1 INTRODUCCIÓN

La Política de Seguridad de la Información y Ciberseguridad establece las responsabilidades, conductas y mejores prácticas que deben aplicarse en Alliance Enterprise, así como las directrices y los lineamientos para la administración y gestión segura de la información .

La Política de Seguridad de la Información y Ciberseguridad de Alliance Enterprise sigue las buenas prácticas definidas en los estándares NTC ISO-IEC 27001:2022, PCI-DSS y NIST, así mismo implementa infraestructura que le permita el aseguramiento de sus activos de información garantizando confidencialidad, disponibilidad e integridad. Por otra parte, las políticas redundan en posibles decisiones más ágiles y acertadas frente a los posibles riesgos que afecten la Seguridad de la Información, así como el manejo oportuno y efectivo de incidentes y/o situaciones adversas que pudieran afectar el normal funcionamiento de las operaciones.

2 OBJETIVOS

2.1 Objetivo General

Establecer los lineamientos y parámetros que permitan a Alliance Enterprise preservar la confidencialidad, integridad y disponibilidad de la información ingresada, procesada y generada en cada uno de los procesos de la organización, con el fin de que sea accedida sólo por personas autorizadas para la realización de funciones exclusivas del negocio (“Confidencialidad”); que su información se encuentre protegida contra modificaciones no planeadas, realizadas de forma accidental o intencionada (“Integridad”) y que esté en el momento y en el formato que se requiera ahora y en el futuro al igual que los recursos necesarios para su uso (“Disponibilidad”).

2.2 Objetivos Específicos

La Política de Seguridad de la Información y Ciberseguridad está orientada al cumplimiento de los siguientes objetivos específicos:

- Proteger los activos de información de Alliance Enterprise y sus clientes salvaguardando su confidencialidad, integridad y disponibilidad.
- Aumentar el nivel de disponibilidad, tolerancia a fallos y capacidad de escalamiento de los Servicios de Alliance Enterprise.
- Promover la mejora continua de los procesos del sistema de gestión de Seguridad de la información en pro de su eficacia y eficiencia.
- Proteger la imagen, los intereses y el buen nombre de Alliance Enterprise.
- Establecer roles, responsabilidades y obligaciones de seguridad de la información dentro de Alliance Enterprise.
- Asegurar que todos los colaboradores mantengan un nivel apropiado de concientización, conocimientos y habilidades necesarios que permitan minimizar la ocurrencia de incidentes de seguridad de la información y ciberseguridad.

- Asegurar que la Compañía esté en capacidad de continuar sus actividades principales de negocio, ante la ocurrencia de incidentes de seguridad de la información y ciberseguridad que puedan afectarla.
- Gestionar los riesgos asociados a seguridad de la información y ciberseguridad.
- Definir las directrices en el marco regulatorio y políticas vigentes.

3 ALCANCE

Aplica a todas las unidades de negocio y apoyo de Alliance Enterprise; y a los procesos realizados a través de terceros y proveedores.

Este alcance incluye a colaboradores, accionistas, clientes, terceros, proveedores, contratistas que como usuarios acceden a cualquier activo de información independiente de su ubicación. Adicionalmente, aplica a toda la información creada, procesada y respaldada que soporta al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre, incluyendo:

- Información almacenada en bases de datos.
- Información respaldada en centros de datos.
- Información almacenada en la nube (Google Drive).
- Información transmitida através de redes públicas o privadas.
- Información impresa, escrita, a mano, en papel, en tableros u otros medios.
- Información enviada por fax o por cualquier otro medio similar.
- Información grabada a través de los medios verificables.
- Documentos físicos (DF).
- Documentos digitales (DD).
- Mensajería Swift procesada en nuestra infraestructura.
- Computadores.
- Servidores.
- Dispositivos de almacenamiento masivo.
- Aplicativos informáticos (APP).

4 Terminología y Definiciones

Access Point: Dispositivo que interconecta dispositivos de comunicación para formar una red inalámbrica.

Activo de Información: Todo documento físico (DF), documento digital (DD) y aplicativos informáticos (APP) que tengan un valor para la empresa y/o soporten o sean parte de la actividad, proceso o giro de negocio de la compañía.

APP: Aplicativos Informáticos.

Aplicativo informático fuera de la custodia de la Unidad de Sistemas o TI (APPnoIT): Todo activo de información orientado al procesamiento y administración de datos que se encuentre administrado por una Unidad, y además se encuentre alojado

en la misma Unidad o en la Unidad de Sistemas. Se incluyen a esta definición los archivos digitales con lógica de programación en su contenido, como por ejemplo: macros en Excel, bases de datos en Access, flujos de trabajo en SharePoint, entre otros.

Aplicativo informático dentro de la custodia de la Unidad de Sistemas o TI (APPIT): Conjunto de programas desarrollados, instalados, administrados y/o actualizados por la Unidad de Sistemas para brindar atención a los clientes con productos o servicios automatizados, así como ofrecer el soporte necesario a toda la estructura administrativa, operativa y contable.

Autorización: Proceso por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información; el proceso determina cuáles actividades son permitidas, por ejemplo, manejo de datos o ejecución de programas.

Autenticación: Proceso mediante el cual el usuario se identifica como uno de los entes a los que se les ha otorgado derechos para ingresar al entorno computacional al que intenta ingresar. Este proceso establece la legitimidad del usuario.

BYOD: Bring your Own Device (BYOD), en castellano «trae tu propio dispositivo», es una política empresarial consistente en que los empleados lleven sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa tales como correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales. También se le conoce como «Bring your own technology» o «trae tu propia tecnología» en castellano, ya que de esta manera se expresa un fenómeno mucho más amplio ya que no sólo cubre al equipo sino que también cubre al software.

Cifrado: Mecanismo por el cual la información y/o datos es transformada de manera tal que sea incomprensible por parte de una personas o sistemas no autorizados.

Confidencialidad: Es proteger la información para que nadie pueda leerla o copiarla, sin autorización del dueño.

Control: Toda actividad o proceso encaminado a mitigar o evitar un riesgo, incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que puedan ser de carácter administrativo, tecnológico, físico o legal.

Crítico: Estado en el cual la pérdida de capacidad de procesamiento pueda llegar a tener consecuencias negativas significativas, desde los siguientes puntos de vista: continuidad del negocio, operacional y de integridad del personal.

Contraseña: Contraseña, password o clave de acceso es una combinación de letras, números y signos, que conoce y debe teclear el usuario para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.

Cuenta de Usuario: Es el identificador que utiliza un Sistema de Información en la autenticación de un usuario.

Custodios de la información: Se denominan así al personal o departamento que proporciona servicios informáticos de todo tipo. Los custodios no necesitan conocer la información para la realización de su trabajo, solamente procesarla, gestionar su almacenamiento y hacerla accesible.

DD: Documentos Digitales.

DF: Documentos Físicos.

Disponibilidad: Asegurar que la información y los servicios del negocio de la organización estén disponibles permanentemente y sean oportunos para los propósitos requeridos.

Dueño: Es la persona responsable de una aplicación que utiliza sistemas de información para proporcionar servicios que apoyan una o varias unidades de negocio. Es el responsable de velar por que se implementen controles que disminuyan el riesgo de la información a su cargo. Es también la persona que tiene la potestad de autorizar el acceso a la información.

Firewall: Es un filtro o cortafuegos (hardware o software) que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean permite o deniega su paso.

Gestión de Riesgos: Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos estratégicos de la Compañía.

Incidente de Seguridad: es cualquier evento desfavorable que amenaza la seguridad de los sistemas de información o la infraestructura que los soporta, y en general todo aquel evento que atente contra la integridad, disponibilidad y confidencialidad de los activos de información. Ejemplos de incidentes incluyen ataques de denegación de servicio, ejecución de código malicioso, acceso no autorizado a recursos, pérdida de datos, divulgación no autorizada etc.

Información Confidencial: Información de uso exclusivo de una persona o grupo de personas externas o internas, que en caso de ser divulgada sin autorización afecta los intereses de la compañía y de los clientes (saldo cuentas, información del cliente guardada por el Banco manual o sistematizada, etc.).

Información Reservada: Información de uso exclusivo de algunos funcionarios de la alta gerencia, la cual en caso de ser divulgada afecta los intereses institucionales (PIN, Clave, proyectos, etc.).

Información Privada: Información de uso exclusivo de una persona o de la entidad o que administra el banco (listados de cartera, listado saldos).

Información Sensible: Información que por su naturaleza, debe mantenerse bajo medidas de seguridad que garanticen el acceso solo al personal autorizado y para el propósito definido. La información en medio magnético, bases de datos, archivos e impresa, que maneje Información Reservada, Confidencial o Privada es clasificada como Sensible.

Información, Clasificación de Datos: La información se clasifica en 3 categorías, Sensible, Interna y Pública.

