la información y Ciberseguridad.
- ✓ Promover continuamente una cultura de seguridad de la información y Ciberseguridad.
- ✓ Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y Ciberseguridad asociados al negocio y su relacionamiento con terceros.

Cada colaborador, funcionario temporal y proveedor, es responsable por aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos en seguridad de la información y Ciberseguridad, de igual forma es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

1.6. ORGANIZACIÓN Y RESPONSABILIDADES

La administración de esta Política será responsabilidad de quienes al interior de UNIPALMA S.A. desempeñen los roles que componen la Organización de Seguridad de la Información y Ciberseguridad así:

1.6.1. Comité de Seguridad de la Información y Ciberseguridad

Responsable por asegurar la planeación, implantación y mantenimiento de La Política de Seguridad de la información y Ciberseguridad; al igual que de la ejecución de las acciones requeridas para mantener los niveles de seguridad establecidos en la infraestructura tecnológica local y en el ciberespacio.

Sus integrantes atribuciones, responsabilidades y funcionamiento se encuentran descritas en el documento denominado Instructivo Reglamento Comité de Seguridad de la Información.

El Auditor Interno podrá asistir como invitado, en su calidad de evaluador del sistema de control interno, en el entendido que su presencia le permite tener un conocimiento actualizado de las actividades adelantadas para el mantenimiento del Modelo de Seguridad de la Información y Ciberseguridad de la organización y poder así de requerirlo, adelantar evaluaciones selectivas al tema.

1.6.2. Seguridad de la Información y Ciberseguridad

El área de Seguridad de la Información y Ciberseguridad será la responsable por emitir lineamientos para asegurar la implantación, mejoras, mantenimiento, verificación y cumplimiento de la Política de Seguridad de la Información y Ciberseguridad y los medios requeridos para lograrlo. Uno de estos medios es la realización de un Modelo de Seguridad de la Información y Ciberseguridad, del cual debe velar por su correcto desarrollo, mantenimiento e implantación. Adicionalmente el jefe de este proceso representará a UNIPALMA S.A. interna y externamente en todo lo referente al tema de Seguridad de la Información y Ciberseguridad.

1.6.3. Tics

Atendiendo los lineamientos emitidos por el área de Seguridad de la Información y Ciberseguridad, debe realizar una gestión efectiva de la Seguridad de la Información y Ciberseguridad en la infraestructura tecnológica local y la establecida en el ciberespacio para la entidad con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, mediante el aseguramiento, actualización, identificación de ciberamenazas, remediación de vulnerabilidades, mantenimiento y monitoreo de los elementos físicos y lógicos necesarios para la prestación de los servicios de la entidad y los prestados a través de terceros. Los resultados de tal gestión serán presentados semestralmente a la junta directiva a través del área de Seguridad de la Información y Ciberseguridad.

1.6.4. Responsable de la Información

Todos los colaboradores de UNIPALMA S.A. deben ser responsables por la confidencialidad y preservación de la información. Se considera Responsable de la información, quien requiere de la información con el objetivo de llevar a cabo su negocio y quien tiene la responsabilidad de administrarla y clasificarla, acorde con la importancia que la misma tiene para su área. También debe velar por el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios para su uso.

1.6.5. Comunidad (Usuarios de la Información)

Son los demás sujetos que utilizan la información y son responsables de proteger los activos de información de UNIPALMA S.A. por medio del cumplimiento de La Política de Seguridad de la Información y Ciberseguridad. Así mismo, deben estar alerta para identificar y reportar cualquier incumplimiento o falta de las normas o procedimientos establecidos.

UNIPALMA S.A. definirán los roles y responsabilidades requeridos para completar la definición de la Organización de Seguridad de la Información y Ciberseguridad, propendiendo siempre por la segregación de tareas como método para reducir los riesgos en el mal uso de la información.

