POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PROTECCIÓN DE RIESGOS PR LTDA. ASESORES DE SEGUROS

1. ÁMBITO DE APLICACIÓN

En el presente documento y en toda norma o procedimiento asociado, cuando se mencione el término ***La Compañía*** deberá entenderse como una referencia a Protección de Riesgos PR Ltda Asesores de Seguros.

2. ALCANCE

Aplica a todos los empleados, asesores, personal tercerizado y proveedores, con los que *La Compañía* tenga vinculación comercial o laboral.

3. INFORMACIÓN

La Política de Seguridad de la Información de La Compañía aplica a todos los Activos de Información físicos, digitales y electrónicos, durante todo su ciclo de vida.

4. OBJETIVOS

La Compañía, consciente de la importancia estratégica de la información, dispondrá de los recursos necesarios para el adecuado uso de la misma y ha definido la presente

Esta política tiene los siguientes objetivos:

- Establecer unas normas obligatorias para proteger la información en *La Compañía*.
- Homologar los términos de seguridad de la información.
- Velar por el cumplimiento normativo.
- Determinar los roles y responsabilidades del manejo de la información.
- Establecer la clasificación de la información.
- Promover el uso correcto de la información según la clasificación de la misma.
- Definir políticas generales de calidad, seguridad y valoración y conservación de la información que garanticen la adecuada gestión de la misma.

5. CUMPLIMIENTO

La Política de Seguridad de la Información es de obligatorio cumplimiento por parte de todos los empleados, asesores, personal tercerizado y proveedores que presten servicios a La Compañía. Si un individuo u organización viola las disposiciones descritas en este documento, en el caso de los empleados se entenderá como una falta grave y si corresponde a vinculaciones de otra naturaleza, se entenderá como incumplimiento a las obligaciones de confidencialidad de información que le asisten, por lo tanto La Compañía se reserva el derecho de tomar las medidas correspondientes, las mismas que podrían incluso conllevar al ejercicio de acciones disciplinarias y legales, a la terminación y/o cancelación de contratos o vínculos contractuales de cualquier naturaleza, según sea el caso, y a que se pretenda la indemnización por los eventuales perjuicios que puedan llegar a causarse como consecuencia de la violación. El no acatamiento de la política aquí descrita, puede hacer vulnerable a La Compañía, exponiéndola a sanciones por parte de los entes de control, pérdidas financieras, de

imagen y credibilidad ante sus clientes y accionistas. Por esto el cabal cumplimiento de la misma hace parte de las responsabilidades de cada uno de los usuarios de la información de La Compañía.

6. ACTUALIZACIÓN Y PUBLICACIÓN

Este documento será modificado por la gerencia de La Compañía y/o por la Junta Directiva en la medida que se requiera y permanecerá en la "carpeta compartida" en una carpeta física y será enviado por correo electrónico a todos los funcionarios.

7. DEFINICIONES

- Activo de Información: Es un conjunto de datos relevantes para los procesos de La Compañía y qué residen en cualquier medio de almacenamiento.
- Calidad de Información: Es una combinación de estrategias, políticas, prácticas y tecnologías para garantizar que la información cumpla con los siguientes criterios:
  - Completitud: Mide el grado en que la información cuenta con todos los datos que se consideran críticos y necesarios para el proceso, para el área ó para el negocio.
  - Exactitud: Mide el grado en que la información cuenta con datos reales y precisos. Refleja la realidad del negocio.
  - Integridad: Mide el grado en que la información cuenta con las suficientes validaciones, las cuales son establecidas por reglas, parámetros y controles.
  - Consistencia: Mide el grado de igualdad de la información a través de toda la historia, y de los sistemas utilizados por la compañía.
  - 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.
  - Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.
- Ciclo de Vida de la información: Hace referencia a las diferentes etapas por las que atraviesa la información desde que es creada hasta su proceso de disposición final. Las etapas del ciclo de vida de la información en *La Compañía* son: Captura/Registro, Distribución, Transformación, Conservación, Uso y Descarte.
- Seguridad de la información: Asegurar la disponibilidad, integridad y confidencialidad de la información con el fin de garantizar la continuidad del negocio minimizando los riesgos de la información en los diferentes procesos.
- Disponibilidad: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- Confidencialidad: Es el acceso a la información únicamente por personas que cuenten con la debida autorización.
- Valoración y Conservación: Hace referencia a las políticas, procesos, prácticas y herramientas usadas para determinar la importancia de la información para el negocio, los medios y tiempos de conservación de la información adecuados según el valor de la misma, desde que ésta es creada hasta su proceso de disposición final.

