POLITICA DE SEGURIDAD DE LA INFORMACION (PSI)

VICEPRESIDENCIA DE RIESGOS

BOGOTÁ D.C. MAYO DE 2019

TABLA DE CONTENIDO

1. TABLA DE ANEXOS

Anexo No. 1. Requisitos mínimos de Seguridad para el desarrollo e implementación de aplicativos.
Anexo No. 2. Definición de información Confidencial

2. TERMINOS Y DEFINICIONES

ACTIVO DE INFORMACIÓN	Son todos aquellos activos que tienen algún tipo de relación con la información de la Compañía
CIBERRIESGO	Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan
CIBERSEGURIDAD	Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio y sistemas interconectados que son esenciales para la operación de La Compañía.
CID	Término que hace referencia a la Confidencialidad, Integridad y Disponibilidad
CIFRAMIENTO	Técnicas de codificación para protección de la información que utilizan algoritmos reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES o AES.
CONFIDENCIALIDAD *(Según C.E 042 de 2012)*	Hace referencia a la protección de información cuya divulgación no está autorizada.
DATOS PERSONALES	Corresponde a cualquier información relacionada con personas físicas, que tenga carácter de privado, que esté ligada a su intimidad y que haga referencia a temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros.
DISPONIBILIDAD *(Según C.E 042 de 2012)*	La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.
DISPOSITIVO MOVIL	Aparato electrónico de uso personal, con capacidad de almacenamiento y procesamiento, con conexión u opción de conexión a internet.
INCIDENTE DE SEGURIDAD	Evento de riesgo operativo que afecta la CID de la Información.
INFORMACION	Para efectos de la presente política, hace referencia a todos los datos de Mundial de Seguros, de sus clientes o sus terceros, conservados por, o en nombre de Mundial de Seguros
INFRAESTRUCTURA COMO SERVICIO – IaaS *(Según C.E 005 de 201)*	Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad la infraestructura que le permite ejecutar software de cualquier tipo, con el propósito de obtener la capacidad de procesamiento informático o de almacenamiento de información mediante servicios estandarizados.
INTEGRIDAD *(Según C.E 042 de 2012)*	La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
PLAN DE CONTINUIDAD DE NEGOCIO	Conjunto de políticas, procedimientos, recursos humanos y tecnológicos dispuestos por la Compañía para recuperar y restaurar sus procesos críticos parcial o totalmente interrumpidos dentro de un tiempo predeterminado después de una interrupción no deseada o desastre
PLAN DE RECUPERACIÓN DE DESASTRES	Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que la Compañía pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.
PLATAFORMA COMO SERVICIO -PaaS *(Según C.E 005 de 201)*	Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las plataformas en las cuales desarrollan y prueban distintas aplicaciones, mediante el uso de lenguajes y herramientas de

	programación que son gestionadas por el prestador de servicios. La entidad no administra ni controla la infraestructura del proveedor.
PROPIETARIO DE UN ACTIVO DE INFORMACIÓN	Persona designada por la Compañía como responsable de un Activo de Información
RIESGO	Probabilidad de ocurrencia de eventos inesperados que tengan afectación directa hacia la consecución de los objetivos de la Compañía
SEGURIDAD DE LA INFORMACIÓN	Conjunto de políticas, procedimientos, recursos humanos y plataforma tecnológica destinados por la Compañía para la protección de la CID de la Información.
SERVICIOS DE COMPUTACIÓN EN LA NUBE	Tecnología que permite el acceso en condiciones de ubicuidad, configurable y por demanda, a un conjunto compartido de recursos computacionales, que se pueden aprovisionar, configurar y liberar rápidamente, con poco esfuerzo de gestión o de interacción con el proveedor de servicios. Dicha tecnología puede prestarse a través de los modelos de servicios SaaS – Software como servicio, PaaS – Plataforma como servicio y IaaS – Infraestructura como servicio.
SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)	Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.
SOC (SECURITY OPERATION CENTER)	Unidad encargada de monitorear, evaluar y defender los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).
SOFTWARE COMO SERVICIO – SaaS *(Según C.E 005 de 201)*	Modelo de servicio en el cual el proveedor de servicios de computación en la nube pone a disposición de una entidad las aplicaciones que corren en la infraestructura de éste, bajo demanda y que pueden ser utilizadas de forma compartida con otros usuarios. La entidad no administra ni controla la infraestructura del proveedor.
VULNERABILLIDAD	Punto débil de un Activo de Información que permite que un atacante o un incidente comprometa su CID

3. MARCO NORMATIVO

Artículo 15 de la Constitución Política de la República de Colombia. – *"Derecho a la intimidad personal y familiar y al buen nombre"*

Ley estatutaria No. 1581 del 17 de octubre de 2013. - *"Disposiciones generales para la Protección de Datos Personales"*

Ley estatutaria No. 1266 del 31 de diciembre de 2008. -" *Disposiciones generales del Hábeas Data y regulación del manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"*

Numeral 4.1, Capítulo Noveno del Título Primero de la Circular Básica Jurídica (Circular 007 de 1996). – *"Reserva Bancaria"*

Parte 1 Titulo 2 Capítulo I *"Canales, medios, seguridad y calidad en el manejo de la información en la prestación de servicios financieros"*

Circular 014 de 2009 emitida por la Superintendencia Financiera de Colombia (modificada por la Circular Externa 038 de 2009). - "*Instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI)"*

Circular 007 de 2018 emitida por la Superintendencia Financiera de Colombia. - *"Requisitos Mínimos para la Gestión de Seguridad de la Información y la Ciberseguridad"*

Circular 005 de 2019 emitida por la Superintendencia Financiera de Colombia. - *"Instrucciones relacionadas con el uso de servicios de computación en la nube."*

Documento CONPES 3854 de 2016 emitido por el Consejo nacional de política económica y social – "*Política nacional de seguridad digital*"

Estándares y buenas prácticas

Requisitos y procedimientos de evaluación de seguridad en la industria de Tarjetas de Pago PCI v2.0

Normas Técnicas Colombianas NTC-ISO/IEC 27001 – 27002

Norma ISO/IEC 27032

Open Application Security Proyect (OWASP project)

Common Vulnerabilities and Exposures – Mitre (CVE – Mitre)

GNU General Public License (GNU - GPL)

Center of Internet Security - CIS

4. OBJETIVOS DE LA PSI

Los objetivos de la PSI, son los siguientes:

- Ofrecer los lineamientos necesarios para garantizar la protección adecuada de los Activos de Información de la Compañía, sus clientes y terceras partes.
- Garantizar la Seguridad de la Información durante los procesos de almacenamiento, procesamiento, consulta, transmisión y destrucción de la información.
- Definir las directrices necesarias para garantizar que los niveles de protección implementados sobre los Activos de Información sean consistentes con su nivel de importancia.
- Aplicar de forma adecuada la protección de la CID de los Activos de información, minimizando la exposición a riesgos de pérdida, fraude, deterioro, corrupción o uso indebido de los mismos.
- Asegurar el cumplimiento de la normatividad legal vigente y la adecuada aplicación de estándares locales e internacionales de Seguridad.
- Fomentar la aplicación coherente de procedimientos y controles de seguridad en todos los procesos de la Compañía.
- Definir las directrices para fomentar la conciencia de Seguridad entre el personal de la Compañía, los clientes y las terceras partes.

6. AMBITO DE APLICACIÓN DE LA PSI

La presente normativa se aplica sin restricciones a:

- La Compañía Mundial de Seguros S.A. y todas sus sucursales, CEN y terceras partes.
- Todo el personal vinculado contractualmente con la Compañía, ya sea de manera permanente o temporal.
- Terceros que en desarrollo de su actividad contractual con la Compañía tengan acceso a sus Activos de Información o a la información de sus clientes
- Terceros que desarrollen, mantengan, adquieran, utilicen, transmitan, transporten o destruyan cualquier tipo de Activo de Información de la Compañía.