Información Interna: Es aquella información de uso de los funcionarios de Grupo con el objeto de realizar la operación normal del negocio. Son ejemplos, las políticas, normas, procedimientos y estándares.

Información Pública: Es aquella que se ha hecho disponible para la distribución pública a través de los canales autorizados de la compañía. Son ejemplos, los boletines de servicios, folletos y anuncios.

Integridad de datos: Proteger y garantizar la exactitud e integridad de la información en el momento de su ingreso a los sistemas y la identificación de cualquier alteración de la información.

Evidencia Digital: Es un tipo de evidencia física que puede tomar muchas formas como son: Registros de aplicaciones, sistema operacional, comunicaciones (logs de transacciones, logs de seguridad, logs de intentos de login fallidos,etc.)

- Imágenes o gráficas
- Documentos en todos los formatos
- Correo Electrónico Y Faxes
- Información Financiera Y Transacciones
- Archivos De caché, cookies
- Archivos eliminados
- Archivos de intercambio

Nivel de seguridad estándar: Nivel de seguridad que restringe a los usuarios la ejecución de algunos comandos o el acceso a algunos archivos basados en permisos y en niveles de acceso. Este nivel de seguridad requiere de auditoría del sistema. Esto incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema.

Riesgo Informático: Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control, y la severidad del impacto adverso resultante. Reduciendo la amenaza o la vulnerabilidad reduce el riesgo.

Seguridad: la información se deberá tratar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta indebida, uso o acceso no autorizado o fraudulento.

Sensitiva: Información que, por su naturaleza, debe mantenerse bajo medidas de seguridad que garanticen el acceso solo al personal autorizado y para el propósito definido.

Sistema: Este término utilizado sin otra palabra que lo designa un conjunto de hardware y software específico.

Software: Creación intelectual que comprende los programas, los procedimientos, las reglas y cualquier documentación asociada pertinente a la operación de un sistema de procesamiento de datos.

Terceros: Personas o empresas diferentes a la compañía y empresas que prestan servicios al mismo. Ejemplo: Clientes, Clientes potenciales, Empresas candidatas a prestar servicios a la compañía.

Transferencia: Mecanismo por el cual se transfiere información de datos personales al responsable y/o encargados del tratamiento de los datos, este puede estar dentro o fuera del país.

Usuario: Persona que usa un sistema o aplicativo. Credencial con contraseña asignada a aquella persona, empleados de las empresas del Grupo y personal de empresas que prestan servicios al mismo para poder acceder a cualquier sistema de información. Es personal e intransferible.

Usuario de la información: Es aquella persona, empleado interno o personal externo, que introduce, borra, cambia o lee la información almacenada en nuestros sistemas informáticos. Para adquirir perfil como usuario es necesaria previa autorización por el dueño del sistema, ya sea de modo individualizado o de forma general (información disponible para todo el personal de un área, etc.).

Vulnerabilidad: Debilidad de un sistema, que da posibilidad de realizar alguna acción que afecte negativamente a éste.

5 PRINCIPIOS Y POLÍTICAS GENERALES

- La gestión de Seguridad de la Información y Ciberseguridad está enmarcada en el lineamiento de Seguridad de la Información y Ciberseguridad definido por Alliance Enterprise y en el cumplimiento del marco regulatorio y requerimientos de los clientes y de las entidades de vigilancia y control.
- La información es uno de los principales activos de Alliance Enterprise y por lo tanto debe ser utilizada de acuerdo con los requerimientos del negocio y los niveles de seguridad definidos por la organización.
- La Gestión de Seguridad de la Información y Ciberseguridad tienen como objetivo preservar y mantener las propiedades de confidencialidad, integridad, disponibilidad de la información.

- La información de Alliance Enterprise y de sus clientes debe mantenerse bajo el criterio de integridad independientemente de su residencia temporal o permanente, o de la forma en que sea transmitida.
- Toda la información de Alliance Enterprise es de su propiedad, independiente del medio en la que ésta se encuentre y por lo tanto debe ser protegida de modificación, eliminación y conocimiento por personas ajenas a la organización o de su utilización para un fin distinto al que le ha sido asignado. Incluso la información que se transmite por voz, cuyo medio de transmisión es el aire, debe ser protegida manteniendo su integridad, confidencialidad y disponibilidad.
- Alliance Enterprise deberá mantener un gobierno de Seguridad de la Información y Ciberseguridad de acuerdo con el tamaño y la complejidad de las operaciones, considerando todos los activos de información física y lógica que se encuentran dentro y fuera de la custodia de sistemas.
- La gestión de Seguridad de la Información y Ciberseguridad en Alliance Enterprise incluye a los empleados, proveedores y terceros; por tanto, se debe asegurar el entendimiento de las responsabilidades para su adecuada gestión, manteniendo disponibles y actualizadas las políticas, procesos y estándares de seguridad de la información.
- Todos los colaboradores son responsables de la adecuada gestión de la información y de proteger los activos de información según su clasificación, siguiendo los lineamientos de Seguridad de la Información y Ciberseguridad dispuestos en la presente política.
- Las Gerencias de las Unidades, o los líderes usuarios que han sido designados como dueños de los activos de información, son los responsables de asegurar la adecuada gestión de acuerdo con los principios y políticas de Seguridad de la Información y Ciberseguridad.

6 POLÍTICA DE USO ACEPTABLE ACTIVOS DE INFORMACIÓN

- Los sistemas de información de ALLIANCE ENTERPRISE, deben utilizarse únicamente con fines relacionados con el cargo y funciones asignadas a cada colaborador, contratista, proveedor y/o tercero. Los sistemas de información no se deben usar con fines personales o particulares.
- Los activos de información de ALLIANCE ENTERPRISE, sólo deben ser utilizados por el personal debidamente autorizado.
- Compartir, divulgar, transferir o acceder a la información dentro y fuera de ALLIANCE ENTERPRISE, se debe realizar de acuerdo con el nivel de clasificación asignada a la información, lo cual debe cumplir con lo establecido en el **Procedimiento de Clasificación y Etiquetado de Activos de Información**.
- Los usuarios que accedan o usen aplicaciones o software de terceros deben cumplir con los derechos de propiedad intelectual y no instalarán software o aplicaciones que no sean autorizadas y debidamente licenciadas.
- Los programas y recursos utilizados en ALLIANCE ENTERPRISE deben tener su correspondiente licencia vigente o autorización de uso explícita.
- Todos los aplicativos o sistemas de información de ALLIANCE ENTERPRISE deben tener asignado un “propietario” el cual será el responsable de definir

controles, perfiles de acceso a la información, así como los usuarios y privilegios que cada uno deba tener sobre ella.

- Los usuarios de los sistemas de información deben cumplir con todas las directivas de uso y las relativas a la seguridad de la información definidas por ALLIANCE ENTERPRISE.
- Cada usuario será individualmente responsable por el manejo adecuado de las claves de acceso o contraseñas asignadas.
- ALLIANCE ENTERPRISE se reserva el derecho a intervenir, monitorear y auditar los accesos realizados por los usuarios a los sistemas de información, así como al contenido accedido.
- El acceso a información o el uso de cuentas de usuarios no asignadas, está prohibida y está sujeto a las medidas disciplinarias y legales aplicables.
- Al realizar sesiones virtuales en donde se requiera grabar, se debe cumplir con la regulación aplicable para la protección de datos personales y esta debe tener la autorización expresa de los integrantes de la sesión. Estas no podrán ser usadas con fines personales o particulares.
- Los sistemas de comunicación y el acceso a internet que tengan los colaboradores, proveedores y terceros de ALLIANCE ENTERPRISE por medio de los equipos designados por la empresa, deben ser utilizados exclusivamente como una herramienta de trabajo y no para actividades personales.
- Todo el contenido que se realice a través de los canales de comunicación de ALLIANCE ENTERPRISE podrá ser objeto de restricciones y controlar su contenido.
- El sistema de correo electrónico corporativo (@ALLIANCEENTERPRISE.com) es parte integral de sus Sistemas de Información, por lo que ALLIANCE ENTERPRISE puede intervenir, auditar e investigar el uso adecuado del mismo. Las cuentas están sujetas a auditorías y revisiones sin previo aviso por el personal autorizado del Área Técnica y el área de Seguridad de la Información o por parte del personal designado por el Comité Estratégico.
- Los activos de información, de acuerdo a lo definido en la presente política, son propiedad de ALLIANCE ENTERPRISE, por tal razón, su alteración, destrucción o distribución fraudulenta o malintencionada, puede generarle graves perjuicios legales y disciplinarios; en tal caso se podrán adoptar las medidas que se consideren necesarias, reservándose el derecho a interponer las acciones legales pertinentes.
- Ante el conocimiento de la violación de alguna de estas normas, se debe reportar el caso de acuerdo a lo establecido en el **Plan De Respuesta Incidentes de Seguridad y Ciberseguridad**.
- Las normas aquí establecidas deben interpretarse como complementarias a las normas legales aplicables para el resguardo y tratamiento de la información y la manipulación de equipos tecnológicos y sistemas de información.
- Todas las actividades de administración y operación que se realicen en los activos de información deben ser orientadas a garantizar el correcto funcionamiento de las operaciones.
- Todos los colaboradores deben reportar al área de Seguridad de la Información cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información.