8. ROLES Y RESPONSABILIDADES DE LOS ACTIVOS DE INFORMACIÓN

La Compañía ha definido los siguientes roles y responsabilidades, necesarios para una adecuada: gestión de la información.

8.1. JUNTA DE SOCIOS

Está integrado por los 4 socios de la compañía y tiene las siguientes responsabilidades respecto a la seguridad de la información:

- Definir, validar, aprobar y comunicar las políticas, procedimientos y controles generales aplicables a todos los Activos de Información de las compañías en cuanto a la seguridad, calidad, valoración y conservación de la información en todo su ciclo de vida.
- Validar que las políticas definidas sean consistentes entre sí, que estén alineadas con las estrategias del negocio, el sistema de control interno y el marco legal vigente.
- Realizar seguimiento a estas políticas de seguridad de la información
- Validar y aprobar los cambios en la definición de los roles y las responsabilidades de gobierno de información.
- Verificar la adecuada gestión de los Activos de Información prioritarios que afectan la continuidad del negocio.
- Ser un conciliador en la resolución de conflictos y temas de incidentes de información.
- Revisar y aprobar los términos del Seguridad de la Información.

8.2. DUEÑO DE ACTIVO INFORMACIÓN – GERENTE

Es el representante del Activo de Información ante la organización y responsable de:

- Definir y verificar las políticas de los activos de información que sean viables y de práctica implementación.
- Diligenciar, verificar y garantizar la adecuada gestión del inventario de los activos de información que tiene bajo su responsabilidad.
- Clasificar y valorar los activos de información según los criterios definidos.
- Definir y valorar los riesgos a los cuales está expuesta la información según su clasificación.
- Definir y verificar los controles y el plan de mitigación para garantizar la seguridad, calidad, valoración y conservación de la información.
- Definir y verificar los indicadores que permitan hacer seguimiento a la implementación de las políticas de sus activos de información y definir planes de mejoramiento.
- Atender y resolver los requerimientos que surjan relacionados con los activos de información.
- Implementar controles para vigilar la política de Seguridad de la Información.

8.3. CUSTODIO DE ACTIVO INFORMACIÓN

Implementar las políticas, procedimientos y controles definidos por la Junta de Socios y/o el Dueño del Activo de Información según la función que desempeña en la organización.

- Identificar riesgos y/o vulnerabilidades de los medios y mecanismos de custodia a los cuales está expuesta la información.
- Apoyar la implementación de los indicadores de seguimiento y los planes de mejoramiento definidos por el Dueño del activo de información.

8.4. USUARIO DE ACTIVO INFORMACIÓN

- Cumplir las políticas definidas para el Activo de Información del cual hace uso.
- Reportar incidentes o eventos relacionados con la información o que atenten contra las políticas o grupo de interés de La Compañía.

9. CLASIFICACIÓN DE LA INFORMACIÓN

La Compañía ha definido la siguiente clasificación de la información, con el objetivo de realizar una gestión de la misma acorde con su nivel de relevancia para los procesos del negocio.

9.1 INFORMACIÓN DE DOMINIO PÚBLICO

Es la información que ha sido declarada de conocimiento público por parte del Dueño del Activo de Información. Este tipo de información puede ser entregada o publicada a todo tipo de público (personas internas, externas de La Compañía y miembros de la competencia) sin restricciones y sin que esto implique daños a los grupos de interés, a las actividades, a los procesos de La Compañía.

9.2 INFORMACIÓN DE USO INTERNO

Es la información que utilizan los empleados de La Compañía para realizar las operaciones diarias del negocio y que no puede ser conocida por terceros sin previa autorización del Dueño del Activo de Información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de manera leve a terceros, a los sistemas y/o procesos de La Compañía.