La infracción o el incumplimiento de la presente PSI por parte de funcionarios de la Compañía, generará la ejecución de acciones disciplinarias contempladas en el Código de Conducta, en el caso de proveedores aplicaran las sanciones establecidas en el contrato suscrito por las partes

7. NATURALEZA DE LA SEGURIDAD DE LA INFORMACIÓN

Fuente: ISO/IEC 27032

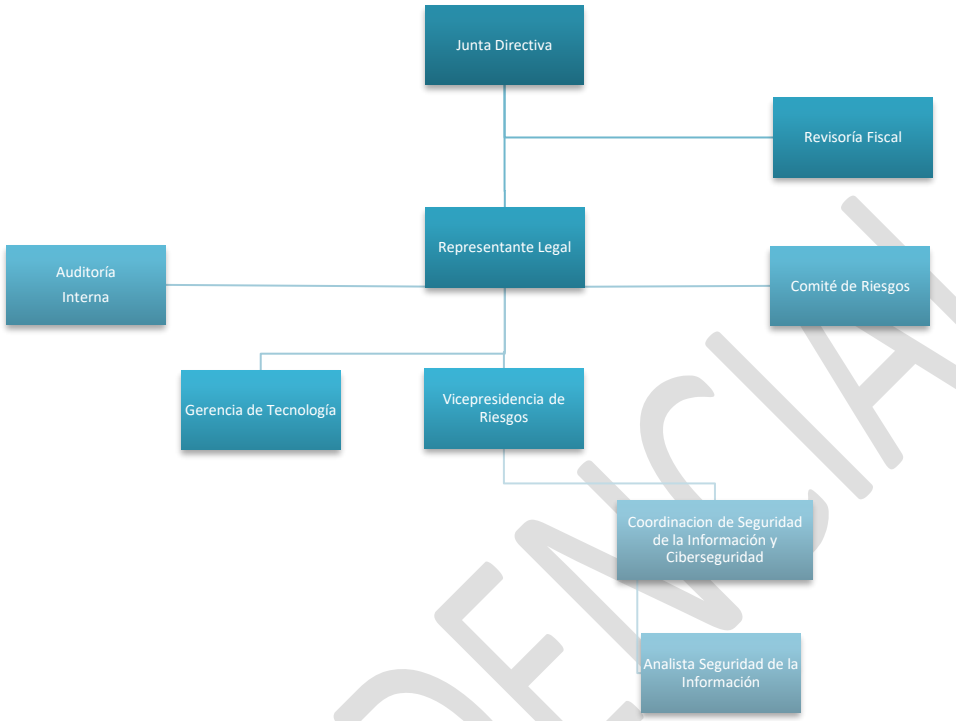
La Compañía ha decidido abordar la gestión de riesgos asociados a la Información, fundamentándose en los niveles de importancia y criticidad de esta, a partir del concepto de Seguridad de la Información. La estrategia se orienta hacia el objetivo de minimizar las amenazas y por ende los riesgos asociados a los Activos de Información, hasta un nivel adecuado para la Compañía.

Es necesario aclarar que la información se encuentra en diferentes estados, por ejemplo, en formato digital (a través de archivos electrónicos), en forma física (ya sea escrita o impresa en papel), así como de manera no representada (como pueden ser las ideas o el conocimiento de las personas).

Además, la información puede ser almacenada, procesada o transmitida de diferentes maneras: en formato electrónico, de manera verbal o a través de mensajes escritos o impresos, por lo que también es posible encontrarla en diferentes estados.

La Ciberseguridad busca proteger la información digital en los sistemas interconectados (procesamiento, almacenamiento y transporte) y se encuentra comprendida dentro de la Seguridad de la Información.

8. RESPONSABILIDADES Y ATRIBUCIONES CON RESPECTO A LA PSI



Se acogen las funciones y responsabilidades establecidas para cada una de las áreas funcionales y administrativas involucradas, de acuerdo con lo establecido en el Manual MIR. Las particularidades se establecen a continuación.

8.2 REPRESENTANTE LEGAL

- Incluir en el informe de gestión anual a que se refiere el artículo 47 de la ley 222 de 1995, un análisis sobre el cumplimiento de las obligaciones establecidas en la Circular Externa 042 de 2012 emitida por la Superintendencia Financiera de Colombia.

8.4. GERENCIA DE TECNOLOGIA

- Monitorear de manera permanente la plataforma tecnológica e informar cualquier novedad que implique perdidas de CID de los Activos de Información a su cargo.
- Coordinar Junto con la Vicepresidencia de Riesgos la ejecución del Plan de Continuidad de Negocio (PCN).

8.8 COORDINACION DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Documentar, revisar, actualizar y someter a aprobación por parte de la Junta Directiva la PSI
- Monitorear el cumplimiento de la PSI, estándares y procedimientos de Seguridad, de forma complementaria al proceso de Auditoría Interna.
- Difundir entre los empleados de la Compañía, la cultura de Seguridad, mediante procesos de capacitación y concientización a funcionarios nuevos, antiguos y a terceros cuya relación contractual con la Compañía involucre de alguna manera acceso a la información.
- Revisar y emitir un concepto favorable o desfavorable de forma previa a la salida a producción de nuevos aplicativos o herramientas tecnológicas, con respecto al adecuado cumplimiento de las políticas, estándares y normas legales vigente.
- Participar de forma activa en los nuevos proyectos adelantados por la Compañía, apoyando a las áreas de negocio en la identificación de riesgos y amenazas que puedan afectar la CID de los activos de información.
- Coordinar el levantamiento y actualización del Inventario de Activos de Información.
- Coordinar los procesos relacionados con la administración de los Incidentes de Seguridad
- Monitorear las violaciones de seguridad, evaluar y sugerir las acciones correctivas para garantizar el mantenimiento de los niveles de seguridad adecuados.
- Participar en las pruebas de seguridad realizadas a la arquitectura de sistemas de la Compañía.
- Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.
- La Coordinación de Seguridad de la Información y Ciberseguridad, será el área encargada de coordinar las comunicaciones y acciones en materia de Ciberseguridad con los organismos de control y autoridades competentes, así mismo reportará a la Alta Gerencia las acciones preventivas o correctivas que tengan a lugar.

8.9 EMPLEADOS Y TERCEROS CONTRATADOS POR DE LA COMPAÑIA

- Reportar y apoyar la gestión de Incidentes de Seguridad
- Atender las capacitaciones de Seguridad de la Información
- Poner en práctica los criterios y directrices de Seguridad de la Información establecidos en la presente normativa
- Procurar que los estándares y procedimientos asociados a cada uno de los procesos se ajusten a lo establecido en el presente documento.

9. GESTION DE ACTIVOS DE INFORMACION

9.1 RESPONSABILIDADES SOBRE LOS ACTIVOS DE INFORMACIÓN

La estrategia de Seguridad de la Información se enfocará en promover una adecuada administración de los Activos de Información de la Compañía, mediante el establecimiento de responsabilidades y funciones específicas sobre los mismos.

Se debe establecer para cada Activo de Información un "Propietario", quien será la persona responsable del mismo, los propietarios deberán tener capacidad de toma de decisiones con respecto a los activos a su cargo, de tal forma que puedan establecer y autorizar (entre otros) los permisos de acceso y los procedimientos de almacenamiento, custodia, transmisión y eventual destrucción del activo.

Los Propietarios de los Activos de Información son responsables del diligenciamiento y actualización del Inventario de Activos, el cual, deberá contener al menos la siguiente información:

<table>
<tr><td>Identificación de la fuente y origen de la información</td><td>Se debe identificar claramente en los casos en que aplique, el destino y la procedencia de los activos de información.</td></tr>
<tr><td>Definición de políticas de uso</td><td>Es responsabilidad de los Propietarios de los Activos de Información, establecer y administrar las políticas de uso adecuado y acceso al activo.</td></tr>
<tr><td>Clasificación de la información asociada al activo</td><td>Los Propietarios deberán asignar un valor a los Activos de Información a su cargo, lo anterior mediante la clasificación de acuerdo con los siguientes criterios:

De acuerdo con su nivel de Confidencialidad:

<table><tr><td>CONFIDENCIAL</td><td>La divulgación de la información está estrictamente limitada y predeterminada solamente a un número restringido y específico de personas que asumen la responsabilidad de protegerla.</td></tr><tr><td>PRIVADA</td><td>Información cuya divulgación se restringe únicamente al personal vinculado directa o indirectamente con la Compañía.</td></tr><tr><td>PÚBLICA</td><td>Información de uso general que por su contenido o contexto no requiere de protección especial y su distribución pública ha sido permitida a través de canales autorizados por la Compañía</td></tr></table>
De acuerdo con su nivel de Integridad:

<table><tr><td>CRITICA</td><td>Información cuya alteración, manipulación, divulgación o destrucción afecta de forma importante a la Compañía</td></tr><tr><td>NO CRITICA</td><td>Información cuya alteración, manipulación, divulgación o destrucción no afecta a la Compañía</td></tr></table></td></tr>
</table>

	De acuerdo con su nivel de Disponibilidad: INDISPENSABLE: La operación de la Compañía puede verse comprometida al no estar disponible el Activo de Información NECESARIA: El Activo de Información es importante para la operación de la Compañía, pero su falta de disponibilidad no afecta fuertemente la operación NORMAL: La falta de disponibilidad del Activo de Información no afecta la operación de la Compañía.