1.6.6. Líneas de defensa.

Con el fin de adoptar y mantener una sólida cultura de Seguridad de la Información y Ciberseguridad, las tres líneas de defensa deben tomar la iniciativa de acuerdo con las siguientes definiciones:

1.6.6.1. Primera línea de defensa

La primera línea de defensa la constituyen las áreas de Tics junto con todos los colaboradores de Unipalma S.A. La Política de Seguridad de la Información y Ciberseguridad reconoce a las áreas de Tics y demás colaboradores como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de seguridad de la información y Ciberseguridad inherentes a los productos, actividades, procesos y sistemas de seguridad. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

1.6.6.2. Segunda línea de defensa

Esta línea de defensa está conformada por las áreas de Seguridad de la Información y Ciberseguridad o áreas equivalentes, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Seguridad de la Información y Ciberseguridad.
El Analista de Seguridad de la Información debe presentar los resultados de gestión directamente a la Gerencia. Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de

Seguridad de la Información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

1.6.6.3. Tercera Línea de Defensa

La tercera línea de defensa juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y Ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

1.7 CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

El cumplimiento de La Política de Seguridad de la Información y Ciberseguridad con sus respectivas normas es obligatorio para la Comunidad. Cada miembro de la Comunidad debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información y sistemas de Información de UNIPALMA S.A, Cualquier incumplimiento de esta Política que comprometa la Confidencialidad, Integridad, Disponibilidad y/o Privacidad y/o Auditabilidad de la información, puede resultar en una acción disciplinaria que puede llegar hasta la terminación del contrato de trabajo y a un posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen.

La Política de Seguridad de la Información y Ciberseguridad está basada en las mejores prácticas en seguridad de la información y Ciberseguridad y está acorde con la legislación nacional e internacional y por ende tomará los pasos necesarios, incluyendo las medidas disciplinarias y/o legales aplicables, para proteger sus activos y el uso de ellos.

1.8. ADMINISTRACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

La Política de Seguridad de la Información y Ciberseguridad se debe preservar en el tiempo. Por lo anterior, es necesario efectuar una revisión anual o ante cambios estructurales y normativos que afecten a Unipalma S.A., para asegurar que ésta cumple con el cambio de las necesidades del negocio. El líder de Seguridad de la Información y Ciberseguridad es responsable por esta tarea y debe llevarla a cabo con la participación del Comité de Seguridad de la Información y Ciberseguridad. Es decir, ante la necesidad de una adición o cambio en la Política, el Analista de Seguridad de la Información y Ciberseguridad proyectará

dichos cambios al Comité de Seguridad de la Información y Ciberseguridad de Unipalma S.A, para su posterior presentación a la Junta Directiva.

Cualquier miembro de la Comunidad puede identificar la necesidad de modificar la Política de Seguridad de la Información y Ciberseguridad. Dichas inquietudes y sugerencias deben ser comunicadas al Analista de Seguridad de la Información.

1.9. EXCEPCIONES A LA POLÍTICA

No hay excepciones a la presente Política.

1.10. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

La Política de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un programa de Seguridad de la información y Ciberseguridad, integrado en el día a día de la operación de UNIPALMA S.A. Un programa efectivo de Seguridad de la Información y Ciberseguridad es un proceso continuo, no un evento. Para lograr los objetivos establecidos en este documento, la presente Política anticipa y autoriza el desarrollo de normas, estándares, procedimientos operativos detallados y otras medidas administrativas, los cuales serán publicados para conocimiento de los funcionarios; así como el desarrollo o la adquisición de herramientas de software que ayuden a detectar o prevenir ataques contra los sistemas donde reside la información de UNIPALMA S.A. ya sea que se encuentre en los aplicativos locales o en el ciberespacio.

2. POLÍTICAS INDIVIDUALES

2.1. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

LA INFORMACION DEL NEGOCIO ES UN ACTIVO VITAL DE UNIPALMA S.A. POR LO TANTO DEBE SER PROTEGIDO

La información de UNIPALMA S.A. sin importar su presentación, medio o formato, en el que sea creada o utilizada para el soporte a las actividades de negocio, se califica como información del negocio o activo de información.

La Seguridad de la información y Ciberseguridad del negocio es el conjunto de medidas de protección que toma UNIPALMA S.A, contra una divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los responsables de la información son los responsables de asegurar que la información del negocio cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información.

UNIPALMA S.A, debe disponer de los medios necesarios para asegurarse de que cada miembro de la Comunidad preserve y proteja los activos de información y los sistemas de información de una manera consistente y confiable.

Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.

