Título Política de Seguridad de los Sistemas de Información de PGA Solutions y Filiales	**Número** 001
Unidad de Origen Seguridad de la Información y Continuidad de Negocio	**Fecha Emisión** 01.03.19
Ámbito de Aplicación PGA Solutions y Filiales de Brasil, Argentina, Perú, Colombia y México	**Entrada en vigor** 01.03.19
Resumen La presente política de seguridad de los sistemas de información es el marco de referencia de seguridad de los Sistemas de información para PGA Solutions y Filiales, estableciendo las directrices básicas para el tratamiento seguro de la información.	
Responsable Actualización Responsable Seguridad de la Información	**Fecha Actualización** 16.03.21
Certificación del documento Responsable Seguridad de la Información y Continuidad de Negocio	**Fecha de Revisión** 16.03.21

ÍNDICE

1 Introducción

1.1 Necesidad

El uso y la incorporación de las nuevas tecnologías de información ofrecen nuevas oportunidades, modelos de negocio y una serie de ventajas competitivas asociadas, permitiendo mejoras de eficiencia y de integración entre los diferentes sistemas de PGA Solutions y Filiales.

En este marco de nuevas tecnologías se hace necesario crear una Política de Seguridad de los Sistemas de Información con unas directrices homogéneas asociadas. El objetivo de estas directrices es la protección eficaz y eficiente, mediante un enfoque preventivo, detectivo, reactivo y dinámico de uno de los activos más valiosos para los procesos de negocio de PGA Solutions y Filiales: ***la Información***, para mantener su confidencialidad, integridad y disponibilidad.

La presente Política de Seguridad de los Sistemas de Información es el marco de referencia de seguridad de los Sistemas de Información para PGA Solutions y Filiales, estableciendo las directrices básicas para el tratamiento seguro de la información. Dichas directrices deben seguir los principios tradicionales de seguridad, a la vez que los expande y adapta para cubrir los nuevos riesgos asociados, entendiendo la seguridad y la protección de los Sistemas de Información como un proceso permanente en PGA Solutions y Filiales.

1.2 Objetivos. Compromiso de la Dirección

PGA Solutions y Filiales considera que la protección de sus activos, y con ella la sostenibilidad del negocio, debe ser uno de los compromisos más importantes de cara a nuestros clientes, accionistas y a la sociedad en general.

Bajo esta consideración, la Dirección de PGA Solutions y Filiales reconoce a la Información y los Sistemas que la sustentan y procesan como uno de sus activos más importantes a proteger, y establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos, garantizando un adecuado control interno de los mismos.

La Política de Seguridad constituye una declaración de la postura de la Dirección de PGA Solutions y Filiales con relación a la seguridad de los Sistemas de Información y establece los objetivos y las responsabilidades necesarias para proteger los activos de información gestionados, garantizando la integridad, disponibilidad y confidencialidad de los mismos, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

La Dirección de PGA Solutions y Filiales adquiere la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la integridad, disponibilidad y confidencialidad de la información, dentro de un marco general de gestión de riesgos de seguridad.

1.3 Alcance y ámbito de aplicación

El ámbito de la presente Política incluye a todas las Unidades, Áreas, Departamentos, empleados y personal subcontratado que acceden a los Sistemas de Información de PGA Solutions y Filiales, así como las empresas externas colaboradoras. La Política es de obligado cumplimiento para todos los Sistemas de Información de PGA Solutions y Filiales y/o que den soporte a sus procesos de negocio y afecta a todos los activos de información sustentados en ellos.

Asimismo, es una obligación legal y ética de PGA Solutions y Filiales garantizar, en los mismos términos, la seguridad de la información que concierne a sus clientes, entidades colaboradoras y a los organismos oficiales competentes.