9.3 INFORMACIÓN RESTRINGIDA

Es información de La Compañía que es utilizada sólo por empleados y un grupo de colaboradores o terceros para realizar sus labores y que no puede ser conocida por otros empleados, colaboradores o terceros sin autorización del Dueño del Activo de Información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante cualquiera de los grupos de Política de Gestión de Información interés de La Compañía (accionistas, empleados, clientes, proveedores) o a los sistemas y/o procesos de La Compañía.

9.4 INFORMACIÓN CONFIDENCIAL

Es aquella información que se encuentra definida por la ley, las regulaciones o el Dueño del Activo de Información como representante de La Compañía. Esta información únicamente puede ser conocida, utilizada y modificada por cualquier empleado y/o colaborador de La Compañía que lo requiera en función de su trabajo, previa autorización del Dueño del Activo de Información. Se debe llevar un registro de las consultas y/o modificaciones realizadas por los Usuarios de la información confidencial.

Para el caso específico de La Compañía, se considera confidencial la información contenida en las Historias Clínicas, así como también cualquier información que contenga la cédula o NIT del cliente que este acompañada de la siguiente información por compañía.

Seguros

(Generales y Vida)

- Valor asegurado
- Beneficiarios
- Valores de Cesión
- Relación de Bienes
- Declaración de Asegurabilidad
- Formulario del SARLAFT
- Información Bancaria
- Pagos de siniestros
- Diferentes titulares de la inversión.

10. POLÍTICAS GENERALES DE LA GESTIÓN DE INFORMACIÓN

- La Junta de Socios es la responsable de definir y articular los mecanismos de gestión de la información.
- Los Activos de Información de La Compañía deben ser identificados, clasificados y etiquetados de manera general para establecer los mecanismos necesarios para su adecuada protección.

- La información que exista en más de un medio (físico, electrónico, etc.) debe tener la misma clasificación, sin importar el formato en el que se encuentre.
- Se debe identificar el dueño de cada activo de información
- Cualquier información perteneciente a La Compañía no puede ser vendida, transferida o intercambiada con terceros para ningún propósito diferente a la de su actividad. En caso de requerirse, debe ser aprobado siguiendo los conductos regulares definidos por el Gerente en representación de La Compañía.
- Es responsabilidad de todo Usuario reportar todo acto que atente contra la seguridad de los activos de información, eventos sospechosos o de mal uso de la información que identifique.
- Identificar los diferentes riesgos asociados con los activos de información, que afectan o impactan los procesos de negocio.
- Realizar controles periódicos de Seguridad de la Información.
- Los usuarios deben hacer uso de los diccionarios de términos que estandarizan los conceptos de negocio.
- Cualquier información o conocimiento generado en los procesos de La Compañía es propiedad de la misma.

11. PILARES DE LA INFORMACIÓN Y SUS POLÍTICAS

Los pilares de la información sobre los cuales La Compañía realizará una gestión son: Calidad, Seguridad y Valoración y Conservación de la información

11.1 CALIDAD DE LA INFORMACIÓN

El dueño y el administrador del activo de información deben:

- Realizar un diagnóstico de la calidad de los activos de información, evaluando nivel de calidad en el que se encuentran, de acuerdo con los principios de completitud, exactitud, integridad, consistencia, efectividad, eficiencia y confiabilidad.
- Analizar las diferentes causas raíz de los problemas que afectan la calidad, en factores tales como el humano, los procesos y la tecnología.
- Establecer planes de acción efectivos para solucionar los problemas de calidad encontrados.

11.2 SEGURIDAD DE LA INFORMACIÓN

- Todos los Usuarios serán responsables de proteger la información a la cual accedan, conforme a su clasificación asegurando su confidencialidad, integridad y disponibilidad.
- El dueño de los activos de información, definirán y validarán los controles para proteger los activos de información contra los riesgos identificados.
- El custodio de los activos de información implementará los controles para proteger los activos de información contra los riesgos identificados.
- **La publicación y distribución de información confidencial o restringida de La Compañía en sitios públicos como internet (Ej.: prezi, slideshare, Dropbox, 4shared etc.), aulas de clase, presentaciones personales, entre otros está prohibida, salvo expresa autorización del dueño de la información. Para el caso de la información de Uso Interno debe ser autorizada por el Dueño del activo de información.**
- La información generada por La Compañía debe cumplir las normas sobre derechos de autor y de propiedad intelectual.