- Todos los colaboradores deben aplicar los controles de seguridad que permitan reducir los riesgos de seguridad de la información mitigando las vulnerabilidades y amenazas identificadas.
- Los colaboradores no deben instalar ningún programa o software desarrollado por ALLIANCE ENTERPRISE en los equipos o estaciones de trabajo fuera de la misma.
- Ningún colaborador debe compartir usuarios y contraseñas de los sistemas de información.
- Está prohibido realizar cambios a los activos de información, sin contar con la autorización formal del responsable del área o del proceso en el que esté el activo.
- Está prohibido utilizar los activos de información de la Compañía para fines diferentes al cumplimiento de las funciones asignadas y el cumplimiento de la misión de la misma.
- Cuando no hay un propósito laboral legítimo, el colaborador no podrá utilizar los sistemas de información de la Compañía para ver, recibir o almacenar materiales inadecuados, ofensivos, vulgares o ilegales o para transmitir comunicaciones abusivas, de hostigamiento, amenazantes, difamatorias o engañosas.
- No está permitido cambiar, alterar, modificar de ninguna forma el hardware o el software de los sistemas de información de ALLIANCE ENTERPRISE.
- Los activos de información de la Compañía deben usarse única y exclusivamente para el propósito para el que fueron asignados.
- Los activos de información no deben ser usados por terceros ajenos a los procesos de la compañía, por lo que los colaboradores deben garantizar el adecuado uso de acuerdo con la **Política De Teletrabajo.**
- La infraestructura de escritorio virtual o VDI debe ser únicamente para uso laboral y no deberá ser accedida desde equipos personales o redes públicas o de terceros. El acceso a estos recursos es responsabilidad del usuario.
- El uso de la información de la compañía debe ser controlado para prevenirla de accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido.

7 GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

7.1 Directorio Ejecutivo

El Directorio Ejecutivo es responsable de la aprobación de la disponibilidad de los recursos necesarios del Sistema de Gestión de Seguridad de la Información - SGSI, así como la revisión y aprobación de los lineamientos y políticas generales para la Alliance Enterprise, adicionalmente tendrá los siguiente responsabilidades:

- Asegurar que se establezcan la política y los objetivos estratégicos de calidad y Seguridad de la Información para el Sistema de Gestión Integrado de la empresa. Y que éstos sean compatibles con el contexto y la dirección estratégica de la organización;

- Asegurar la integración de los requisitos del sistema de gestión integrado en los procesos de la organización;
- Promover el uso del enfoque a procesos y el pensamiento basado en riesgos
- Comunicar la importancia de una gestión de Calidad y Seguridad eficaz y conforme con los requisitos del sistema de gestión Integrado;
- Asegurar que el Sistema de Gestión Integrado logre los resultados previstos
- Compromete, dirige y apoya a las personas, para contribuir a la eficacia del sistema de la empresa;
- Promover la mejora.
- Asegurar que la integridad del sistema se mantiene cuando se planifican e implementan los cambios en la empresa.
- Definir la planeación estratégica de la empresa (Definir el marco general de la empresa, objetivos, misión, visión y las estrategias o actividades para su logro) el análisis interno y externo de la empresa y generar planes de acción a implementar para su seguimiento y control.
- Establecer, implementar y realizar seguimiento a la Política y Objetivos de la empresa.
- Asegurar la disponibilidad de recursos necesarios por proyectos o por proceso y para la funcionalidad de la empresa estén disponibles;
- Tomar decisiones frente a los procesos de los cuales son responsables.
- Analizar datos de desempeño de la empresa (indicadores de gestión) a su cargo y tomar acciones para el mejoramiento.
- Asegurar que el personal a su cargo está ejecutando las labores definidas utilizando los recursos, infraestructura y registros definidos.
- Realizar seguimiento financiero, administrativo y operativo de la empresa.
- Participar en las reuniones directivas para la mejora de la empresa.
- Realizar el seguimiento por lo menos una vez al año de los elementos de entrada establecidos en el numeral 9.3 Revisión por la Dirección así como los elementos de salida derivados de las decisiones relacionadas con las oportunidades de mejora y cambios en el sistema de gestión integrado.

Pronunciarse sobre el perfil de riesgos operativos y de Seguridad de la información y evaluar la factibilidad económica de los planes de acción establecidos por los Líderes de procesos.

7.2 Dirección de Riesgos y Control:

Son responsabilidades de la Dirección de Riesgos y Control:

- Informar al comité de riesgos y seguridad de la información, sobre el cumplimiento de la política y aspectos principales de los riesgos de operación relacionados a seguridad de la información y ciberseguridad de la compañía según el nivel de exposición.
- Presentar para aprobación las actualizaciones presentadas sobre la presente política al Directorio Ejecutivo.

7.3 Gerencia de Seguridad de la Información:

Son responsabilidades de la Gerencia de Seguridad de la Información:

- Asegurar la implementación, verificación y cumplimiento de la política, proponer mejoras y definir los mecanismos necesarios para lograrlo, mediante el alineamiento a las directrices y políticas de la compañía y de los organismos de control en caso que apliquen.
- Definir los controles y actividades a aplicar para mitigar los riesgos de seguridad de la información y ciberseguridad a los que está expuesta la organización, asesorando a los usuarios sobre su implementación, siguiendo las metodologías definidas.
- Desarrollar y ejecutar el proceso de validación y monitoreo del cumplimiento de los controles de seguridad de la información y ciberseguridad, identificando las oportunidades de mejora y definiendo planes de acción correctivos y/o preventivos en coordinación con las unidades evaluadas.
- Planificar y realizar la capacitación anual de concientización de seguridad de la información y ciberseguridad para todos los colaboradores de la organización.
- Atender, coordinar y resolver consultas de los clientes y las entidades reguladoras (si aplican), proveedores y/o consultores especializados en temas relacionados a la seguridad de la información y ciberseguridad de la organización.
- Coordinar y/o realizar el monitoreo de los recursos informáticos para verificar el cumplimiento de los controles y las políticas adoptadas, así como el cumplimiento de los requerimientos de negocio.
- Coordinar la gestión de incidentes relacionados con seguridad de la información y ciberseguridad notificados por las partes interesadas.
- Para la evaluación de los riesgos de seguridad de la información y ciberseguridad, será responsable de definir la metodología de evaluación de riesgos la cual debe estar alineada al modelo de riesgos de la compañía.
- Establecer en coordinación con los dueños de los activos de información, los procesos y/o controles necesarios para mitigar los riesgos de seguridad de la información, con el fin de lograr un entorno seguro para los activos de información.
- Coordinar la realización de pruebas de penetración, con el fin de detectar vulnerabilidades y debilidades que puedan presentarse. Así mismo coordinar y hacer seguimiento a los planes de acción para el cierre de los hallazgos que se lleguen a encontrar.
- Realizar capacitación y sensibilización en seguridad de la información y ciberseguridad.

7.4 Comité de Riesgos y Seguridad de la Información

Tiene como responsabilidad dirigir, evaluar y realizar seguimiento a la estrategia, programa y planes enfocados en gestionar la Seguridad de la Información.
.

- El Comité es el responsable de analizar y evaluar el impacto de los eventos relevantes relacionados con seguridad de la información y ciberseguridad, y podrá establecer o proponer planes de acción para su mitigación.
- Pronunciarse y proponer procesos, y controles necesarios para la mitigación de los riesgos de Seguridad de la Información y Ciberseguridad.
- Realizar seguimiento al plan de trabajo anual, a la ejecución de los planes de acción y al cumplimiento de las métricas de Seguridad TI y no TI definidas de acuerdo con los lineamientos de la compañía.
- Pronunciarse sobre los informes generados por las auditorías de los clientes y de las posibles revisiones de los entes de control sobre la gestión de seguridad de la información y ciberseguridad en Alliance Enterprise.
- Analizar los nuevos lineamientos que deban proponerse para aprobación del Comité de Alta Dirección; que pudieran derivarse de cambios significativos en el perfil de riesgo según el criterio de materialidad, nueva regulación, eventos relevantes, nuevos riesgos, cambios en ambiente de negocios, entre otros.

El Comité deberá estar conformado mínimo por el área de Riesgos y Seguridad de la Información.

Las sesiones del Comité serán anuales y con mayor periodicidad en caso de que el Comité decida.

Es responsabilidad de la Dirección de Riesgos y Control, el desarrollo y gestión del Comité de Riesgos y Seguridad de la Información.