9.2 ETIQUETADO DE LA INFORMACIÓN

En la medida en que sea posible, los propietarios de los Activos de Información, deberán rotular, etiquetar o marcar los activos de información con la clasificación asignada a este de acuerdo con su nivel de confidencialidad (Confidencial, Privado o Público). Por ejemplo:

- Documentos en Word o PDF: Marca de agua
- Carpetas físicas y correspondencia: Rotulado o etiquetas

Según la clasificación de confidencialidad asignada al Activo de Información, las marcas deben ser " CONFIDENCIAL", " PRIVADO". No es estrictamente necesario rotular la información clasificada como pública.

9.3 ANALISIS DE RIESGOS

Los propietarios de los Activos de Información, con el apoyo de la Coordinación de Seguridad de la Información y Ciberseguridad, serán los encargados de identificar, medir, controlar y monitorear los niveles de riesgos inherentes y residuales asociados a los Activos de Información que se encuentren bajo su responsabilidad, siguiendo los lineamientos de la metodología descrita en el manual MIR.

10. SEGURIDAD EN LOS RECURSOS HUMANOS

Con el propósito de asegurar que todos los funcionarios y terceros contratados tengan claridad sobre sus deberes, responsabilidades con respecto a la Seguridad de la Información, se definen los siguientes lineamientos:

10.1 PROCESOS DE SELECCIÓN Y CONTRATACION

- Como parte del proceso de selección, debe adelantarse un proceso de verificación de antecedentes a cada aspirante a un cargo en la Compañía.
- Todo aspirante directo deberá contar con una visita de seguridad, de la cual se deberá dejar las evidencias respectivas de las siguientes validaciones:
    - Detalle la información socioeconómica del aspirante.
    - Detalle de antecedentes penales y disciplinarios.
    - Detalle de la verificación de referencias.
- La contratación de personal temporal que ocupe cargos catalogados como críticos, deberá contar con visita de seguridad.
- Se debe definir y documentar los roles y responsabilidades de cada cargo con respecto al cumplimiento de la presente PSI y a la normatividad legal vigente.
- Deben firmarse acuerdos de confidencialidad como parte del contrato de trabajo.
- Debe implementarse y documentarse procedimientos para la evaluación, selección, contratación y seguimiento de terceros.
- Todos los empleados Directos o Temporales, deberán firmar un acuerdo de confidencialidad.
- Todos los empleados Directos o Temporales, deberán firmar la autorización de protección de datos acorde a la ley 1581 de 2012.
- Los contratos de trabajo de empleados Directos o Temporales, deberán contar con las obligaciones de cara a la seguridad de la información y los activos entregados para la ejecución de las labores para las que es contratado, en cuanto a conservar la CID.
- Los contratos de trabajo deberán incluir obligaciones y responsabilidades para el manejo de la información recibida por parte de externos (clientes, intermediarios y proveedores).

10.2 DURANTE LA RELACION LABORAL

- Todos los empleados están obligados a conocer y cumplir los lineamientos impartidos en la presente política.

- Los empleados de la Compañía deberán recibir capacitación y concientización permanente acerca de Seguridad de la Información, así mismo todos los funcionarios están en la obligación de asistir a las capacitaciones y presentar las evaluaciones que permitan establecer el grado de preparación del funcionario de cara a la seguridad de la información
- Las normas, estándares, políticas y procedimientos de Seguridad de la Información estarán permanentemente disponibles para consulta todos los empleados de la Compañía.
- Es obligatorio que todos los empleados conozcan su rol y responsabilidades de seguridad de la información.
- Todos los funcionarios tendrán la obligación de atender las pruebas que se realicen al plan de continuidad de negocio.
- El incumplimiento a los lineamientos de la presente política y procedimientos conexos a la seguridad de la información dará lugar a la aplicación de las sanciones establecidas en el código de conducta.

10.3 DESVINCULACION DE EMPLEADOS

- Todos los empleados de la Compañía deben devolver todos los Activos de Información que estén a su cargo al momento de la terminación de su contrato.
- Los derechos de acceso a la información y a los medios de procesamiento de esta de todos los empleados de la Compañía deben ser retirados al momento de la terminación de su contrato.

10.4 TRASLADO DE EMPLEADOS

- Todos los empleados que cambien de cargo, deben devolver los Activos de Información que estén a su cargo.
  Todos los accesos a aplicaciones de los empleados que cambien de cargo serán revocados y es responsabilidad del jefe inmediato del área actual verificar el retiro efectivo de los privilegios.
- Es responsabilidad del jefe inmediato del área futura, solicitar los activos de información necesarios para las nuevas funciones del colaborador de manera previa al traslado.

11. CIBERSEGURIDAD

11.1 SEGURIDAD FISICA

11.1.1 AREAS SEGURAS

Con el objetivo de prevenir robos, daños, accidentes o desastres, la Compañía deberá establecer controles de acceso físico a sus instalaciones según su nivel de importancia, sensibilidad de los sistemas y Activos de Información alojados en estas. Los requisitos mínimos exigidos para tal efecto son:

- Se deberá implementar controles físicos de acceso en los puntos de ingreso, zonas de carga (si aplica), parqueaderos y todas las áreas de la Compañía, utilizando combinaciones de:
  a) Procedimientos de seguridad:(ej.: autorización de acceso a personas por parte de funcionarios autorizados)
  b) Medidas de control físico: Puertas, cerraduras, llaves, armarios, contenedores, cajas fuertes, etc.
  c) Medidas tecnológicas: Sistemas automáticos de control de acceso, circuito cerrado de televisión (CCTV), alarmas o dispositivos de detección de intrusos, etc.
- Todos los dispositivos técnicos de seguridad deberán instalarse y conservarse de conformidad con las recomendaciones de los fabricantes, y deberán ser probados regularmente.
- Los dispositivos técnicos de seguridad (particularmente los CCTV) deben ubicarse de manera tal que proporcionen la cobertura más eficiente, las cámaras del CCTV deben capturar la fecha y hora, tener una imagen clara tanto de día como de noche, no deben grabar las pantallas, los teclados o los terminales de ningún sistema.
- Las grabaciones de cámaras de CCTV ubicadas en oficinas de atención al público o sitios sensibles deberán ser conservadas por lo menos ocho (8) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.
- Los sistemas de control de acceso deben ser a prueba de fallos (Ej.: fallas eléctricas) y deben ser revisados periódicamente.
- Se debe proveer medios de identificación a todo el personal para ingresar a las instalaciones de la Compañía. La identificación de visitantes debe ser visible en todo momento mientras se encuentren dentro de las instalaciones
- La Compañía proveerá a todos los funcionarios y terceros que ejecuten sus labores dentro de las instalaciones de la Compañía un carnet de identificación y una tarjeta electrónica de acceso a las instalaciones, así mismo estos de manera obligatoria deberán portar en todo momento los elementos indicados anteriormente, de no hacerlo se aplicaran las sanciones previstas en el Código de Conducta.
- Debe existir un procedimiento claro para el acceso de los visitantes a las instalaciones de la Compañía, este procedimiento deberá ser sometido a auditorías periódicas
- Las salidas de emergencia designadas deben contar con mecanismos de seguridad que cumplan con los requisitos de seguridad de los organismos locales de riesgos.