2 Política y Directrices de Seguridad de los Sistemas de Información

Las directrices de la Política de Seguridad de PGA Solutions y Filiales han sido definidas de acuerdo con el estándar ***ISO/IEC 17799*** **/ 27001** que establece un marco de referencia de seguridad respaldado y reconocido internacionalmente. Este marco tecnológico, organizativo y procedimental de seguridad se soportará en un conjunto de Procesos, Normas, Estándares, Procedimientos y herramientas de seguridad para la protección de activos de información.

2.1 Mantenimiento y Difusión del Cuerpo Normativo de Seguridad de los Sistemas de Información

a) Se designará un propietario del Cuerpo Normativo, formado por Política, Normativas, Estándares y Procedimientos de Seguridad de Sistemas de Información, cuya responsabilidad sea la creación, revisión periódica, adecuación y alineamiento de su contenido con los planes estratégicos de PGA Solutions y Filiales.

b) La revisión formal de la presente Política se efectuará al menos una vez cada dos años. Adicionalmente se deberán considerar los cambios producidos en el marco legal vigente, la inclusión de resultados relevantes de auditorías o análisis de riesgos y las sugerencias de mejora al Cuerpo Normativo.

c) Se establecerá el procedimiento necesario para la divulgación del Cuerpo Normativo, con el objetivo de que sea conocido y aplicado por todos los usuarios dentro del ámbito de aplicación del presente documento, concienciándolos con relación a la seguridad de los Sistemas de Información.

2.2 Organización y Gestión de Seguridad

2.2.1 **Responsabilidad General**

a) La seguridad de los activos informáticos y de la información por ellos gestionada es responsabilidad de todas las Áreas de Negocio y Soporte, así como de todas y cada una de las personas asignadas a ellas.

b) Consecuentemente, todos los empleados de PGA Solutions y Filiales y aquellos terceros subcontratados, son copartícipes de dicha responsabilidad, debiendo trabajar, desde la posición que ocupen e independientemente de la responsabilidad que explícitamente se les asigne, hacia la consecución de una adecuada seguridad de la información.

c) Para ello, deberán conocer, asumir y cumplir la Política, Normativas y Procedimientos de seguridad vigentes, estando obligados a mantener el secreto profesional y la confidencialidad de los datos manejados en su entorno laboral y debiendo comunicar, con carácter de urgencia y según los procedimientos establecidos, las posibles incidencias o problemas de seguridad que se detecten.

d) El incumplimiento manifiesto de las normas de seguridad podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

e) Se formará adecuadamente al personal en los procedimientos de seguridad y el correcto uso de los Sistemas de Información para minimizar los posibles riesgos de seguridad.

f) Se evitarán las concentraciones de riesgos derivados de la ausencia de segregación de funciones y dependencia unipersonal de funciones críticas para el negocio. En caso de que no sea factible, se establecerán controles compensatorios.

2.2.2 **Responsabilidades Específicas**

a) Se establecerá una función específica de la protección de la información y gestión del fraude electrónico mediante la asignación de responsabilidades específicas en materia de definición, utilidad, uso y reporte de los controles de seguridad, por una parte, y de la implantación, operación y gestión de los mismos, de otra.

b) Dicha infraestructura organizativa estará liderada por un Comité de Seguridad y Protección de la Información Electrónica que, con la representatividad adecuada, supervise la gestión efectiva y eficiente de los riesgos e incidentes de seguridad, coordinando a los diferentes Departamentos que dentro de PGA Solutions y Filiales tienen responsabilidades específicas sobre la seguridad de los Sistemas de Información.

c) Este Comité se constituirá como Órgano responsable de establecer la estrategia, impulsar, priorizar, y efectuar el seguimiento de los Proyectos, Planes y Programas de Seguridad de los Sistemas de Información, coordinando y asegurando su adecuado soporte por las distintas Áreas responsables y adaptándose a las necesidades de las Unidades de Negocio para dar cumplimiento a los objetivos de seguridad establecidos por la Dirección e informar a ésta de su estado y evolución,

d) Se realizarán revisiones independientes de las vulnerabilidades existentes, riesgos asociados y controles establecidos.

e) Se establecerán controles organizativos y técnicos específicos para mantener la seguridad de los activos accedidos por terceros, y en los casos en que la responsabilidad del procesamiento de la información haya sido delegada en otra organización.

f) Se establecerán los mecanismos apropiados para la cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicaciones, así como organismos públicos o privados dedicados a promover la seguridad de los Sistemas de Información.