7.5 Gerente de Riesgos y Procesos

Es responsable de apoyar en el desarrollo, custodia, mantenimiento y actualización de la política para la gestión de riesgos, velando por la oportunidad en la incorporación de mejoras, lineamientos corporativos y cambios regulatorios.

Es el responsable de:

- Acompañar al Director de Riesgos y Control y Gerente de Seguridad de la Información en los cambios y actualizaciones de la política con el fin de ajustarla a los lineamientos y directrices de la compañía y de los organismos de control que apliquen.
- Apoyar a la presentación de los cambios en la política ante el Comité de Alta Dirección para su aprobación.
- Apoyar al Gerente de Seguridad de la Información en las metodologías de identificación, clasificación y evaluación de riesgos relacionados con seguridad de la información y ciberseguridad.

7.6 Oficiales de Seguridad

El rol de oficial de seguridad, también es responsable de proteger los activos de información del impacto de los posibles riesgos y cumplimiento de políticas, para dirigir el desafío de mantener la seguridad y ciberseguridad, apoyando el cumplimiento del principio de segregación de funciones; menor privilegio y 4 eyes, en los diferentes productos o servicios de la compañía que tengan habilitada dicha opción.

El rol debe ser establecido entre dos funcionarios de distintas áreas no dependientes jerárquicamente dentro de la organización y en la medida que el proceso lo permita, usar herramientas para establecer un flujo de aprobación o clave compartida para las operaciones críticas en materia de seguridad.

El rol puede estar conformado por integrantes de:

- La Gerencia del área dueña de la información.
- La Gerencia de Seguridad de la Información.

Con el objeto de contar con respaldo de las funciones durante las ausencias del funcionario asignado a cada rol, debe establecerse unos funcionarios de respaldo para cada uno dentro de sus mismas áreas. Los funcionarios de respaldo deben estar capacitados y tienen las mismas responsabilidades que los oficiales principales durante el desempeño de sus funciones.

Entre sus funciones principales están:

- Gestionar la entrega de nuevas cuentas de usuario
- Parametrizar las restricciones de seguridad definidas en esta política
- Licenciar software que requiera este rol
- Aprobar los flujos de ruteo de la información
- Configurar parámetros de seguridad
- Monitorear los logs de eventos con el fin de detectar incidentes de seguridad
- Verificar que la información está asegurada en los diferentes sistemas en cuanto a confidencialidad, integridad y disponibilidad

7.7 Proveedores y/o Terceros

Los proveedores y/o terceros de servicios deben acatar y cumplir las políticas de seguridad de la información que establezca la Compañía y tienen la responsabilidad de mantener y asegurar los activos, información o recursos a los que tengan acceso, para ello debe implementar los mecanismos necesarios para asegurar la información de la Compañía y de sus clientes.

7.8 Clientes

Los clientes que tengan acceso a los recursos de Alliance Enterprise deben cumplir las políticas de seguridad y mantener seguros los recursos, así como tendrán la responsabilidad de informar cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los activos de información.

7.9 Colaboradores de Alliance Enterprise

Los colaboradores son los responsables de proteger los activos de información de la compañía a través del cumplimiento de la política de seguridad de la información y ciberseguridad. Así mismo, deben reportar cualquier incumplimiento de normas o procesos establecidos que pongan en riesgo la información.

Los colaboradores que tengan el rol de Dueño de Activo de Información, son responsables de definir el valor y la criticidad de la información que se custodia, procesa o transporta a través del activo de información; con base en esta, definir los privilegios de su uso y generar los mecanismos para garantizar las condiciones mínimas de seguridad y mitigación de los riesgos asociados a los mismos.

Alliance Enterprise podrá definir otros roles y responsabilidades adicionales que apoyen al adecuado desarrollo de esta política, propendiendo siempre por la segregación de tareas como método para reducir los riesgos en el uso de la información.

Los clientes que tengan acceso a los recursos de Alliance Enterprise deben cumplir las políticas de seguridad y mantendrá segura los recursos, así como tendrá la responsabilidad de informar cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los activos de información.

7.10 Cumplimiento de la Política

La política de seguridad de la información y ciberseguridad es de obligatorio cumplimiento. Cada colaborador debe entender y asumir su responsabilidad respecto a la administración de la información y de los activos que la soportan.

Cualquier incumplimiento de esta política que resulte comprometiendo la confidencialidad, integridad y disponibilidad de la información podrá generar una sanción disciplinaria de acuerdo a lo establecido en el contrato laboral, el reglamento interno de trabajo y el **Código de Ética y Conducta** respectivamente.

La política de seguridad de la información y ciberseguridad en Alliance Enterprise considera buenas prácticas definidas en ISO/IEC 27001, PCI-DSS y NIST por tanto tomará las medidas aplicables para garantizar su cumplimiento, sin embargo, el contenido de este documento, es lo que ha definido la empresa.

7.11 Mecanismos de seguridad de los sistemas en Alliance Enterprise

Identificación y Autenticación Individual: Todos los colaboradores que accedan a información de la compañía deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal.

Control y Administración del Acceso a la Información: El uso de la información de la compañía debe ser controlado para prevenirla de accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido.

Administración y Uso de Contraseñas: Alliance Enterprise, deberá mantener mecanismos adecuados para asegurar el uso de contraseñas que se ajusten a las mejores prácticas, con el fin de garantizar al mayor nivel posible, la existencia de un control de acceso robusto. Ver **Política de Password**.

7.12 Habeas Data Alliance Enterprise

Alliance Enterprise, buscando garantizar la protección de derechos fundamentales de las personas y específicamente la intimidad, el buen nombre, la autonomía y la imagen, se regirá en sus actuaciones por los mandatos consagrados en la ley de protección Hábeas Data, teniendo como principios rectores la buena fe, la legalidad, la autodeterminación informática, la libertad y transparencia.
Que en cualquier caso y bajo el desarrollo de las actividades propias, sean estas permanentes u ocasionales, Alliance Enterprise será quien actúe como responsable del tratamiento de datos, teniendo la facultad de conocer, actualizar y rectificar la información allí registrada bajo el marco legal definido por la Constitución política, artículo 15, Ley 1266 de 2008, Ley 1581 de 2012, Decreto 1377 de 2013.

7.13 Política de Seguridad de Recursos Humanos

a. Se deben establecer responsabilidades de seguridad de la información en todo el ciclo de vida laboral o contrato para todos los empleados, contratistas, terceros, practicantes y usuarios de terceras partes. De acuerdo con las necesidades del negocio, se debe aplicar una verificación de antecedentes antes de conceder el acceso a los recursos de información o las instalaciones de la Compañía.
b. Los empleados y usuarios de terceras partes serán informados acerca de las Políticas de Seguridad de la Información de la Compañía y las acciones a tomar en caso de incumplimiento de la misma.
c. El responsable de la seguridad de la información realizará planes de concientización a los empleados, tanto al ingreso como a lo largo de su relación laboral.
d. La desvinculación o cambio de cargo de un empleado debe ser gestionada y controlada apropiadamente de tal manera que los activos de información que le fueron asignados sean devueltos en las mejores condiciones y que la información a la que tenga acceso se entregue o se disponga de acuerdo con la necesidad del líder de área.

8 Directrices Estratégicas

8.1 Seguridad de la información

Directriz: La información del negocio es un activo vital de Alliance Enterprise y por lo tanto debe ser protegida. La información de la organización, sin importar la presentación, medio o formato, en la que sea creada o utilizada, se califica como medio de información del negocio o activo de información.

La seguridad de la información y ciberseguridad, se logra implementando un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y recursos tecnológicos.

Alliance Enterprise debe disponer de los medios necesarios para asegurarse de que cada colaborador preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, sobrepasar

cualquier control de seguridad o ciberseguridad mediante actos como: realizar copias no autorizadas o exportar sin autorización material de la compañía tal como software, manuales, fuentes, información técnica, información de clientes; introducir código malicioso o programas malicioso en la red; intentar tener accesos no autorizados a datos de la compañía o de otros empleados mediante el uso de sniffers, spoofing o cualquier otro monitoreo de red o de infraestructura; escanear puertos o realizar escaneos de seguridad sin la debida autorización de la Gerencia de Seguridad de la Información; violaciones contra la propiedad intelectual de la compañía; proveer información sobre los empleados de la compañía a terceras partes, Estará sujeta a la aplicación de sanciones o medidas disciplinarias.

8.2 Ciberseguridad

Directriz: Se deben proteger los activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

Alliance Enterprise busca proteger su información ante los peligros actuales y constantes mediante la prevención que le permita registrar el comportamiento de los sistemas de información para actuar de manera temprana ante cualquier amenaza que pueda comprometer la confidencialidad, integridad, disponibilidad y privacidad de la información y las medidas a tomar para su correspondiente mitigación. Es por esto que adopta medidas para la mitigación de riesgos internos y los relacionados con el ciberespacio

8.3 Activos de información

Directriz: Los activos de información deben estar ubicados en lugares que los protejan de daños causados por desastres naturales, daños en instalaciones físicas o incidentes de seguridad o ciberseguridad, garantizando su confidencialidad, integridad, disponibilidad y privacidad independiente del medio en que se encuentren. Estos activos deben ser valorados y clasificados de acuerdo a su criticidad e impacto.