En las oficinas de atención al público, se debe disponer de los mecanismos necesarios para evitar que personas no autorizadas

atiendan a los clientes o usuarios en nombre de la Compañía.

11.1.2 SEGURIDAD DE LOS EQUIPOS

- Los equipos y dispositivos que soporten el funcionamiento de la red de la Compañía como routers, servidores, switches, etc., deben mantenerse en un armario que se pueda cerrar de manera segura.
- Las consolas de los servidores deben estar permanentemente protegidas y en lo posible, deben estar fijadas dentro de armarios.
- Todos los equipos de cómputo de la Compañía deben ubicarse o protegerse de modo tal que se reduzca los riesgos de amenazas y peligros ambientales.
- Los computadores y dispositivos portátiles, en la medida que sea lo posible, deben permanecer asegurados con guayas de seguridad. los discos duros de los computadores portátiles deben tener medidas de ciframiento, de tal forma que se garantice que, en caso de pérdida o robo, la información será inaccesible.
- Los dispositivos móviles como teléfonos celulares o tabletas que tengan acceso a la red o a la información de la Compañía, deberán contar con medidas de protección que impidan su acceso por parte de personas no autorizadas.
- Todos los equipos de cómputo deben contar con medidas de protección ante interrupciones o fallas en el suministro de energía eléctrica.
- Todas las instalaciones de terceras partes que contengan Activos de Información de la Compañía deben reunir al menos los requisitos de seguridad definidos en la presente normativa y cumplir con las normativas locales en materia de Seguridad de la Información.
- Los servidores, terminales, equipos de cómputo y redes locales deberán contar con mecanismos o procedimientos necesarios que eviten la instalación de programas no autorizados o dispositivos que capturen o almacenen información.
- Se encuentra prohibido el uso de dispositivos como memorias USB, Discos duros Externos, unidades de lectura / escritura de CD o DVD. Las excepciones a la presente norma deberán ser avaladas por el Vicepresidente de Operaciones, quién podrá a su vez solicitar el concepto a la Coordinación de Seguridad de la Información y Ciberseguridad.
- Los equipos de cómputo de terceros que sean conectados a las redes de la Compañía deberán ser sometidos a procedimientos o protocolos de revisión y autorización de accesos que garanticen que la conexión sea realizada en condiciones de seguridad.

11.2 GESTION DE OPERACIONES Y COMUNICACIONES

11.2.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

- Se debe documentar y mantener de acuerdo con los requisitos del Sistema de Gestión de Calidad, todos los procedimientos realizados en la operación de la Compañía. Esta documentación debe estar disponible a los usuarios que la requieran.
- La totalidad de los cambios realizados en los diferentes sistemas de información de la Compañía deberán ser documentados y controlados adecuadamente.

11.2.2 ENTREGA DE SERVICIO A TERCEROS

La contratación de terceros deberá realizarse teniendo en cuenta parámetros y procedimientos establecidos por la Compañía para su evaluación, selección, contratación, seguimiento y desvinculación, los cuales a su vez deberán tener en cuenta los requisitos de seguridad establecidos en la normatividad legal vigente y en la presente normativa.

Los terceros contratados que, en desarrollo de su actividad, tengan acceso a información Confidencial de la Compañía o de sus clientes o realicen la atención parcial o total de los canales de prestación de servicios financieros a los que se refiere la Circular Externa 042 de 2012 o de los dispositivos usados en ellos, deberán cumplir como mínimo, con los siguientes requisitos:

- Incluir en los contratos que se celebren o en aquellos que se prorroguen, por lo menos, los siguientes aspectos:
  a) Acuerdos de niveles de servicio y operación.
  b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
  c) Cláusulas de propiedad de la información.
  d) Restricciones y requisitos de seguridad sobre el software y hardware empleado por el tercero.
  e) Especificación sobre las normas de Seguridad de la Información y Protección de Datos que aplican.
  f) Procedimientos a seguir cuando se presenten Incidentes de Seguridad
  g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.
  h) Procedimientos para intercambio de información Confidencial

- Los terceros contratados deberán disponer de planes de contingencia y continuidad de negocio debidamente documentados. Los terceros deberán verificar que estos planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

- Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados cuando se encuentren en las instalaciones de la Compañía.
- Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con la Compañía. En caso de que la información sea enviada por correspondencia física, se deberá garantizar que este proceso se realice en condiciones de seguridad.
- Implementar medidas de protección administrativas, físicas y técnicas razonables apropiadas a la sensibilidad de la información manejada.
- Los terceros son responsables de capacitar a sus empleados acerca de los requisitos de seguridad establecidos en la presente normativa y de garantizar su cumplimiento.
- Es responsabilidad del área a la cual el tercero le brindara apoyo, la verificación de los niveles de acceso de usuario, ingresos y retiros de funcionarios del tercero en cualquier aplicativo o herramienta de software de la Compañía.
- Las credenciales de usuario creadas sobre los sistemas requeridos por el tercero serán creadas por la Gerencia de Tecnología para todos los aplicativos, dichas credenciales serán entregadas al área solicitante mediante documento físico.
- Cuando los terceros contratados correspondan a Centros de Atención Telefónica (Call Center, Contact Center), estos deberán cumplir, como mínimo con los siguientes requerimientos:
  - ✓ Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.
  - ✓ Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.
  - ✓ Dotar a los equipos de cómputo que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por Mundial de Seguros. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.
  - ✓ Garantizar que los equipos de cómputo destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.
  - ✓ En los equipos de cómputo usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos ocho (8) meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

Los terceros contratados para la prestación de servicios de computación en la nube deberán cumplir de forma estricta con lo establecido en el numeral 18.1 de la presente política, sin perjuicio de lo establecido en el presente numeral.

Se deberá implementar los procedimientos necesarios para verificar el cumplimiento de las obligaciones señaladas en el

presente numeral, los cuales deberán ser informados previamente a la Auditoría Interna o a quien ejerza sus funciones.

11.2.2.1 TRANSMISION DE INFORMACION A TERCEROS CONTRATADOS

A continuación, se establecen los requisitos mínimos para el intercambio de información entre la Compañía y sus Intermediarios, Centros Estratégicos de Negocio, Proveedores o cualquier otro tercero que sea vinculado contractualmente con la Compañía.

- Las áreas de la Compañía responsables de la información recibida o enviada a terceros, deben garantizar que esta se encuentre protegida de una manera consistente con su nivel de CID.
- Todos los terceros deberán suscribir el acuerdo de confidencialidad previo a cualquier transmisión de información.
- No está permitido transferir información confidencial a través de repositorios en internet tales como Dropbox, Wetransfer, Box, Google Drive o similares.
- No está permitido transferir información confidencial a través de sistemas de mensajería instantánea o correo electrónico, en caso de ser requerido, cualquier tipo de documento que contenga información confidencial que sea enviado como adjunto o como parte de un mensaje de correo electrónico deberá ser sometido a procesos de cifrado.
- Las bases de datos o archivos que contengan información confidencial deberán ser cifrados y transmitidos a través del canal seguro dispuesto por la Compañía.

12.2.2.1.1 LINEAMIENTOS ESPECIFICOS DEL CANAL SEGURO

FTPS CORPORATIVO

Los terceros que no dispongan de sistemas de transferencia segura deberán utilizar el esquema FTPS implementado por la Compañía. Para habilitar el repositorio el área solicitante deberá radicar ticket a la mesa de servicio relacionando los siguientes requisitos en el formato destinado por la Gerencia de Tecnología:

- Razón social del tercero.
- IP pública del tercero.
- Estructura de los archivos a transmitir.
- Capacidad de almacenamiento.
- Relación de las personas que accederán desde el tercero al repositorio.
- Periodicidad de borrado de la información almacenada.

El repositorio no deberá almacenar información superior a 30 días calendario, para ello se realizarán eliminaciones periódicas a los archivos que excedan el periodo de tiempo indicado.

Para la interacción con el FTPS los terceros podrán utilizar las siguientes herramientas:

- FileZilla versión 3.2.2.1 o superior
- WinSCP versión 5.9.2 o superior

En caso de que el tercero utilice una herramienta diferente, las partes realizaran una revisión conjunta de la herramienta a utilizar verificando que esta cumpla las directrices del presente documento.