2.2. PROPIEDAD INTELECTUAL

LA PROPIEDAD INTELECTUAL DE LA INFORMACION DEBE MANTENERSE

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de UNIPALMA S.A.

Todo el material que es desarrollado mientras se trabaja para UNIPALMA S.A. se considera que es de su propiedad intelectual y de uso exclusivo de la misma, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de UNIPALMA S.A.

2.3. RESPONSABLES DE LA INFORMACIÓN

CADA ACTIVO DE INFORMACION DE UNIPALMA DEBE TENER UN RESPONSABLE QUE DEBE VELAR POR SU SEGURIDAD CON BASE EN LOS RIEGOS A LOS QUE ESTA EXPUESTA

UNIPALMA S.A. utiliza información para realizar sus actividades. Esta se crea y se entrega a cada miembro de la Comunidad para que pueda desarrollar y cumplir sus respectivas metas dentro del marco del negocio.

La información y los Sistemas de Información que UNIPALMA S.A. utilice para el desarrollo de sus objetivos de negocio deben tener asignado un Responsable, quien la utiliza en su área y es el responsable por su correcto uso. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso. En UNIPALMA S.A. actuarán como Responsables de la información, los Subdirectores, Directores y demás titulares de las dependencias que reporten directamente a la Gerencia o a quienes éstos deleguen.

2.4. CUMPLIMIENTO DE REGULACIONES

UNIPALMA S. A. DEBE CUMPLIR CON LAS REGULACIONES LOCALES E INTERNACIONALES DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

La Política de Seguridad de la Información y Ciberseguridad está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la privacidad, Seguridad de la Información y Ciberseguridad. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Modelo de Seguridad de la Información y se deben establecer acciones específicas para mantener alineada permanentemente a UNIPALMA S.A. con tales disposiciones. Ejemplo de estas disposiciones son el licenciamiento de software y circulares de la Superintendencia financiera entre otras.

Así mismo y con el fin de mantener un buen nivel de seguridad, esta Política se debe apoyar en las mejores prácticas de seguridad de la información y Ciberseguridad.

2.5. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD A QUE ESTÁ EXPUESTA LA INFORMACIÓN DE UNIPALMA S.A. DEBEN SER IDENTIFICADOS, EVALUADOS Y MITIGADOS ACORDE CON SU VALOR, PROBABILIDAD DE OCURRENCIA E IMPACTO EN EL NEGOCIO

La información del negocio se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través del Comité de Seguridad de la Información y Ciberseguridad, se debe realizar periódicamente un análisis del estado del negocio frente a la seguridad de la información, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo Responsable.

Establecidos el nivel de riesgo y el valor de la información, cada responsable debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por UNIPALMA S.A.

Cada usuario de la información y Sistemas de Información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de UNIPALMA S.A., y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información y la Ciberseguridad.

2.6. CAPACITACIÓN Y CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

UNIPALMA DEBE ESTABLECER UN PROGRAMA PERMANENTE DE CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA LOS USUARIOS Y TERCEROS

UNIPALMA S.A. debe contar con un programa permanente que permita asegurar que los usuarios y terceros están informados acerca de sus responsabilidades en Seguridad de la Información y de las continuas amenazas que ponen en riesgo la información que maneja.

Los funcionarios y terceros deben estar enterados de los procedimientos de seguridad de la información que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo. Como parte de su programa de capacitación, el nuevo personal debe asistir durante el periodo de inducción, a una charla sobre los requerimientos de seguridad de la información de UNIPALMA S.A.

2.7. SEGURIDAD EN EL PERSONAL

UNIPALMA S.A. DEBE PROVEER LOS MECANISMOS NECESARIOS PARA ASEGURAR QUE SUS EMPLEADOS CUMPLAN CON SUS RESPONSABILIDADES EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DESDE SU INGRESO HASTA SU RETIRO

Los empleados que ingresen a Unipalma S.A. deben seguir un proceso de selección, y una vez vinculados, se les socializara el documento “Política de la Seguridad de la Información y Ciberseguridad” para su conocimiento y certificación.

Los contratos de los empleados deben incluir cláusulas que indiquen las responsabilidades correspondientes para con la seguridad de la Información y el cumplimiento del código de ética y conducta, haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.

