Seguros Atlántida, S.A. **En cumplimiento al art.22 de NRP-20 (Norma Técnica Para la Gestión Integral de Riesgos de las Entidades Financieras).**	Seguros Atlántida Año 2023

I. Políticas y procedimientos implementados durante el año.

Manuales	Manual de Gestión de Seguridad de la Información
	Manual de Controles de Seguridad de la Información
	Manual de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad
Políticas	Política de Incidente de Seguridad de la Información
	Política de Seguridad de la Información y Ciberseguridad
	Política de Externalización
	Políticas Específicas de la Seguridad de la Información
	Política de Dispositivos Móviles
	Política de Respuestas a incidentes de Seguridad de la Información y Ciberseguridad
	Política de Contingencia y Continuidad de Negocio
Programa	Programa de Seguridad de la Información
Plan	Plan Programa de Pruebas de Continuidad de Negocio
Procedimiento	Procedimiento de Respaldo de información

II. Medidas relevantes adoptadas para la Gestión Integral de Riesgos.

A. Riesgo de Liquidez.

Para la gestión de riesgo de liquidez, se monitorean los indicadores relacionados a este riesgo; establecidos en la Ley de Sociedades de Seguros de El Salvador, en la cual se disponen ciertos porcentajes como máximos y mínimos; además de la aplicación del método de Liquidez por Plazos

de Vencimiento y Simulación de escenarios de Tensión; como prueba de tensión aplicable a los rubros de balance.

B. Riesgo de Mercado.

Para la gestión de riesgo de mercado, se monitorea de acuerdo a la Ley de Sociedades de Seguros, se debe de mantener un portafolio equilibrado, que debe de cumplir con ciertos porcentajes que establecen plazos y límites máximos en las inversiones, activo fijo y bienes de capital; además de la aplicación de VAR (Value Ar Risk), como prueba de tensión, aplicable al portafolio de inversiones.

C. Riesgo de Crédito.

Para la gestión del riesgo de crédito, en el proceso de otorgamiento de fianzas, se aplica de acuerdo con el Manual de Política y suscripción de fianzas, que contiene la metodología para dicho proceso.

D. Riesgo Operacional.

Para la gestión del riesgo operacional, se aplica lo establecido en el Manual de Riesgo Operacional, la Metodología adoptada es en base a probabilidad e impacto. En cuanto a probabilidad de ocurrencia, los rangos van de 1 a 5 de la siguiente forma: 1 Remoto, 2 Poco Probable, 3 Posible, 4 Muy probable y 5 Cierto. En cuanto a su impacto la valoración es de 1 a 5 de la siguiente forma: 1 Insignificante, 2 Bajo, 3 Moderado, 4 Alto y 5 Extremo. Al multiplicar la probabilidad por el impacto se obtiene el grado de riesgo, los resultados por rango se describen de la siguiente forma: 1 Insignificante, de 2 a 4 Aceptable, de 5 a 9 Tolerable, de 10 a 19 Importante y de 20 a 25 Inaceptable. Después de obtener los grados de riesgo y consultar e identificar los controles se establece la ponderación de la efectividad de los controles de la siguiente forma: 30% Controles Altos, 60% Controles Medios, 90% Controles Bajos y 100% Sin Control. El riesgo operacional se define como la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, y la infraestructura.

E. Riesgo Legal.

El Riesgo Legal desde un punto de vista del riesgo operacional se clasifica en función de las causas que lo originan, se puede agrupar en tres grandes grupos: riesgo de documentación, riesgo de legislación y riesgo de capacidad; Seguimiento a litigios a favor o en contra de la compañía, reportados por el área legal.

F. Riesgo de Continuidad de Negocio.

La entidad posee un plan sistemático y organizado que permite, en caso de alguna emergencia, reactivar las áreas claves del negocio para reestablecer paulatinamente la operatividad hasta alcanzar la totalidad de esta; elaboración de políticas, manuales y planes referente a la continuidad de negocio.

G. Riesgo Estratégico

Al inicio de cada año se presenta a Junta Directiva para su aprobación los planes de trabajo y las principales estrategias a seguir durante todo el año, estas estrategias son monitoreadas para verificar el cumplimiento constantemente a lo largo del año, al cierre del año se evalúan los resultados finales.

H. Riesgo Reputacional

Es la posibilidad de que se produzcan pérdidas, debido al desprestigio, a la formación de una opinión pública negativa sobre los servicios prestados por la empresa y sus prácticas de negocios, que fomente la creación de una mala imagen o un posicionamiento negativo en el mercado, en los clientes, en los emisores, en los proveedores, en los socios comerciales, en el ente regulador y conlleve a una disminución del volumen de sus operaciones y clientes, a la caída de ingresos, etc.; seguimiento a cambios por normativas, actualización a manuales, políticas y procedimientos

I. Riesgo técnico

Posibilidad de pérdidas por una gestión inadecuada de la política de suscripción de riesgos, política de reaseguro, incumplimiento de los límites y condiciones de las pólizas, notas técnicas y bases actuariales; seguimiento a indicadores técnicos.

A. Riesgo de Seguridad de la Información y Ciberseguridad.

Es la probabilidad de que una amenaza se materialice y la información estratégica de la compañía o datos de clientes queden expuestos o sean modificados y utilizados de manera incorrecta; desarrollo de políticas, manuales y procedimientos, implementación de controles de seguridad, capacitación y concientización.