Es responsabilidad de las áreas encargadas de interactuar con los terceros, establecer el mecanismo de notificación al proveedor una vez se deje disponible información para descargar, así mismo se deberá establecer con el tercero la forma en que este notificará la transmisión de datos de retorno, este procedimiento deberá ser incluido en el Acuerdo de Niveles de Servicio (ANS).

La Dirección de Soporte Tecnológico generará el usuario y contraseña que utilizará el tercero para la conexión y transmisión de la información. La entrega de las credenciales de usuario deberá ser en medio escrito y en sobre sellado al área solicitante para que esta redirija el documento al tercero mediante entrega formal.

CANAL SEGURO PROPIEDAD DE LOS TERCEROS

Para los casos en que por definiciones del área de negocio se deba utilizar el esquema de transmisión segura propiedad del tercero; el área solicitante deberá garantizar que dicho esquema cumpla con los siguientes requisitos:

Las formas de trasferencia segura deberán ser de alguno de los siguientes tipos:

- FTPS (FTP/SSL).
- SFTP. (SSH/FTP)
- Portales corporativos de transferencia de datos que implementen el protocolo TLS v 1.2 o superior.

Se debe disponer de un proceso de eliminación periódica de la información transferida; este proceso de eliminación deberá realizarse como mínimo 1 vez al mes teniendo en cuenta la fecha desde la cual se almacena la información en el repositorio.

Se debe disponer de control de acceso al repositorio impidiendo que personal diferente al designado por el tercero acceda al repositorio.

11.2.3 PLANEACION Y ACEPTACION DEL SISTEMA

- Se debe establecer de forma clara los criterios de prueba y aceptación para los nuevos sistemas de información de la Compañía, teniendo en cuenta que la evaluación de estos debe ser adecuada al nivel de complejidad de cada herramienta. Antes de la entrada a producción, los resultados de las pruebas realizadas podrán ser revisada por el (las) área(s) responsable(s) y por la Vicepresidencia de Riesgos.
- Se debe realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y en general, tenga la posibilidad de acceder a los dispositivos y sistemas de información utilizados en la Compañía. En desarrollo de lo anterior, se deberá establecer procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de dispositivos y software autorizado.
- Se debe implementar, documentar, ejecutar y mantener los procedimientos de aseguramiento tecnológico necesarios para garantizar que se tiene en funcionamiento sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para la operación de la Compañía.

11.2.4 PROTECCION CONTRA SOFTWARE MALICIOSO

- Se debe implementar controles y herramientas de detección, prevención y recuperación de los sistemas informáticos ante ataques de software malicioso, así como los procesos de capacitación y concientización necesarios al personal de la Compañía.

11.2.5 PROTECCION DEL SOFTWARE

- La totalidad del software que se instala y se utiliza en la Compañía debe encontrarse adecuadamente licenciado bajo las normas legales aplicables, garantizando que la Compañía opere permanentemente dentro de un marco de cumplimiento normativo.
- Está prohibido para los usuarios de los sistemas de la Compañía, descargar, instalar o ejecutar software sin previa autorización de la Gerencia de Tecnología
- Todo software de código libre o cerrado que sea instalado en los equipos de cómputo de la Compañía deberá contar con la licencia respectiva, la cual deberá reposar de manera física o digital en los repositorios destinados para tal fin y deberá contar con el aseguramiento correspondiente.
- Todo software bajo Licencia de software de código abierto deberá cumplir los lineamientos mínimos de la licencia GNU GPL (GNU General Public License) o MIT License (Massachusetts institute of Technology), en caso de que el software utilice algún otro estándar de licenciamiento su instalación será aprobada por la Vicepresidencia de Riesgos

- No está permitido el uso de versiones portables de software.
- Está prohibido que los empleados generen copias del software dispuesto por la Compañía.
- Está permitida la instalación de software de prueba (demo o trial), si y solo si . se garantiza la desinstalación del software una vez finalice el periodo de prueba otorgado por el proveedor.
- No está permitido realizar pruebas a funcionalidades de software en los ambientes de producción, toda prueba deberá realizarse en el ambiente controlado destinado para tal fin.

11.2.6 COPIAS DE RESPALDO (BACK UP)

- Se debe tomar copias de seguridad de la información necesaria para la operación normal de los procesos de la Compañía, las copias de seguridad deben ser sometidas a pruebas de integridad periódicamente, de forma tal que se garantice plenamente la CID de la Información.
- Todos los usuarios cuya información se constituya en soporte importante para el desarrollo de la operación de la Compañía, deberán contar con un Back up diario a fin de mitigar perdidas de información

11.2.7 GESTION DE MEDIOS

- Se debe implementar, documentar y ejecutar procedimientos de manejo, almacenamiento, custodia y destrucción de medios magnéticos.

11.2.8 INTERCAMBIO DE INFORMACION

- Las llamadas telefónicas realizadas por los clientes a las líneas de atención o a los centros de atención telefónica establecidos por la Compañía, al igual que las llamadas de las áreas que intervienen en el proceso de inversiones de la Compañía (Back, Middle y Front Office) deberán ser grabadas en su totalidad y deberán ser conservadas al menos por un periodo de dos años, periodo durante el cual, deberán estar disponibles para su consulta. En caso de que las grabaciones sean objeto o soporte de una reclamación, queja o proceso de tipo judicial, estas deberán conservarse hasta el momento en que dicho proceso sea resuelto.
- La información que viaja entre las oficinas o sedes de la Compañía deberá estar cifrada usando hardware de propósito específico o software, o una combinación de los dos, empleando siempre mecanismos de Cifrado Fuerte. La Compañía deberá evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.
- Se deben documentar de forma clara los acuerdos y procedimientos para el intercambio de información entre la Compañía y entidades externas.

11.2.9 USO ADECUADO DEL CORREO ELECTRONICO

- La cuenta de correo electrónico asignada por la Compañía es de uso individual, por consiguiente, ningún funcionario de la Compañía o Tercero con acceso a cuentas de correo, debe utilizar una cuenta de correo que no sea la asignada. En los casos en que manejen cuentas de correo colaborativas (Ej: cumplimiento@segurosmudial.com.co, consumidorfianciero@segurosmundial.com.co), el área responsable de la cuenta deberá implementar y mantener los procedimientos necesarios para que la custodia este coordinada por un usuario responsable. En caso de que este usuario sea modificado, la entrega deberá ser realizada mediante acta y reinicio de contraseñas.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo a los objetivos estratégicos de la Compañía. El correo Corporativo no debe ser utilizado para actividades de índole personal.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Compañía. Cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los Usuarios de correo electrónico corporativo tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana o resulten ofensivas para los funcionarios de la Compañía y el personal provisto por terceros.
- No es permitido el envío de archivos que contengan archivos ejecutables o cuyas características se consideren peligrosas bajo ninguna circunstancia.
- Todos los mensajes enviados deben ajustarse al estándar de formato e imagen corporativa definidos por la Compañía y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- No está permitido él envió o recepción de información Confidencial (Bases de Datos, Información de clientes etc.) a través de correo electrónico, estos envíos se realizarán mediante canales de comunicación seguros definidos para cada caso.
- No está autorizado el acceso a cuentas de correo electrónico personales, las excepciones a esta política serán autorizadas por el área de Seguridad de la Información, parametrizadas y monitoreadas en los diferentes mecanismos de control basados en hardware y software de la Compañía. La cuenta de correo Corporativa no debe estar ligada a ningún tipo de Red Social, Foro, Blog etc., está prohibido vincular la cuenta de Correo con Redes de carácter personal.
- En caso de asignar a un tercero una cuenta de correo con el dominio corporativo esta deberá contar con un estudio previo de Funcionalidad a fin de determinar las opciones que esta cuenta tendrá habilitadas.
- En caso de detectar cuentas de correo con un alto flujo de correo Spam esta será cerrada y se efectuará un análisis de esta.