Se debe mantener un registro por empleado de su conocimiento y entendimiento de la Política de Seguridad de la Información y Ciberseguridad, mediante la certificación de este documento y las demás normas y procedimientos que se expidan al respecto.

UNIPALMA S.A. desarrollará un programa de manejo de sugerencias en seguridad de la información y Ciberseguridad, por medio del cual los colaboradores reportarán vulnerabilidades y riesgos que detecten.

2.8. TERCEROS QUE ACCEDEN INFORMACIÓN DE UNIPALMA S.A. LOCAL O REMOTAMENTE EN LOS APLICATIVOS LOCALES O EN EL CIBERESPACIO.

LOS TERCEROS QUE UTILIZAN LOCAL O REMOTAMENTE INFORMACIÓN DE UNIPALMA S.A. DEBEN CUMPLIR CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

El uso de la información de UNIPALMA S.A, por Terceros, que se encuentre en los aplicativos locales o en el ciberespacio y se acceda de manera ya sea local o remotamente, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política. En los contratos se debe incluir la obligación de proteger la información de UNIPALMA S.A, los requisitos de seguridad para mitigar los riesgos sobre la información y Ciberseguridad y las consecuencias a que estarían sujetos en caso de incumplirla.

Cada relación con un tercero debe tener un representante de alto nivel (tales como Gerentes, Subdirectores, Directores o sus Delegados) dentro de UNIPALMA S.A, que vele por el correcto uso y la protección de la información del negocio. Por lo anterior, y dadas las características de los negocios que se manejan en UNIPALMA S. A., donde terceros suministran información financiera para procesos de análisis y valoración, deberán suscribirse los acuerdos de confidencialidad respectivos con el fin de garantizar que la información suministrada se conserve en reserva.

2.9. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL.

TODOS LOS USUARIOS QUE ACCEDEN LA INFORMACIÓN DE UNIPALMA S.A. DEBEN DISPONER DE UN MEDIO DE IDENTIFICACIÓN Y EL ACCESO DEBE SER CONTROLADO A TRAVÉS DE UNA AUTENTICACIÓN PERSONAL.

Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de UNIPALMA S.A. ya sea local o en el ciberespacio. Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.

Los usuarios de UNIPALMA S.A. una vez creados y asignadas sus autorizaciones en el Sistema de Información, podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo, UNIPALMA S.A, definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

2.10. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN LOCAL O EN EL CIBERESPACIO.

EL USO DE LA INFORMACIÓN DE UNIPALMA S.A. DEBE SER CONTROLADO PARA PREVENIR ACCESOS NO AUTORIZADOS. LOS PRIVILEGIOS SOBRE LA INFORMACIÓN DEBEN SER MANTENIDOS EN CONCORDANCIA CON LAS

NECESIDADES DEL NEGOCIO, LIMITANDO EL ACCESO SOLAMENTE A LO QUE ES REQUERIDO.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información y Sistemas de Información se mantengan protegidos localmente y en el ciberespacio de una manera consistente con su valor para el negocio y con los riesgos de pérdida de Confidencialidad, Integridad, Disponibilidad, Privacidad y auditabilidad de la información.

Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso realizado localmente y en el ciberespacio a la información de UNIPALMA S.A. deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de UNIPALMA S.A. debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.

2.11. CLASIFICACIÓN DE LA INFORMACIÓN.

LOS RESPONSABLES DE LA INFORMACIÓN DEBEN CLASIFICAR LA INFORMACIÓN BASADOS EN SU VALOR, SENSITIVIDAD, RIESGO DE PÉRDIDA O COMPROMISO, Y/O REQUERIMIENTOS LEGALES DE RETENCIÓN.

Al igual que otros activos, no toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Toda la información de UNIPALMA S.A. será clasificada por el Dueño (Responsable) de la Información con base en un análisis de alto nivel del impacto al negocio en seguridad de la información y Ciberseguridad, que determine su valor relativo y nivel de riesgo a que está expuesta.

Según los riesgos que se detecten, el Responsable de la información y el Analista y/o Líder de Seguridad de la Información, determinarán los controles que sean necesarios para proveer un nivel de protección de la información apropiado y consistente en toda UNIPALMA S.A., sin importar el medio, formato o lugar donde se encuentre. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

Por lo tanto, no se debe asumir que otros protegen la información, ya que es deber de los funcionarios de UNIPALMA S.A, tomar las medidas necesarias para proteger la información.