Se debe prever que los activos de información, se encuentren localizados en áreas seguras y debidamente protegidos contra amenazas que puedan afectar su buen uso, disponibilidad y confidencialidad. Los controles o medidas que se implementen deben estar acorde con la valoración de la información y los riesgos asociados. Para tal fin, se debe contar con una metodología que permita tener una matriz de activos de información debidamente valorada, de tal forma que se defina el aseguramiento de los mismos de acuerdo a su clasificación. La actualización de esta matriz se debe realizar, preferiblemente una vez al año (ver metodología en el **Instructivo para Gestión de Activos de Información).**

La valoración de los activos de información se encuentra alineada al nivel de exposición de riesgos de seguridad de la información y ciberseguridad, y por ende los tiempos de cierre para los planes de acción resultado de las debilidades u oportunidades de mejora de los controles están alineados a los definidos en la metodología de riesgo de la empresa.

TABLA DE EQUIVALENCIA DE VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN VS. NIVEL DE EXPOSICIÓN DEL RIESGO		
Valoración del Activo de Información	*Criticidad del Riesgo*	*Tiempo para el Cierre de Planes de Acción.*
Restringido	*Muy Alto / Critico*	*Máximo: 3 Meses para el cierre de los planes.*
Privado	*Alto*	*Máximo: 6 Meses para el cierre de los planes.*
Público	*Bajo*	*Máximo: 9 Meses para el cierre de los planes.*

8.4 Clasificación de la Información

Directriz: La información de Alliance Enterprise, debe ser clasificada de acuerdo a los criterios de confidencialidad, integridad y disponibilidad. Esta clasificación debe ser revisada periódicamente por los dueños de los activos de información.
La información debe ser clasificada de acuerdo con el valor que ésta le aporta a la compañía en los distintos estados de su ciclo de vida. Esto permitirá asociar los recursos que generen un mayor desempeño, seguridad y disponibilidad al momento en el que la información sea más sensible para la compañía.
La información por su sensibilidad debe ser catalogada de acuerdo a la clasificación de activos de información:

Tipo 1. Información Pública: Es clasificada como tal, si en el caso de que dicha información no estuviera disponible, el resultado no generaría ningún efecto, además, la divulgación o no de esta información no causa ningún tipo de pérdida económica, impacto legal, ni de imagen para la compañía.
Tipo 2. Información de Uso Interno: Es clasificada como tal, si en el caso de que dicha información se filtrara fuera de la compañía, el resultado generaría pérdidas económicas no significativas. El acceso a esta información es provisto únicamente a personal de la compañía o trabajadores externos autorizados, de tal modo, que ellos puedan consultarla libremente.
Tipo 3. Información Confidencial: Es clasificada como tal, si en el caso que dicha información se filtra fuera de la compañía, el resultado generaría importantes pérdidas económicas, impacto legal y de imagen institucional. La divulgación de dicha información requiere la aprobación del Dueño. Así mismo, en caso que la información requiera ser divulgada a terceros o proveedores se requerirá un acuerdo de confidencialidad firmado.

Los dueños de los activos de información son los responsables de clasificar todos sus activos de información aplicando la metodología definida a través del“Inventario de Activos de Información” que permite identificarlos y aplicar los controles de acuerdo a su clasificación según su contenido.

Algunos de los controles ejecutados para garantizar la integridad, confidencialidad y disponibilidad de los activos de información son:

- Permisos de acceso y modificación limitados

- Ejecución de copias de respaldo
- Conexiones de acceso limitadas a direcciones IP
- Cifrado de Información
- Control periódico de revisión de reglas de firewall
- Evaluación y gestión de vulnerabilidades
- Ejecución de Hacking Ético y Pruebas de penetración
- Servidores de salto a la zona segura
- Alertas de modificaciones o cambios sobre los sistemas de información a través del correlacionador de eventos
- Configuración de servicios en alta disponibilidad
- Monitoreo de la gestión de la capacidad
- Replicaciones de ambientes virtualizados
- Control periódico de aplicación de parches de seguridad
- Monitoreo sincronización Carbonite
- Contención de ataques mediante IPS
- Custodia de cuentas de altos privilegios
- Monitoreo cruzado de los enlaces de comunicaciones
- Replicación Base de datos entre ambientes (Producción y Contingencia)
- Hardening a nivel de sistema y sistemas de información
- Monitoreo vigencia certificados
- Control de accesos físicos(Datacenter producción y contingencia)
- Restricción de acceso a internet
- Segregación de funciones (Matrices de roles y perfiles – Control de acceso lógico)
- Cumplimiento principio 4 eyes
- Nivel de encriptación VPN site to site
- Control Antivirus
- Bloqueo dispositivos almacenamiento extraíble
- Sensibilización en seguridad de la información y ciberseguridad.

8.5 Gestión de Riesgos de Seguridad de la Información y Ciberseguridad

Directriz: Alliance Enterprise debe contar con una gestión efectiva de los riesgos de seguridad de la información y ciberseguridad, que apoye al logro de la estrategia corporativa, con el objetivo de identificar oportunidades para el fortalecimiento de los controles de los procesos y del negocio.

Se debe contar con una metodología para la gestión de riesgos de seguridad de la información y ciberseguridad la cual debe estar alineada con la gestión de riesgo de la empresa.

Se debe coordinar la solución de los planes de acción asociados a aquellos riesgos según su perfil, teniendo en cuenta el nivel actual de exposición del riesgo o su impacto causado. Por lo anterior se debe seguir en lo posible, el cumplimiento del cierre en los tiempos de solución según la siguiente prioridad:

- Nivel de Criticidad Crítico: Máximo 3 meses

- Nivel de Criticidad Alto: Máximo 6 meses

- Nivel de Criticidad Bajo: Máximo 9 meses

8.6 Gestión de Incidentes de Seguridad de la Información y Ciberseguridad

Directriz: Dar a conocer los lineamientos generales definidos por la Gerencia de Seguridad de la Información y aprobada por el comité de Riesgo y Seguridad de la Información, para el manejo de los posibles incidentes de seguridad de la información y ciberseguridad que puedan presentarse al interior de Alliance Enterprise.

Alliance Enterprise, gestionará un incidente desde el momento anterior a su ocurrencia, hasta la forma en cómo se debe aprender y obtener la experiencia para eventos futuros de acuerdo a los siguientes pasos:

- Preparación
- Detección
- Contención
- Erradicación
- Recuperación
- Seguimiento

Todos los incidentes de seguridad de la información son registrados acorde al plan de respuesta a incidentes de seguridad de la información y ciberseguridad.

8.7 Calidad de la información.

Directriz: La información de Alliance Enterprise, debe cumplir con los siguientes criterios de calidad.

Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

8.8 Capacitación y sensibilización sobre la seguridad de la Información y ciberseguridad.

Directriz: Alliance Enterprise debe desarrollar programas anuales o cada vez que se requiera, de capacitación y sensibilización sobre la seguridad de la información y ciberseguridad. Adicionalmente se debe publicar esta política por el medio que se considere adecuado y se debe informar al personal a través de las capacitaciones anuales.

El nuevo personal al momento de vincularse, debe recibir capacitación sobre seguridad de la información y ciberseguridad, quedando como evidencia la evaluación que mide la eficacia de la capacitación, a través de la herramienta de Classroom.

Para el desarrollo de los programas de capacitación y sensibilización deberán asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades con respecto a la seguridad de la información y ciberseguridad.

8.9 Control de acceso y requerimientos mínimos para los sistemas informáticos

8.9.1 Identificación y autenticación individual

Directriz: Todos los colaboradores que accedan a cualquier sistema informático de la Compañía deben disponer de un usuario y clave, los cuales son de uso personal e intransferible. Así mismo, todo sistema informático debe ser diseñado, desarrollado e implementado teniendo como referencia los requerimientos mínimos para proteger la seguridad de la información, tales como: claves de acceso, restricción de acceso, segregación de funciones y logs de auditoría. Estas condiciones deben conservarse a lo largo de su vida útil.

Cada colaborador es responsable por los accesos, consultas y cualquier tipo de novedad que se realice con los usuarios que tiene asignados, tales como: creaciones, modificaciones, y eliminaciones.

La creación, configuración y uso de los usuarios genéricos por usuarios finales están prohibidos. Cuando las condiciones de la operación lo requieran deben ser autorizados por el Gerente o Director del área usuaria con el visto bueno de la Dirección de Riesgos y Control. Para estos casos se deben firmar actas de responsabilidad por los colaboradores que compartirán el usuario.