2.3 Clasificación y Control de Activos

a) Se mantendrá y actualizará de forma regular un inventario de los activos de información de PGA Solutions y Filiales, designándose para cada uno un responsable y, en su caso, custodio del mismo. Asimismo, deberán clasificarse los activos de información de acuerdo a su sensibilidad y criticidad para el negocio, en función de la cual se establecerá el nivel de seguridad exigido.

2.4 Seguridad Física y Ambiental

a) Los Sistemas de Información deberán ser emplazados en áreas seguras protegidas con controles de acceso físicos adecuados al nivel de criticidad de los mismos.

b) Los sistemas y la información que estos soportan deberán estar adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

2.5 Gestión de Sistemas, Operaciones y Comunicaciones

a) Se establecerán y documentarán procedimientos para la gestión y operación correcta y segura de los Sistemas de Información, incluyendo explícitamente procedimientos de respaldo de información, gestión de incidencias e incidentes. Para ello, se establecerán estándares de gestión y operación y se adoptarán las mejores prácticas en materia de seguridad, con el fin de asegurar la adecuada actualización, configuración y parametrización de seguridad de todos los Sistemas de Información de PGA Solutions y Filiales.

b) Se establecerán los mecanismos organizativos y tecnológicos necesarios para facilitar la monitorización continua, en la medida de lo posible, de los eventos de seguridad que acontezcan en los Sistemas de Información de PGA Solutions y Filiales.

c) Se establecerán las medidas necesarias para mantener los entornos de Desarrollo y Producción separados e independientes, tanto desde el punto de vista de los Sistemas de Información, como de los datos almacenados y procesados y del personal que accede a ellos, todo ello para mantener la seguridad de los datos reales de producción.

d) En el caso de servicios externalizados, se impondrán controles técnicos, organizativos y/o contractuales específicos que contemplen las directrices expuestas en esta Política.

e) Se establecerán sistemas y procedimientos de protección detectivos, preventivos y correctivos contra software malicioso, garantizando la actualización periódica y regular de los mismos.

f) Toda información que se transmita a través de redes de comunicaciones, públicas o privadas, deberá ser adecuadamente protegida mediante mecanismos de confidencialidad, autenticación, integridad, no repudio, control de tráfico y estrategias de segmentación y planificación de redes que tengan en cuenta los aspectos relativos a la seguridad de los datos y de los sistemas que los procesan. Los accesos realizados desde o a través de redes no controladas ni gestionadas directamente por PGA Solutions y Filiales deberán garantizar un nivel de seguridad equivalente o superior al de los accesos internos.

g) El almacenamiento, manipulación, transporte, destrucción o desecho de cualquier activo que soporte información de PGA Solutions y Filiales deberá garantizar la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado.

h) La actividad realizada sobre los activos de información de PGA Solutions y Filiales, relativa al procesamiento, almacenamiento o transmisión de información, deberá registrarse adecuadamente con el fin de poder realizar un seguimiento de la misma, de acuerdo a los requerimientos legales, de negocio y de investigación de incidentes.