11.2.10 USO ADECUADO DE INTERNET

- No está permitido
  - ✓ El acceso a páginas con contenido que atente contra la ética y la moral de las personas, tales como, sitios con contenidos de hacking, discriminatorio, pornográfico, xenofóbico y demás condiciones que degraden la condición humana y que atenten contra las políticas de la Compañía o la legislación vigente.
  - ✓ El acceso y el uso de sistemas de mensajería instantánea, servicios interactivos o servicios multimedia que tengan como objetivo fines diferentes a los establecidos en los lineamientos estratégicos de la Compañía.
  - ✓ El intercambio de información con terceros a través de sistemas de intercambio de archivos.
  - ✓ La descarga, uso, intercambio o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución o cualquier otro tipo de información o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables o herramientas que atenten contra la CID de la infraestructura tecnológica, entre otros. En caso de requerir la descarga e instalación de algún tipo de software el usuario deberá solicitar a la Gerencia de tecnología su instalación; para ello deberá contar con el visto bueno del Jefe Inmediato y de la Coordinación de Seguridad de la Información y Ciberseguridad.

- La Compañía proveerá de los equipos y medios suficientes para efectuar el monitoreo permanente de los sitios visitados por los funcionarios o terceros contratados con acceso a la red, así mismo podrá inspeccionar registrar y evaluar las actividades realizadas durante la navegación o el uso de la red interna.
- Ningún funcionario o tercero contratado podrá asumir una posición en nombre de la Compañía en foros, redes de opinión, encuestas o medios similares, en los cuales la alta dirección no haya autorizado su participación.
- Para todos los funcionarios se ha definido un perfil de navegación el cual se ajusta a las funciones de su cargo, en caso de requerir algún tipo de cambio o elevación de perfiles, se deberá solicitar Visto bueno a la Coordinación de Seguridad de la Información y Ciberseguridad.
- Toda La información contenida en las aplicaciones de Google contratadas por la Compañía de manera corporativa son propiedad de la Compañía por tal razón esta será sujetas de monitoreos permanentes.
- Los usos de internet no considerados en las restricciones anteriores se encuentran permitidos siempre y cuando estos se realicen de manera ética y responsable y se ajusten a las políticas descritas en este documento.

11.2.11 USO ADECUADO DE LA RED CORPORATIVA

La red corporativa es la principal herramienta que dispone la Compañía para el desarrollo de su actividad, por tal razón esta herramienta contara con un monitoreo especial y permanente; a continuación, se indican las restricciones de uso aplicables a todos los usuarios:

- No está permitido bajo ninguna circunstancia conectar equipos de cómputo o dispositivos móviles de índole personal a la red Corporativa. Las excepciones a esta política deberán ser autorizadas por la Gerencia de Tecnología.
- No está permitido compartir a través de la red corporativa ningún tipo de Información externa o software que no se encuentre debidamente licenciado o tenga cubiertos los requisitos legales de derechos de autor.
- Es responsabilidad de los usuarios velar por el buen desempeño de la red y garantizar que sus accesos se ajustan a las atribuciones de su cargo.

11.2.12 USO ADECUADO DE LAS CONEXIÓNES VPN

Los funcionarios y terceros contratados que por razón de sus cargos o en cumplimiento del contrato suscrito, requieren conexión VPN, deberán cumplir los siguientes lineamientos:

- Los usuarios que tengan asignada conexión VPN son responsables en todo momento de la utilización de esta herramienta, por tanto, cualquier daño o perjuicio generado a la Compañía por el uso inadecuado de la herramienta, dará lugar a iniciar las acciones administrativas que correspondan.
- No está permitido el uso de múltiples conexiones VPN ni la utilización de agentes proxy para establecer la conexión.
- Toda sesión VPN que se encuentre en estado de inactividad, tendrá un tiempo establecido previo a la cancelación de la sesión.
- Todos los equipos de cómputo (servidores, equipos de mesa, equipos portátiles, etc.) que se conecten a los sistemas de la Compañía, deberán contar con un software antimalware, el cual será exigido por la herramienta.
- En caso de evidenciar la utilización inadecuada del usuario, la Compañía se reserva el derecho de cancelar el usuario, sin perjuicio de iniciar las acciones administrativas que den a lugar.
- Toda solicitud de conexión VPN deberá contar con visto bueno de la Gerencia de Talento Humano, esta solicitud deberá especificar claramente las razones que generan la necesidad de dicha conexión para el funcionario, así mismo se deberá aclarar si el funcionario realizara teletrabajo.
- Toda solicitud de usuario o conexión VPN para funcionarios o Centros estratégicos de Negocio, deberá contar con concepto de la Coordinación de Seguridad de la Información y Ciberseguridad. Para el caso de terceros contratados se deberá documentar en el contrato la entrega de los usuarios junto con los procedimientos de activación e inactivación de usuarios correspondientes.

11.2.13 MONITOREO

La Compañía debe proveer e implementar mecanismos de monitoreo que permitan garantizar lo siguiente:

- La totalidad de los relojes de los sistemas de información de la compañía deben estar sincronizados con la hora oficial colombiana, suministrada por la Superintendencia de Industria y Comercio.
- Las aplicaciones de la Compañía deben mantener un funcionamiento correcto respecto a sus parámetros de seguridad y salvaguardas contra posibles ataques.
- Se realicen pruebas periódicas de seguridad a la arquitectura de sistemas de la Compañía.
- Los riesgos asociados a la CID de Los Activos de Información de la Compañía se mantengan en niveles adecuados.

11.3. CONTROL DE ACCESO

Con el propósito de asegurar el acceso a los diferentes recursos informáticos de la Compañía y minimizar el riesgo de acceso no autorizado, se establecen los siguientes lineamientos:

11.3.1 CONTROL DE ACCESO A USUARIOS

Para asegurar el acceso de usuarios a los aplicativos y herramientas de software provistos por Seguros Mundial, se establecen los siguientes lineamientos:

- Los usuarios de los aplicativos deben contar con un identificador de usuario (ID) que debe ser único. En caso de intermediarios y puntos de venta autorizados por Seguros Mundial, este identificador deberá corresponder al número de la cédula de ciudadanía de la persona responsable o a un código alfanúmerico que lo identifique de forma única.
- Las contraseñas de usuario deben cumplir con los siguientes requisitos de seguridad:

  a) Debe tener como mínimo 10 caracteres de longitud

  b) No debe contener los caracteres “.”, “-“ o “_”

  c) Debe contener mayúsculas, minúsculas, números y (si así lo permite el software), caracteres especiales

  d) No debe contener secuencias de números o letras (Ej: **Pepito123**, **Juabcd987**, **Mundial123**)

  f) No puede contener la palabra “Mundial” en mayúsculas, minúsculas o en combinaciones de las mismas

- Los intermediarios y puntos de venta de Seguros Mundial a los que se les sea habilitado acceso a los sistemas de Seguros Mundial deberán al menos cumplir con lo siguiente

  a) Tener instalado y actualizado un software antivirus

  b) Conocer y manterner actualizado a su personal en cuanto a las principales ciberamenazas y riesgos latentes en internet, para lo cúal pueden tener en cuenta las publicaciones realizadas en el CAI Virtual de la Polícía Nacional de Colombia. https://caivirtual.policia.gov.co/. En caso de requerir información adicional o capacitaciones específicas, podrán consultar con la Vicepresidencia de Riesgos de Seguros Mundial

- El ID de usuario y la contraseña de acceso a los aplicativos provistos por Seguros Mundial son de uso personal e intransferible. El préstamo de usuarios y contraseñas será considerado como un incumplimiento al contrato o acuerdo comercial establecido. Cualquier acto relacionado con fraude o suplantación derivado con el mal uso del ID de usuario o contraseña, deberá ser asumido directamente por la persona o entidad responsable del ID de usuario.

- Los Usuarios genéricos serán permitidos siempre y cuando el aplicativo o la herramienta de software en donde sean implementados garantice la trazabilidad necesaria que permita la identificación y la verificación de las acciones realizadas por el usuario, así mismo la contraseña del usuario deberá cumplir los requerimientos indicados anteriormente.

- Las Contraseñas genéricas no están permitidas.

- Debe existir un procedimiento formal y documentado para la inscripción, modificación y retiro de usuarios en todos los sistemas de información de la Compañía.

- Es responsabilidad de los usuarios administradores de cada Activo de Información (aplicativos, herramienta de software, carpetas compartidas, etc.) revisar periódicamente los privilegios de acceso otorgados mediante un procedimiento debidamente formalizado y documentado.