La presente directriz abarca el uso de dispositivos de autenticación como tokens (hardware –software) y smartcards, las cuales son de uso personal e intransferible. Es responsabilidad del colaborador mantener los dispositivos en lugares que garanticen su uso personal e integridad.

Una vez cumplida la vigencia de los dispositivos, cambio de funciones del colaborador, o al momento de retiro del colaborador de la Compañía, estos deberán ser entregados a la Gerencia de Seguridad de la Información. Una vez cumplida la vigencia de los dispositivos de autenticación, estos deben ser destruidos.

8.9.2 Control y administración del acceso a la información

Directriz: La información de la Compañía debe ser protegida para prevenir los accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a los temas estrictamente requeridos.

Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el negocio y con la valoración de los riesgos asociados.

Los accesos no deben comprometer la segregación de tareas y responsabilidades. El acceso a la información de la compañía debe ser otorgado basado en lo que es

requerido para realizar las actividades relacionadas con su función y bajo las premisas de menor privilegio.

8.9.3 Administración de cuentas de Usuarios

Directriz: Se debe utilizar un estándar en la creación de las cuentas de usuario de los empleados en todos los sistemas informáticos utilizados en Alliance Enterprise, de forma tal que exista uniformidad y facilidad de identificación de los empleados.

Todos los usuarios que se creen en aplicaciones internas y externas para uso de los colaboradores de la compañía deben cumplir con los siguientes esquemas de creación:

SWIFT:
- Se antepone el %BIC4% seguido de la primera letra del nombre y el primer apellido.

Alliensoft:
- Se antepone el %BIC4_% seguido de la primera letra del nombre y el primer apellido.

Correo:

- %primer_nombre.%%primer_apellido% @allianceenterprise.com

Sistema Operativo (Administradores):
- Se antepone el ADMINSB. Seguido la primera letra del nombre y el primer apellido.

Sistema Operativo (Otros usuarios)
- Se antepone el SBXA. seguido la primera letra del nombre y el primer apellido.

Las demás:
- Deben llevar la primera letra del nombre y el primer apellido.

Excepciones:
- En caso que se llegue a repetir, se utilizará la primera letra del primer y segundo nombre y el primer apellido. En caso que se repita nuevamente se utilizará lo anterior y adicionalmente la primera letra del segundo apellido.

- En el caso de aplicativos externos en donde no se tiene el control de la aplicación, el ID del usuario no cumplirá estos parámetros.

8.9.4 Requerimientos mínimos de seguridad de los sistemas informáticos

Directriz: La Gerencia de Seguridad de la Información será responsable de los módulos de seguridad de los diferentes sistemas informáticos de Alliance Enterprise; guardando independencia entre la operatividad y la administración de estos módulos.

Las claves que se administran de forma centralizada deben cumplir con la política en cuanto a:

- Complejidad
- Longitud
- Vigencia
- Historial

Los sistemas informáticos deben cumplir con los parámetros establecidos en la Política de Password.

a. Referente al módulo de seguridad

Los sistemas informáticos deben cumplir con los siguientes parámetros:

1. Los sistemas deben proporcionar mecanismos para autenticación de usuarios a través de interfaz gráfica.
2. Permitir la parametrización y creación de diferentes perfiles de usuario.
3. Permitir la asignación de perfiles a usuarios que garanticen una adecuada segregación de funciones.
4. Ser independiente tanto en el acceso como en la administración a los demás módulos de administración o parametrización.
5. No se debe contratar o montar sistemas de información que tengan claves quemadas en código.
6. Las contraseñas almacenadas por el sistema deben ser cifradas.
7. Las contraseñas no deben ser mostradas en texto legible en pantalla.

b. Referente a los log de auditoría

Los sistemas informáticos deben contar con log que permitan:

1. Registrar, monitorear y auditar las acciones realizadas por los usuarios como:
   - Fecha y hora de eventos realizados, descripción de evento y usuario.
   - Acciones de usuario de creación, eliminación y modificación de datos en interfaces gráficas.
   - Eventos de inicio y finalización de sesión, intentos fallidos de ingreso a los sistemas.
2. Preservar la integridad de los registros y estar disponibles cuando requieran ser consultados.
3. Ser de uso exclusivo de las áreas de Seguridad de la Información, Plataforma Tecnológica y la Dirección de Riesgo y Control.
4. Los logs de eventos del sistema deben almacenar un histórico por lo menos 30 días como mínimo.
5. Logs de aplicaciones que registran acciones de usuario de servicios productivos, se deben almacenar por 2 años de acuerdo con la circular externa 042 de 2012 de la SFC.
6. Los logs de SWIFT, de acuerdo al requisito del Shared Infrastructure Programme para los Service Bureaus, serán almacenados por 1 año.

El histórico de los logs es almacenado en el Correlacionador de eventos – SIEM, por un año.

Excepciones: Pueden existir aplicativos que por sus limitaciones en parámetros de seguridad no permitan cumplir con alguno de los lineamientos expuestos anteriormente.

8.9.5 Administración y uso de contraseñas por parte de los usuarios

Directriz: Todos los colaboradores de Alliance Enterprise deben definir claves de acceso a los sistemas informáticos que cumplan con las condiciones de complejidad que dificulten su conocimiento por personal no autorizado. Adicionalmente, deben protegerlas para garantizar su confidencialidad y uso personal.

Las contraseñas de acceso a los sistemas informáticos que definen los usuarios deben cumplir con los parámetros establecidos en la **Política de Password**.

Se recomienda en la medida que técnicamente sea posible la implementación de la autenticación multifactor la cual proporciona una capa adicional de protección contra los ataques de autenticación más comunes (por ejemplo, la navegación de hombro, la reutilización de contraseñas, o contraseñas débiles) y proporciona una mayor protección contra el compromiso de cuentas para el procesamiento de transacciones maliciosas. Los atacantes suelen utilizar los privilegios de una cuenta comprometida para moverse lateralmente dentro de un entorno y progresar en un ataque.

NOTA: Esta información se da a conocer en las capacitaciones de seguridad de la información. Los detalles de este capítulo incluyendo lo referente a los mecanismos de doble factor de autenticación están disponibles en la **Política de Password.**

8.9.6 Administración y monitoreo de usuarios de altos privilegios

Directriz: Los usuarios con altos privilegios en servidores, bases de datos y aplicaciones deben estar identificados y se guarda registro de las actividades que realicen, a través de logs de auditoría. Los usuarios primarios de los sistemas que permitan la definición de usuarios nombrados con menores privilegios para la ejecución de actividades de administración, deben ser custodiados de forma segura en una herramienta para la administración de claves. Así mismo, los usuarios que acceden directamente a las bases de datos por sus funcionalidades no se pueden incluir dentro de los parámetros de contraseña ya que afectan la ejecución de procesos y tareas de las aplicaciones.

Los usuarios primarios son aquellos que traen preestablecidos los sistemas, que permiten realizar la configuración de tareas de administración. Deben utilizarse para tareas especiales que no se pueden ejecutar con el usuario asignado al Administrador, Gerente o Analista de Seguridad de la Información. No deberán ser utilizados para tareas rutinarias o periódicas del sistema o aplicación a no ser que la aplicación así lo requiera y por ningún motivo se podrán utilizar para:

- Actualización de Sistema operativo o aplicaciones.
- Asignación de autorizaciones especiales a un usuario.
- Configuración de dispositivos o parámetros de la aplicación.

La asignación de la contraseña tendrá los siguientes lineamientos. La contraseña de los súper-usuarios está constituida por lo menos por 17 caracteres alfanuméricos y caracteres especiales; las contraseñas asignadas por cada colaborador deberán cumplir con las normas de la presente política para la asignación de contraseñas. Se deben custodiar usando una herramienta para almacenar y administrar contraseñas.

Excepciones: Pueden existir usuarios de altos privilegios de los servidores, bases de datos, aplicaciones y equipos de comunicaciones que no pueden cumplir con la norma de asignación de contraseñas, debido a que tienen ligados procesos o tareas automáticas.

8.9.7 Criptografía

Directriz: Todos los flujos de datos entre aplicaciones están protegidos mediante el uso de mecanismos seguros para soportar la confidencialidad, integridad y autenticación mutua de dichos flujos. Los flujos de datos internos se protegen contra divulgación, modificación y acceso no intencional de los datos mientras se encuentren en tránsito.

Los algoritmos criptográficos aprobados por Alliance Enterprise para su uso están descritos en el **Procedimiento de Criptografía**.:

Las claves criptográficas deben estar disponibles operativamente tanto tiempo como lo requiera el servicio criptográfico correspondiente.

Nota: Los computadores de los cargos críticos, es decir, personal de las áreas de Administración de Servicios, Soporte, Plataforma Tecnológica y Seguridad de la Información, que cuenten con acceso a la zona segura, deberán contar con cifrado de discos en sus equipos portátiles de propósito general.