2.6 Control de Accesos

a) Los permisos de acceso a las redes, sistemas y a la información que esos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

b) Cualquier concesión de acceso a los recursos de los Sistemas de Información de PGA Solutions y Filiales llevará asociado un proceso previo formal de perfilado funcional o alternativamente de petición, evaluación de la necesidad de acceso y aprobación.

c) Todos los empleados, personal externo o subcontratado, así como entidades colaboradoras y clientes que accedan a los Sistemas de Información de PGA Solutions y Filiales, deberán

registrarse y asociarse a un identificador personal e intransferible. Se evitará el empleo de usuarios genéricos, salvo en el caso de imposibilidad tecnológica, que deberá ser justificada, evaluada, documentada y aprobada formalmente, con la obligación de ser regularizada en el momento que ésta desaparezca.

d) Todos los accesos realizados a los Sistemas de Información de PGA Solutions y Filiales por los usuarios registrados llevarán asociado un proceso de identificación, autenticación de las credenciales de acceso y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas.

e) Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

f) Se establecerán normativas, procedimientos y medidas técnicas específicas para la protección de sistemas portátiles y accesos remotos de empleados o colaboradores.

2.7 Mantenimiento y Desarrollo de Sistemas

a) Se establecerán mecanismos para la inclusión de especificaciones relacionadas con seguridad de la información durante las fases de diseño, pruebas y aceptación, dentro del ciclo de vida de desarrollo de las aplicaciones de PGA Solutions y Filiales, así como para la autorización de nuevos sistemas de tratamiento de información y mecanismos de control de cambios que permitan realizar análisis de riesgos previos a la puesta en producción.

b) El desarrollo y mantenimiento de sistemas y aplicaciones deberá incluir los controles y registros apropiados que garanticen la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas de seguridad en la programación. Los controles criptográficos, uso y gestión de claves deberán ser objeto de consideración especial, requiriendo la participación directa de expertos en dichas áreas.

2.8 Gestión de Continuidad de Negocio

a) Se establecerá un proceso de gestión de continuidad de negocio para garantizar la recuperación de los procesos críticos para PGA Solutions y Filiales en caso de desastre, reduciendo el tiempo de indisponibilidad a niveles aceptables desde el punto de vista de negocio mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

b) La Gestión de la Continuidad de Negocio de PGA Solutions y Filiales se instrumentará en distintos Planes, con diferente alcance y ámbito de actuación.

El Plan de Continuidad de Negocio en PGA Solutions y Filiales posibilitará una respuesta uniforme y coordinada, en el plazo previsto, a cualquier interrupción de la actividad empresarial, a fin de conseguir la continuidad en el negocio, protegiendo al personal, la organización y los activos de nuestros clientes y accionistas.

El Plan de Continuidad de la Actividad corresponderá principalmente a un Centro, y garantizará la continuidad de las actividades críticas desarrolladas en el Centro, ante la posibilidad de que suceda una contingencia.

El Plan Global de Recuperación de Sistemas, inscrito dentro del marco de la Gestión de la Continuidad de Negocio de PGA Solutions y Filiales, establecerá las recomendaciones para el desarrollo de los Planes de Recuperación de Sistemas, como parte del Plan de Continuidad de la Actividad del Centro tratado.

En los Planes de Recuperación de Sistemas se evaluará el riesgo y el impacto ocasionado por un desastre en los sistemas y se planificará y ejecutará la recuperación de los mismos.

2.9 Cumplimiento Normativo

a) PGA Solutions y Filiales adquiere el compromiso de adaptar sus Sistemas de Información a la normativa legal vigente específica de cada país dónde se opere o tenga presencia, adoptando las medidas técnicas y organizativas necesarias, especialmente aquellas regulaciones legales relativas al tratamiento de los datos de carácter personal, registros contables, información privilegiada y la salvaguardia del secreto profesional y bancario.

b) Se incluirán cláusulas y garantías en los acuerdos de nivel de servicio con las empresas subcontratadas que garanticen los requerimientos de servicio y seguridad exigidos por PGA Solutions y Filiales, así como el cumplimiento de la normativa legal vigente.

c) Se desarrollarán e implantarán estructuras organizativas, procedimientos y herramientas específicas que permitan tanto un control interno global y continuado como una auditoría independiente de la idoneidad y cumplimiento de los controles que se deriven de la presente Política de Seguridad de los Sistemas de Información.

d) Se establecerán las medidas necesarias para evitar la desactivación, accidental o malintencionada, de los mecanismos de seguimiento y auditoría.