2.12. CONTINUIDAD DEL NEGOCIO

TODOS LOS RECURSOS DE INFORMACIÓN Y LOS PROCESOS ASOCIADOS YA SEAN LOCALES O EN EL CIBERESPACIO, DEBEN CONTAR CON UN PLAN DE CONTINUIDAD DEL NEGOCIO Y ESTAR PREPARADOS PARA ATAQUES A LA

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. LA CONTINUIDAD DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD SE MANTIENE DURANTE SITUACIONES DE CONTINGENCIA.

La información debe estar disponible para su uso autorizado cuando UNIPALMA S.A. la requiera en la ejecución de sus tareas regulares. Por lo que se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de UNIPALMA S.A, tanto localmente como en el ciberespacio, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que utilice UNIPALMA S.A. como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso.

UNIPALMA S.A. establecerá medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques en seguridad de la información y Ciberseguridad como son los de negación de servicios y el ingreso de código no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a UNIPALMA S.A. de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

2.13. SEGURIDAD FÍSICA

TODAS LAS ÁREAS FÍSICAS DEL NEGOCIO DEBEN TENER UN NIVEL DE SEGURIDAD ACORDE CON EL VALOR DE LA INFORMACIÓN QUE SE PROCESA Y ADMINISTRA EN ELLAS. LA INFORMACIÓN CONFIDENCIAL O SENSITIVA AL NEGOCIO DEBE MANTENERSE EN LUGARES CON ACCESO RESTRINGIDO CUANDO NO ES UTILIZADA. TODOS LOS FUNCIONARIOS DEBEN CUMPLIR CON LAS DIRECTRICES PARA LA PROTECCIÓN FÍSICA DE LA INFORMACIÓN RESTRINGIDA O SENSITIVA QUE USEN.

Las áreas físicas construidas para soportar toda la operación del negocio deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.

Los recursos informáticos de UNIPALMA S.A. deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.

La información clasificada como confidencial o restringida no se dejará desatendida o sin control, por lo que UNIPALMA S.A. desarrollará un programa que permita prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual esta comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

2.14. NO REPUDIO (RECONOCIMIENTO DE LAS TRANSACCIONES REALIZADAS)

LA AUTENTICIDAD DE UN NEGOCIO O TRANSACCIÓN ELECTRÓNICA QUE REALICE UNIPALMA S.A. DEBE SER ASEGURADA YA SEA LOCALMENTE O EN EL CIBERESPACIO.

Unipalma S.A. se está apoyando día a día más en los medios electrónicos para realizar su negocio. Por lo tanto, para cualquier negocio o transacción que se haga por estos medios, Unipalma S.A. debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio).
Al realizar negocios electrónicos ya sea localmente o en el ciberespacio, se deben generar rastros que le permitan a Unipalma S.A. resolver conflictos cuando alguna de las partes niegue su participación. Estos se deben generar, guardar y ser accedidos acorde con las Políticas y las Normas que regulen estos aspectos en Unipalma S.A.

2.15. ADMINISTRACIÓN DE ALERTAS

UNIPALMA S.A. DEBE SER ALERTADA EN EL MISMO INSTANTE EN QUE EXISTAN VIOLACIONES A LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las situaciones o acciones que violen la presente Política deben ser detectadas, registradas e informadas al área de Seguridad de la Información de manera inmediata (alertas). Se debe desarrollar un programa de manejo de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información para UNIPALMA S.A. Dicho programa debe incluir la definición de una organización de reacción inmediata, con el objetivo de atender éstas y otras situaciones que UNIPALMA S.A. considere como críticas.

2.16. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

LOS REGISTROS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE UNIPALMA S.A. DEBEN SER REVISADOS PERMANENTEMENTE PARA ASEGURAR EL CUMPLIMIENTO DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Los Responsables de la Información deben definir los eventos considerados como críticos (por ejemplo: intentos de acceso fallidos al sistema de información, borrado o alteración de información, entre otros) y los respectivos registros de seguridad de la información y Ciberseguridad que deben ser generados. Los registros de seguridad de la información y Ciberseguridad deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna a los responsables, así como a los niveles requeridos. Los registros y los medios que los generan y administran

deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas.