8.9.8 BYOD (Del Inglés traiga su propio dispositivo)

Directriz: Los colaboradores que por sus labores requieren tener acceso a los recursos de información de la compañía a través de sus dispositivos personales, deben aceptar las políticas y controles que se establezcan con el fin de proteger los activos de información a los cuales acceden. Solo se permite el uso de dispositivos móviles tales como Smartphones para recibir las alertas generadas por la herramienta de monitoreo en horarios no operativos, generación de doble factor de autenticación. De ser necesaria la revisión de correo corporativo, en estos dispositivos, debe tener instalada la aplicación DLP corporativa, la cual cuenta con controles como:

- Evitar captura de pantalla
- Generación de perfil de trabajo

Estos dispositivos no pueden estar conectados en la misma red a la que pertenecen los equipos de la organización.

La información que puede visualizar el empleado a través de su dispositivo móvil, es confidencial y de uso exclusivo para el desarrollo de sus funciones dentro de la compañía.

Los siguientes son requerimientos mínimos de seguridad que deben ser configurados en los dispositivos que hagan uso de este servicio:

a. Inclusión de PIN: Requisito indispensable para la visualización del correo, suele utilizar la función de seguridad propia de los Smartphones y establece un bloqueo automático por inactividad.
b. Será responsabilidad de todos los colaboradores, dar aviso a la Dirección de Plataforma Tecnológica sobre la pérdida o hurto de su dispositivo, para realizar el cambio de contraseña del correo. En los casos de retiro del funcionario se debe inactivar el correo.
c. Mecanismos de autenticación: Los colaboradores que utilicen su Smartphone tendrán que tener por lo menos alguno de los siguientes mecanismos de autenticación: Reconocimiento facial, acceso biométrico, clave o patrón.

A continuación, se exponen algunas recomendaciones que deben ser tenidas en cuenta para el uso de dispositivos personales:

- Instalar antivirus en los dispositivos.
- Actualizar la versión del sistema operativo del dispositivo.
- Evitar la adulteración del sistema operativo.
- Realizar siempre conexiones a redes inalámbricas seguras.
- Cifrar la información del dispositivo.
- Habilitar el sistema de borrado remoto de información de los dispositivos móviles en caso de pérdida.

Es responsabilidad del colaborador hacer buen uso de la información de la organización que reposa en su dispositivo personal y debe cumplir con acuerdos contractuales y políticas de seguridad de la organización. El incumplimiento acarrearía sanciones disciplinarias y legales.

8.9.9 Acceso a Red Inalámbrica

Directriz: Los equipos de cómputo, que hagan uso del servicio de red inalámbrica, deben tener en cuenta las siguientes recomendaciones:

- Estar protegida con mecanismos seguros como WPA/WPA2
- No se debe utilizar redes Wi-Fi abiertas o que usen mecanismos inseguros de encriptación como el WEP.
- Se recomienda cambiar la contraseña que trae por defecto los dispositivos routers (módems) o extensores inalámbricos
- No utilizar redes Wi –Fi públicas.

Nota: Ver **Política de Teletrabajo** para mayor información.

8.9.10 Acceso remoto

Directriz: El acceso remoto a los activos de información para los colaboradores y personal externo (proveedores, clientes), se dará cumpliendo con lo definido para cada

uno de los casos, siempre contando con la autorización de acceso descrita en la presente política.

Se deben establecer procesos que identifiquen la permanencia y uso del acceso remoto, el cual debe estar sujeto a las condiciones de seguridad en la presente política.
Es responsabilidad de los colaboradores de Alliance Enterprise y personal externo (proveedores, clientes) al que le sea otorgado este acceso, hacer buen uso de este recurso, velando por los principios de seguridad de la información. Los perfiles de acceso remoto serán definidos de acuerdo a las funciones del colaborador y las necesidades del proveedor o cliente identificando claramente los activos de información que por sus funciones o servicios prestados deben acceder. Para el caso de personal externo debe ir aprobada el Director de Riesgos y Control y el Gerente de Seguridad de la Información. Adicionalmente, para los usuarios externos (proveedores, Clientes) que hagan uso de este servicio deben tener firmada una cláusula de confidencialidad que garantice la protección de la información.

Las conexiones remotas por defecto deben estar restringidas y únicamente se deben permitir los accesos a personal autorizado y por periodos de tiempo establecidos a través de una conexión VPN con doble factor de autenticación y con mecanismos de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de la información. Los usuarios una vez establecen su conexión VPN acceden a escritorios virtuales los cuales se encuentran hardenizados para que puedan acceder a los recursos autorizados de acuerdo a su rol. Los usuarios relacionados directamente con la operación de los clientes y requieran conexión hacia la zona segura, deberán conectarse adicional al escritorio virtual al servidor de salto con doble factor de autenticación.

Responsabilidades de los colaboradores:

- Contar con las aprobaciones requeridas para establecer conexión remota y acatar las condiciones de uso establecidas para dichas conexiones.
- Establecer la conexión en un entorno seguro. Abstenerse de realizarlo en sitios públicos como café internet.
- Asegurar que la conexión a internet sea de confianza y con mecanismos mínimos de seguridad. No conectarse a redes abiertas.
- Establecer conexiones remotas en computadoras asignadas por Alliance Enterprise.. Bajo ninguna circunstancia, en computadores públicos, hoteles o cafés internet, entre otros.
- Garantizar la seguridad física del equipo utilizado para establecer las conexiones. Ejemplo: No dejarlo a la vista de personas que puedan manipularlo, resguardarlo o custodiarlo cuando no se esté utilizando.
- No dejar desatendida la estación cuando se tenga establecida una conexión remota.
- Dar aviso al grupo de Plataforma Tecnológica o Seguridad de la Información de cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

Nota: Ver **Política de Teletrabajo** para mayor información.

6.9.11 Servidor de Salto

Directriz: Con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, los usuarios relacionados con las operaciones de los clientes que requieran gestionar los servicios productivos, deberán conectarse a través de un servidor de salto. Este servidor deberá contar con un proceso de hardening y al menos los siguientes controles:

- Conexión por medio de doble factor de autenticación.
- No se podrán compartir archivos desde el servidor de salto a la estación del operador.
- No se podrán capturar pantallas (Print Screen)
- La función de copiar y pegar solo estará disponible dentro del servidor mas no para copiar y pegar fuera de él.
- Este servidor no podrá contar con salida a internet.
- No se podrá ejecutar líneas de comando, modificación de registros.
- El panel de control deberá estar bloqueado.
- Los servidores destino deberán contar con los agentes de correlacionador de eventos con el fin de establecer el origen de las conexiones, por tanto, las IP 's del servidor de salto deberán estar monitoreadas a través del SIEM.
- Este servidor deberá escanearse a nivel de antivirus preferiblemente de forma diaria totalmente.
- Bloqueo automático a los 15 minutos.

8.10 Bloqueo de dispositivos de almacenamiento masivo

Directriz: Con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, el uso de dispositivos de almacenamiento masivo, sólo serán permitidos para apoyar las actividades propias del negocio que ameriten su utilización bajo la autorización del líder del proceso y el del Gerente de Seguridad de la Información. Es responsabilidad de los colaboradores limitar el uso de estos medios.

Nota: La excepción para la habilitar los medios de almacenamiento, solo se realizará de forma temporal de acuerdo a lo definido en el formato Solicitud Autorización Uso de Medios Extraíbles.

8.11 Uso adecuado del Internet

Directriz: Los empleados de Alliance Enterprise no pueden usar los sistemas informáticos o equipos de la compañía para descargar material desde Internet el cual se considere inapropiado, ofensivo, ilegal o que pueda atentar contra la seguridad de la información.

El uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando para todos los casos, los siguientes lineamientos que no están permitidos:

- El acceso a las siguientes categorías las cuales se consideran inapropiadas, o que van en contra de la ética moral, leyes vigentes o políticas aquí establecidas:

    - Categoría Adulta.
    - Categoría Juegos.
    - Categoría de Alcohol y Tabaco.
    - Categoría de Engaño y Plagio.
    - Categoría de Pornografía.
    - Categoría de Pornografía infantil.
    - Categoría de Cultos.
    - Categoría de Citas.
    - Categoría de Apuestas.
    - Categoría de Hacking.
    - Categoría de Discriminación.
    - Categoría de Actividades ilegales.
    - Categoría de Drogas ilegales.

- Categoría para el almacenamiento a través de la nube

  Nota: Debido a que Alliance Enterprise cuenta con almacenamiento en la nube a través de la plataforma Google WorkSpace , el único almacenamiento autorizado es Google Drive Corporativo.
- El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, que tengan como objetivo intercambiar información o fines diferentes a las actividades propias del negocio.