11.3 VALORACIÓN Y CONSERVACIÓN DE LA INFORMACIÓN

- Todos los activos de información deben tener definido los tiempos y medios de conservación en el inventario de activos de información, los cuales serán determinados para cada caso por el Gerente.
- Todos los documentos que soporten las operaciones que realiza La Compañía o que posean un valor legal, probatorio, fiscal, contable o histórico, deberán ser conservados en los centros de administración

documental (Archivos) que defina la organización. No se permite la creación de archivos alternos sin autorización.

- Ningún usuario está autorizado para destruir archivos físicos, salvo la autorización que emita en cada caso el Gerente, esta autorización se dará en los comités semanales y debe ser registrada en las actas. Cuando exista copia digital en el software de La Compañía y en los archivos de la aseguradora, no será necesaria la autorización expresa del Gerente.
- Los documentos electrónicos deben almacenarse en el archivo digital (software AIS).

12. USO DEL CORREO ELECTRÓNICO, INTERNET, DISPOSITIVOS MÓVILES, AIS, SISTEMAS INTERNOS DE LAS COMPAÑÍAS DE SEGUROS, ACCESO A LAS OFICINAS.

- Todos los empleados tienen correo @proteccionderiesgos.com y cualquier tema de la compañía debe ser exclusivamente manejado por este correo o por el correo prltda@asesorsura.com. Está prohibido abrir los correos personales desde lo equipos de La Compañía. Se hará un chequeo trimestral de todos los computadores. Salvo por el gerente y la asistente de gerencia, nadie puede tener la clave de acceso directo al servidor de su correo electrónico y todos los correos deben manejarse a través del Outlook vigente de cada empleado.
- Facebook YouTube y Twitter están deshabilitados de todos los computadores de La Compañía, salvo el de la gerencia que maneja las redes sociales de la compañía.
- La clave de la red de internet de la compañía no debe ser entregada a ningún visitante sin autorización del gerente o de su suplente.
- El manejo de AIS está restringido a la asistente de gerencia, el gerente, su suplente y las directoras técnicas de seguros de vida y seguros personales. Cada uno debe manejarlo con su propia clave y desde su propio equipo.
- Está prohibido compartir cualquier clave personal de cualquier funcionario, específicamente:
  - Claves de acceso a sistemas de las aseguradoras.
  - Claves de acceso a AIS.
  - Claves de acceso a correos electrónicos corporativos diferentes a prltda@asesorsura.com
  - Clave de acceso a computadores de dotación y celular subsidiados con acceso a correo electrónico.
  - Claves de la alarma de la oficina
- Cuando nuestro *oursourcing* de tecnología haga un back up al disco duro externo o haga las revisiones preventivas o correctivas, es indispensable que esté siempre en acompañado por el asistente administrativo de gerencia, el gerente o de su suplente.
- El teléfono celular de la compañía y los funcionarios comerciales que tengan su correo debe estar permanentemente bloqueado.
- Solo los comerciales podrán sacar sus computadores de dotación de las instalaciones de la empresa. Con autorización del gerente, los técnicos podrán llevarlos a sus hogares para trabajar en proyectos específicos.
- Solamente tendrán llave de la oficina, Argenis Díaz (o quien tenga su cargo a la fecha), Catherine Aguiar (o quien tenga su cargo a la fecha), la Gerente y el Subgerente. Cada una de estas personas tiene una clave privada de acceso.
- Salvo para temas corporativos de Protección de Riesgos y recepción de documentos de clientes en tránsito a las aseguradoras no debemos tener nada en los archivos físicos o copias. Cualquier documento confidencial o restringido, debe ser guardo bajo llave.
- Solamente el gerente o el subgerente podrán tener acceso a la llave del lugar donde se guarda la memoria externa que tiene la información del servidor y de los equipos de la compañía.

LA JUNTA DE SOCIOS