2.17. CONECTIVIDAD

TODAS LAS CONEXIONES A REDES PÚBLICAS DEBEN SER AUTENTICADAS PARA PREVENIR QUE LA INFORMACIÓN SEA DEVELADA O ALTERADA

Las conexiones a la red privada de UNIPALMA S.A. deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida a otras empresas deben realizarse sobre redes aprobadas por UNIPALMA S.A.
Los miembros de la Comunidad que se conecten a la red privada deben cumplir con la presente Política antes de que se realice la conexión. Esto aplica igualmente a cualquier conexión actual o futura en la red de UNIPALMA S.A, que utilice redes públicas.

Se requiere la aprobación del responsable de la Información para poder acceder remotamente a la información de UNIPALMA S.A., y dichos accesos deben cumplir con la Política de Identificación y Autenticación.

2.18. USO DE LOS RECURSOS INFORMÁTICOS DEL NEGOCIO LOCAL Y EN EL CIBERESPACIO, DE DISPOSITIVOS MÓVILES Y DE TRABAJO MÓVIL

LOS RECURSOS INFORMÁTICOS PROVISTOS A LA COMUNIDAD LOCALMENTE Y EN EL CIBERESPACIO SON PARA USO EXCLUSIVO DEL NEGOCIO.

Los recursos informáticos de UNIPALMA S.A. tanto locales como en el ciberespacio, son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Miembros de la comunidad que intenten acceder a información para la que no tienen un requerimiento autorizado de negocio, están violando la presente Política.

En el uso de la información de UNIPALMA S.A. tanto locales como en el ciberespacio, no se debe presumir privacidad, por lo que cuando ésta sea utilizada se podrán crear registros de la actividad realizada, que pueden ser revisados por UNIPALMA S.A. de acuerdo con lo dispuesto en el documento que contiene las Normas de Seguridad de la Información y Ciberseguridad, que deben ser conocidas y aceptadas por todos los funcionarios. En caso de ser así, se ejecutarán los procedimientos correspondientes acorde con las regulaciones de UNIPALMA S.A.

UNIPALMA S.A. se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por UNIPALMA S.A. podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y

eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Área de Seguridad de la Información o el Área de Tics.

Para acceder a la información de Unipalma S.A. tanto locales como en el ciberespacio, a través de medios tales como los dispositivos o trabajo conectado remoto, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

2.19. SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD EN LOS PROCESOS DE ADMINISTRACIÓN DE LOS SISTEMAS

CADA PROCESO DE ADMINISTRACIÓN DE SISTEMAS DE UNIPALMA S.A. DEBE CUMPLIR CON LA PRESENTE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Actividades, normas y responsabilidades en seguridad de la información y Ciberseguridad deben ser incluidas dentro de cada uno los procesos de administración de sistemas de Unipalma S.A., para lograr el cumplimiento de la Política y las Normas de Seguridad de la Información y Ciberseguridad.

El área de Tics debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura. Los requerimientos de seguridad de la información y Ciberseguridad deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información y Ciberseguridad. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información y Ciberseguridad que han sido previamente establecidos. El nivel de Seguridad de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

La implantación de un sistema nuevo o cambio significativo a los existentes debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.

La realización de un cambio tecnológico a nivel local o en el ciberespacio que no considere los requerimientos de seguridad de la Información y Ciberseguridad hace que Unipalma S.A. este expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad y sus respectivas normas, y en caso de exponer a Unipalma S.A. a un riesgo en seguridad de la información y/o Ciberseguridad, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo responsable de la Información.

El área de Tics registra, asigna, hace seguimiento y resuelve situaciones (problemas) que comprometen la disponibilidad de los servicios que provee tecnología al negocio. Las fuentes de este proceso son los problemas derivados de situaciones que rompen o comprometen la Política de Seguridad de la Información y Ciberseguridad. Por lo tanto, todos los problemas de seguridad de la información y Ciberseguridad de UNIPALMA S.A. deben ser administrados por este proceso, el que con base en un análisis posterior determinará si corresponden a violaciones, problemas o vulnerabilidades en seguridad de la información y/o Ciberseguridad, dando paso a los procedimientos establecidos para cada caso.