11.3.2 RESPONSABILIDADES DE LOS USUARIOS

- Los usuarios de los sistemas de información de la Compañía deben seguir las políticas y las buenas prácticas en materia de utilización de contraseñas.

- Cuando los usuarios se retiren de sus equipos, deben procurar dejar bloqueada las sesiones mediante el uso de las teclas (Control+Alt+Supr) o (Windows + L)
- Se debe mantener el sitio de trabajo limpio, evitando dejar al alcance documentos importantes, así mismo el escritorio de Windows debe mantenerse al mínimo de documentos u accesos directos que permitan acceder a información sensible.

11.3.3 USUARIOS PRIVILEGIADOS

Se consideran usuarios privilegiados, a los siguientes:

- Las cuentas de superusuario, como las de los administradores de bases de datos (DBAs), administradores de sistemas operativos (root), aplicaciones e infraestructura
- Cuentas de administración local.
- Cuentas de emergencia.
- Cuentas de administrador de aplicaciones.
- Cuentas de administrador de máquina virtual.
- Cuentas de usuario que administren datos personales

Los usuarios privilegiados deberán cumplir con exigencias de tipo contractual con la Compañía, de forma tal que se garantice que cualquier posible daño malintencionado sobre los Activos de Información pueda ser cubierto jurídicamente. Adicionalmente deberán cumplir con lo siguiente

- Almacenar de forma segura las credenciales de usuario
- Mantener procedimientos de cambios de contraseña de forma periódica
- Evitar mantener ID de usuarios o contraseñas almacenados en scripts o procedimientos batch
- En la medida de lo posible, implementar mecanismos de doble autenticación.

La Compañía podrá implementar mecanismos fuertes de autenticación (Ej: tokens o sistemas de doble autenticación) en caso que lo considere necesario.

11.3.4 CONTROL DE ACCESO A LAS REDES DE LA COMPAÑÍA

- Los administradores de la red, deben garantizar que los usuarios solamente tengan acceso a los servicios y recursos que específicamente están autorizados a utilizar.
- El acceso a la red por parte de terceros debe realizarse en condiciones de seguridad y mediante procedimientos debidamente documentados.

11.3.5 CONTROL DE ACCESO A HERRAMIENTAS UTILITARIAS

- Se debe restringir y controlar estrictamente el uso de programas utilitarios y herramientas de acceso a bases de datos que puedan eventualmente superar los bloqueos y seguridades lógicas establecidas en los aplicativos, sistemas operacionales y diferentes controles implementados por la Compañía.

11.3.6 CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACION

- Se debe impedir el acceso a los usuarios de soporte tecnológico a la información administrada en los aplicativos
- Las actualizaciones no autorizadas sobre la información de las bases de datos (UDBU - *Unauthorized DataBase Update*) se encuentra prohibida. En caso de ser requerido, debe tramitarse una medida correctiva para los datos mediante la gestión de un Incidente de Seguridad

11.4. DISPOSITIVOS MOVILES

Los siguientes lineamientos aplican a los dispositivos móviles de tipo SmartPhone, Tablets, Phablets y similares. Otro tipo de dispositivos móviles será evaluado por la Dirección de Seguridad de acuerdo a la tarea que se vaya a realizar.

11.4.1 USO DE DISPOSITIVOS PERSONALES EN FUNCIONES DE LA COMPAÑÍA

- Los funcionarios que utilicen dispositivos móviles de su propiedad para ingresar a aplicativos o herramientas de software de la Compañía, deberán aplicar en todo momento las políticas y buenas prácticas de seguridad establecidas en el presente documento.

11.4.2 USO DE DISPOSITIVOS MÓVILES PROPIEDAD DE LA COMPAÑÍA

- Según las funciones relativas a cada cargo, la Compañía podrá suministrar dispositivos móviles a sus funcionarios.
- No está permitido almacenar o administrar en estos dispositivos información de carácter personal.
- El dispositivo contará con la aplicación que la Compañía disponga para la administración y control del mismo.
- El dispositivo contará con software antivirus actualizado.
- De forma previa a la entrega del dispositivo, el funcionario deberá cursar y aprobar la capacitación que la Dirección de Seguridad en la Información dispone sobre el tema.
- No está permitido la instalación de aplicaciones diferentes a las provistas por la Compañía, en caso de requerir aplicaciones adicionales se deberá realizar requerimiento a la Gerencia de Tecnología.

- Todas las aplicaciones serán descargadas desde los repositorios Oficiales del fabricante del sistema operativo, en caso de detectar anomalías por posible Jailbreak (ruptura del esquema de seguridad interno), la Compañía podrá aplicar el código de conducta.
- No está permitido realizar cambios en la configuración del sistema operativo del dispositivo, en caso de ser requerido, el funcionario deberá realizar la respectiva solicitud a la Gerencia de Tecnología quien evaluará la incidencia.
- Periódicamente por parte de la Gerencia de Tecnología se realizará Back Up al dispositivo por lo tanto el funcionario está en la obligación de mantener disponible el dispositivo en las fechas que se requiera, en caso de encontrar datos personales estos serán borrados y no serán parte del Back Up.
- La Gerencia de Tecnología realizará actualización de los dispositivos en cuanto a parches de seguridad sobre el sistema operativo y las aplicaciones, por lo tanto, el funcionario está en la obligación de mantener el dispositivo disponible en las fechas en que se requiera.
- Todos los dispositivos móviles estarán conectados en un segmento de red independiente cuando el funcionario se encuentre en la Compañía, en caso de estar fuera y requerir conectarse a la red corporativa esta conexión se realizará a través de una conexión VPN, en caso de requerir conectarse a una red externa el funcionario acepta conocer los riesgos que esto implica.
- Los siguientes sistemas operativos son aceptados por la compañía:

NOMBRE	VERSION	FABRICANTE
Android	6.0.1 o Superior	Google Android Open Source Project Open Handset Alliance
iOS	9.2.1 o Superior	Apple Inc.
Windows Phone	8.1.2 o Superior	Microsoft

- Respecto a otros Sistemas Operativos y dada su antigüedad se estudiará por parte de la Gerencia de Tecnología la viabilidad de permitir la conexión sobre el dispositivo.
- Para los dispositivos con sistema Operativo Android adicional al patrón de seguridad el dispositivo deberá contar con código de bloqueo PIN activo.
- Para los dispositivos con sistema Operativo IOS adicional al reconocimiento de Huella el dispositivo deberá contar con código de bloqueo PIN activo,
- En caso de pérdida o hurto del dispositivo el funcionario está en la obligación de informar la situación a la Coordinación de Seguridad de la Información y Ciberseguridad e instaurar la correspondiente denuncia ante la autoridad competente.

11.5. CIFRAMIENTO

Toda la información clasificada como Confidencial que sea transportada entre las oficinas de la Compañía o que sea intercambiada con terceros, deberá contar con mecanismos de Cifrado fuerte. En este sentido, se definen los siguientes

lineamientos:

Para terceros Contratados:

- Todo activo de Información entregado al proveedor deberá enviarse al tercero a través de un canal que implemente alguno de los protocolos seguros FTPS o SFTP, lo cual se acordará con el tercero al momento de su contratación.
- Todo tercero que tenga acceso a información Confidencial deberá suscribir el acuerdo de confidencialidad de la Compañía.
- La Compañía podrá requerir que la información que se encuentre en reposo deba ser Cifrada
- Todas las Contraseñas o claves necesarias para descifrar la información deberán ser comunicadas por un medio separado de los datos cifrados.

Para aplicaciones:

- En la medida en que sea posible, las aplicaciones Web públicas deberán contar con un certificado digital firmado por la Autoridad Certificadora, en ningún caso el certificado podrá ser auto firmado por el desarrollador sea este inhouse o un tercero contratado.
- Los ambientes de desarrollo y pruebas podrán tener certificados auto firmados, siempre y cuando cumplan los requisitos del RFC 6960.
- Las aplicaciones deberán contar con ciframiento de los datos en los campos de login, así mismo las ventanas que capturen datos con información confidencial deberán cifrar la información en el momento de la captura.
- Los Datos que viajen entre los componentes de la aplicación deberán contar con ciframiento en todo momento.

Los siguientes son algoritmos y protocolos de cifrado aceptados por la Compañía:

- RSA Con llave mínima de 2048 bits
- AES Con llave mínima de 256 bits
- SHA-2 o SHA-3 Con llave mínima de 256 bits
- SFTP
- FTPS
- HTTPS
- SSL Versión 3 o superior
- TLS Versión 1.1 o superior

11.6. DIVULGACION EN LA INFORMACION

El Numeral 3.4 de la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia define que las Entidades vigiladas deben cumplir como mínimo los parámetros allí consagrados, para lo cual se definen los siguientes mecanismos de divulgación de información:

- Previo a cualquier venta online sea esta realizada por un tercero o directamente por la Compañía se deberá informar al cliente las medidas de seguridad mínimas a tener en cuenta a través del canal en línea.
- En el portal web se publicarán periódicamente Tips de seguridad a fin de brindarle al cliente información que le permita adoptar prácticas seguras a través de este canal.
- Junto con la póliza de seguro se deberá entregar al cliente un documento de recomendaciones de seguridad en el cual se le informe la posibilidad de validar la autenticidad de su póliza.
- De manera permanente, se remitirá a todos los funcionarios Tips de seguridad a fin de brindarles herramientas para la adopción de buenas prácticas.
- En los casos de ventas Online se deberá generar registro de la operación en la cual se detalle lo siguiente:
    - Fecha y Hora (dd/mm/aaaa hh:mm).
    - Dirección IP desde la cual se efectúa la compra.
    - Numero de operación.
- En casos de pagos mediante tarjeta debito se debe ocultar los números a excepción de los últimos 4 dígitos, adicional en caso de pagos con tarjeta de crédito se deberá ocultar el N° de verificación.

11.7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE

La totalidad de los aplicativos adquiridos, contratados o desarrollados por la Compañía deben cumplir con los lineamientos establecidos en el Anexo No. 1 del presente documento “Requisitos Mínimos de Seguridad de la Información para Aplicativos”, Adicionalmente, los procesos de desarrollo de software deberán cumplir con lo siguiente:

- Mantener tres ambientes independientes, uno para el desarrollo de software, otro para la realización de pruebas y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no deberá influir en el desempeño de los otros dos
- Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.
- Se debe tener debidamente documentados y en operación los procedimientos de control de cambios

- Cuando sea requerido tomar copias de la información de clientes o cualquier información clasificada como Confidencial para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su protección y destrucción, una vez concluidas las mismas.
- Se deberá contar con procedimientos y controles para el paso de programas a producción, el objetivo será garantizar que el software que se encuentre en operación este catalogado.
- Se deberá implementar interfaces para los clientes o usuarios de los diferentes sistemas de la Compañía que cumplan con los criterios de seguridad y calidad de la información, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.
- La Gerencia de Tecnología deberá mantener documentada y actualizada, al menos la siguiente información:
    a) Parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones
    b) Versión de los programas y aplicativos en uso
    c) Soportes de las pruebas realizadas a los sistemas de información
    d) Procedimientos de instalación del software.
- De forma previa a la puesta en producción, los aplicativos nuevos debe superar satisfactoriamente las pruebas funcionales y de seguridad, para tal efecto debe contar con el visto bueno del área usuaria y de la Vicepresidencia de Riesgos.
- Los desarrollos de software contratados por medio de terceros, deben cumplir con los requerimientos de seguridad establecidos en el presente numeral.

11.8. SERVICIOS DE COMPUTACIÓN EN LA NUBE

Todos los servicios contratados por la Compañía en modalidad Cloud, deberán contar con un análisis de riesgo operativo y de seguridad, previo a la contratación de este. El informe de este análisis deberá ser remitido a la Superintendencia Financiera de Colombia, al menos quince días antes de su salida a producción. El mencionado informe deberá contener al menos lo siguiente:

- Nombre del proveedor y subcontratistas asociados a la prestación del servicio
- Relación de los procesos que serán manejados en la nube, incluyendo las aplicaciones, tipos de datos, productos y servicios asociados a estos.
- La ubicación física o región en donde se procesarán o almacenarán los datos
- Las certificaciones otorgadas al proveedor del servicio o sitio de procesamiento
- La relación de auditorías a las que se somete el proveedor de servicios contratado
- La información sobre los niveles de servicio establecidos
- El diagrama con la plataforma tecnológica que soportará los servicios contratados

No se podrán contratar terceros de servicios de computación en la nube que ofrezcan niveles de servicio inferiores al 99.95% de disponibilidad o que no tengan al menos una entre las certificaciones ISO 27001, ISO 27017, ISO 27018 o alguna norma equivalente.

Los servicios implementados por la Compañía en modalidades de SaaS, IaaS o PaaS deberán cumplir con los lineamientos establecidos en la Circular Externa 005 de 2017.

12. GESTION DE INCIDENTES DE SEGURIDAD

Con el objetivo de garantizar que la información relacionada con eventos de riesgo que afectan la CID de los Activos de Información sean gestionados adecuadamente, de forma tal que se pueda tomar acciones correctivas de forma oportuna, se establecen los siguientes lineamientos:

- Los incidentes de seguridad deben ser reportados a través de los canales establecidos por la Compañía para el registro de eventos de riesgo operativo (SARO), estableciendo claridad en que corresponden a eventos que afectan la CID de los Activos de Información.
- Las áreas responsables de los terceros contratados deben garantizar que todos sus funcionarios adopten el procedimiento de registro de eventos de riesgo operativo y por ende, de incidentes de seguridad.
- El área de Seguridad de la Información debe gestionar la atención rápida, efectiva y adecuada de los incidentes de seguridad.
- Los incidentes de seguridad que sean detectados y que por su *modus operandi* pueden afectar a la ciudadanía, deben ser reportados al Centro Cibernético Policial. En caso de que el estado colombiano, sea víctima de un ciberataque, la Compañía estará en disposición de apoyar las acciones requeridas por las autoridades competentes.
- La alta dirección es la única autorizada para dar información a externos respecto a un incidente de seguridad.

13. CONTINUIDAD DE NEGOCIO

La Compañía debe implementar un Plan de Continuidad de Negocio (PCN) con el objetivo de garantizar una adecuada respuesta, recuperación y minimización del impacto potencial de las fallas o desastres que afecten a los Activos de Información. El PCN debe estar coordinado por un equipo de manejo de crisis nombrado por la alta gerencia de la Compañía y deberá incluir planes para:

- Manejo de emergencias
- Continuidad de los procesos del negocio
- Plan de Recuperación de Desastres – (PRD)
- Plan de comunicaciones

El PCN deberá priorizar la continuidad de los procesos críticos de la Compañía, los cuales deberán ser determinados mediante la metodología de Análisis de Impacto de Negocio (AIN). El AIN y el PCN serán revisados y actualizados de forma anual o cuando se requiera por efectos de ajustes a los procesos de la Compañía.
La administración del PCN incluirá las siguientes responsabilidades:

- Gestión y actualización de la documentación relacionada con el PCN
- Coordinación de los procesos de capacitación y divulgación a usuarios
- Supervisión de la ejecución de las pruebas y la documentación de las mismas
- Coordinación de la documentación de los PCN y resultados de las pruebas a los mismos, realizadas por los terceros contratados por la Compañía

14. CUMPLIMIENTO

La Compañía deberá mantener una estrategia de cumplimiento enfocada a garantizar y sustentar adecuadamente la observancia de la normatividad legal vigente en materia de Seguridad de la Información, las disposiciones y obligaciones asociadas a la observancia de los contratos con terceras partes y garantizar que los terceros y personal externo que se cuentan con acceso a los Activos de Información de la Compañía cumplan con sus obligaciones contractuales, incluida la presente normativa.

Todas las áreas de la Compañía están en la obligación de tener en cuenta y documentar como parte de su plan de trabajo, el cumplimiento de las obligaciones en materia de Seguridad de la Información, los derechos de propiedad intelectual sobre materiales didácticos y publicitarios utilizados y el licenciamiento de software.

La Compañía adoptara medidas informativas orientadas a los consumidores financieros, con el fin de brindarles mecanismos de protección al momento de realizar operaciones a través de los canales de comercio electrónico.