3. SEGURIDAD EN NUEVAS TECNOLOGÍAS Y RIESGOS EMERGENTES

Es importante implementar un plan de Seguridad de la Información y Ciberseguridad, con relación a las nuevas tecnologías. Para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se debe:

- ✓ Establecer políticas de seguridad sobre las tecnologías que se implementen en Unipalma S.A.

- ✓ Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios, de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de Seguridad de la Información y Ciberseguridad.

- ✓ Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de proveedores que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos.

- ✓ Incluir en el plan de continuidad del negocio los requisitos y controles de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.

- ✓ Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de la organización, en materia de seguridad.

4. REGULACION

En Unipalma S.A. debe cumplir con las regulaciones de Seguridad de la Información y Ciberseguridad vigentes en el país y con regulaciones internacionales que se le obliguen a adoptar, como ejemplo se encuentran:

- ✓ **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.

- ✓ **Ley 1273 de 2009**: Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- ✓ **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- ✓ **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del habeas 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.

5. CAMBIOS POSTERIORES A LA CREACIÓN DE LA POLITICA.

FECHA	VERSIÓN	NATURALEZA DEL CAMBIO
10/06/2014	1	Creación de la política
01/06/2016	2	Se actualiza el documento para alinearlo con la nueva versión de la norma ISO 27001:2013 y con nuevas directrices de Seguridad de la Información (Ej: Ley de Protección de Datos Personales).
20/02/2019	3	Se incluye el compromiso de la gerencia con la política de seguridad de la información
01/02/2021	4	Se actualiza el documento para incluir temas relacionados a la Ciberseguridad y sistemas de Información de Unipalma
14/03/2022	5	Revisión, actualización y alineamiento con la Política de Seguridad de la Información y Ciberseguridad del grupo AVAL así: • Se actualiza el texto de introducción de la Política • Se incluye las definiciones relacionadas con seguridad de la información y Ciberseguridad • Se actualiza el objetivo de la política incluyendo temas relacionados con la Ciberseguridad. Circular 029/2014 • Se incluye al numeral 2.5 ALCANCE correspondiente a la “Declaración de compromiso” de la política de seguridad de la información y Ciberseguridad. • Se incluye en el numeral 2.6 “ROLES Y RESPONSABILIDADES” las definiciones de Líder de seguridad de la información y Ciberseguridad, Seguridad informática y Ciberseguridad, responsable de la información y las tres líneas de gestión de seguridad de la información y Ciberseguridad

		• Se incluye en el numeral 2.9 “IMPLANTACION Y PROGRAMACION DE LA POLITICA”. Involucra el desarrollo e implantación de un programa de seguridad de la información y Ciberseguridad • Se actualiza el numeral 3.19 “SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD EN LOS PROCESOS DE ADMINISTRACIÓN DE LOS SISTEMAS” en cuanto a mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura. Igualmente, a lo relacionado a registro y seguimiento de situaciones que comprometan la disponibilidad de los servicios que provee tecnología al negocio.
01/11/2022	6	✓ Se incluye portada para la presentación de la política ✓ Se agregan los ajustan las definiciones de Activo de Información, Colaborador, Responsable de la Información, Riesgo Inherente, Sistema de gestión de Seguridad de la Información y Ciberseguridad. ✓ Se elimina el objetivo del documento y se ajusta el objetivo General. ✓ Se ajusta la organización del documento y el alcance de acuerdo con los lineamientos corporativos. ✓ Se ajusta la organización de responsabilidades de acuerdo con su rol dentro de la comunidad. ✓ Se actualiza el esquema de las 3 líneas de defensa. ✓ Se actualiza el nombre del responsable del área de seguridad de la información y ciberseguridad que pasa a ser el Analista SI y Ciberseguridad como responsable del área. ✓ Se incluyen el ítem seguridad en nuevas tecnologías y riesgos emergentes. ✓ Se incluye el ítem regulación, con las normas de Seguridad de la Información y Ciberseguridad vigentes en el país y regulaciones internacionales que se le obliguen a adoptar.