  Nota: Debido a que Alliance Enterprise cuenta con la plataforma Google WorkSpac, se permite la utilización de Google chat como herramienta de mensajería interna.
- La descarga, intercambio y/o instalación de juegos, música, películas, o archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica, entre otros.
- Cada uno de los usuarios, es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente y/o los lineamientos de seguridad de la información de Alliance Enterprise.
- Los colaboradores y/o terceros (proveedores, clientes), al igual que las empresas de outsourcing, no pueden asumir en nombre de Alliance Enterprise, posiciones personales en encuestas de opinión, foros u otros accesos web similares.

Alliance Enterprise debe definir categorías de acceso para las áreas que lo requieran con la autorización del Gerente o Director, y que vayan acordes con los procesos que gestionan, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información. Cualquier cambio o excepción deberá estar soportado y con las aprobaciones respectivas. Ver **Procedimiento de Restricción de Acceso a Internet.**

8.12 Uso adecuado del correo electrónico corporativo

Directriz: Las cuentas de correo electrónico son personales y de uso exclusivo para el desarrollo de funciones del negocio, por lo tanto, la información gestionada a través de este medio es responsabilidad de cada usuario y debe cumplir con las condiciones de confidencialidad, integridad y disponibilidad reglamentadas en esta política.

La utilización del correo electrónico corporativo para asuntos diferentes a los relacionados con el negocio puede afectar la seguridad de la información. Algunos ejemplos de eventos de riesgo relacionados son:

- Fuga de información.
- Proliferación de virus de computador.
- Pérdida de la confidencialidad de la información.

No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico.
- Enviar mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Utilizar la dirección de correo electrónico de Alliance Enterprise como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, entre otras, o cualquier otro sitio no relacionado con actividades laborales.
- Enviar archivos con las siguientes extensiones no permitidas tales como música, vídeos, ejecutables, etc. (ade, adp, bat, chm, cmd, com, cpl, exe, hta, ins, isp, jar, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc,wsf, wsh).

El correo electrónico corporativo no debe usarse para actividades que comprometan la reputación de la compañía, los activos de información y los recursos de Alliance Enterprise.

Alliance Enterprise deberá implementar mecanismos que le permitan monitorear el uso adecuado del correo electrónico corporativo, con el fin de asegurar la disponibilidad de los recursos y mantener la confidencialidad de la información.

8.13 Escritorios limpios

Directriz: No deben dejarse desprotegidos documentos con información confidencial o sensible. Se debe garantizar su adecuada custodia de tal manera que se aseguren las condiciones de confidencialidad, integridad y disponibilidad de la información.

Durante la jornada laboral, todos los empleados deben tener en cuenta las siguientes recomendaciones:

- Evitar dejar información sensible a disposición de personas no autorizadas
- Guardar bajo llave documentación que a su criterio sea importante, confidencial o secreta.
- Evitar dejar en lugares visibles y fácilmente accesibles CDs, USBs o cualquier otro tipo de dispositivo de almacenamiento de información.
- Bloquear su estación de trabajo al momento de ausentarse de su puesto de trabajo.
- No dejar encima del escritorio documentos que contengan: Nombre de usuario y contraseña; Contratos con información a terceros; Números de Cuentas Corrientes; Y listado con datos de funcionarios.

Al finalizar la jornada laboral, todos los empleados deben:

- Dejar bloqueada su estación de trabajo.
- Ordenar su escritorio de forma que no quede información sensible expuesta, no debe quedar ningún documento encima del puesto de trabajo.
- Guardar bajo llave la información sensible y cerrar con llave cajones y archivadores.
- Al concluir una reunión o ausentarse de los puestos de trabajo, los colaboradores de Alliance Enterprise deben revisar que no se esté dejando al alcance de otras personas información confidencial, cuya pérdida o divulgación no autorizada pueda afectar el desarrollo de la operación normal o generar riesgos legales con partes interesadas.

- Evitar el uso de fotocopias o cualquier otro medio de reproducción no autorizado por Alliance Enterprise; cámaras, escáner, entre otros.

8.14 Escritorios de computadores

Directriz: Los escritorios de los computadores deberán contar con los iconos mínimos requeridos para el acceso a los aplicativos. Se debe evitar dejar en los escritorios, información confidencial o privada de fácil acceso. La adopción de esta medida, adicionalmente fortalece el orden y el respaldo adecuado de la información.

8.15 Envío, intercambio y entrega de información a terceros

Directriz: El envío, intercambio y entrega de información confidencial tanto al interior como a terceros, se debe hacer bajo condiciones de seguridad, la información debe entregarse a través de un medio seguro o protegido garantizando su destino y el propósito de su uso.

Toda la información suministrada a terceros, debe entregarse habiendo surtido los procesos de autorización respectiva y establecido un acuerdo de confidencialidad de la información.

Toda la información debe entregarse a través de un medio seguro o protegido, con el fin de evitar la pérdida de su confidencialidad e integridad y para aquellos casos que lo permitan, la información entregada debe estar despersonalizada.

- Para el envío de información confidencial por medio electrónico se enviará en formato PDF o un archivo comprimido .7ZIP con clave, la cual será por defecto el número de identificación del tercero a quien se le envié la información.
- Los funcionarios no deben enviar correos electrónicos con información sensible de las partes externas sin haber pasado por aprobación por parte de la Dirección General requerida y la Gerencia de Seguridad de la Información.
- Los terceros deben cumplir con las políticas de seguridad de la información y ciberseguridad, que tengan algún tipo de relación con la transferencia de información en medios físicos.

Nota: Ver Procedimiento Transferencia y/o Intercambio de Información.

8.16 Uso de Programas Utilitarios Privilegiados

Directriz: Se debe restringir, y si es requerido por labores de la operación, controlar el uso de software capaz de sobrepasar o anular los controles normales de seguridad.

Se deben usar procedimientos robustos de control de acceso para la identificación, autenticación y autorización de los programas de utilidad privilegiada.

La utilización de programas utilitarios de altos privilegios debe estar aprobada por la Gerencia de Seguridad de la Información y deben ser registrados en la **Bitácora de Programas Utilitarios Privilegiados.**

8.17 Uso de software autorizado

Directriz: Todo el software utilizado por Alliance Enterprise debe ser instalado y configurado por el personal autorizado por la Dirección de Plataforma Tecnológica.

La instalación y configuración de software debe cumplir con la aprobación del Gerente del área usuaria previo análisis de la Dirección de Plataforma Tecnológica, y en caso de dudas de la Gerencia de Seguridad de la Información

Nota: Se debe garantizar la validación de fuentes y de integridad de las descargas de software. Antes de instalar el software, se debe validar la legitimidad de la fuente y efectuar verificaciones de integridad (por ejemplo, mediante un checksum) cuando sea técnicamente posible.

8.18 Continuidad y disponibilidad de la información

Directriz: Los activos críticos de información y los procesos asociados, deben contar con estrategias enfocadas en preservar su disponibilidad.

La información debe estar disponible para su uso cuando la Compañía lo requiera. Por lo tanto, Alliance Enterprise deberá desarrollar, un programa de Gestión de Continuidad del Negocio que permita identificar los procesos vitales de la compañía, definir estrategias y planes de respuesta, así como implementar y probar periódicamente procesos para asegurar su recuperación razonable y oportuna,

buscando mantener los niveles de seguridad establecidos. La Gestión de Continuidad del Negocio es liderada por la Dirección de Riesgos y Control.

Los registros físicos y electrónicos de Alliance Enterprise deben ser conservados un mínimo de años de acuerdo con la regulación vigente y aquellos que sean objeto de un proceso legal o de investigación interna por el tiempo que sea requerido.

8.19 Controles ambientales

Directriz: La custodia de la información deberá realizarse en condiciones que no causen el deterioro de los activos de información.

Se deben implementar medidas de control físico y procedimientos de seguridad operacionales para proteger la información, el software y el hardware de daños intencionales o accidentales.

Todo sistema debe contar con planes de emergencia y contingencia, los cuales deben ser probados y actualizados periódicamente.

8.20 Copias de seguridad

Directriz: Alliance Enterprise debe garantizar la existencia de actividades adecuadas para la administración de copias de respaldo sobre la información necesaria para ejecutar los procesos críticos, garantizando la existencia de mecanismos adecuados para restaurar de forma completa y oportuna la información en caso de ser necesario.

La Dirección de Plataforma Tecnológica es la encargada de definir y/o mantener los procesos de respaldo acorde con las herramientas tecnológicas implementadas. Las estrategias de respaldo de la información deben estar alineadas a los activos y procesos críticos, así como a la estrategia de continuidad definida.

Las copias de respaldo de los activos críticos, deberán ser almacenadas en lugares seguros de acuerdo a la presente política con el fin de velar por el principio de confidencialidad.

Los respaldos de los activos críticos de valor sensible deben tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

8.21 Control de virus y otro tipo de código malicioso

Directriz: Toda la infraestructura de procesamiento de información de Alliance Enterprise, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores.

La Dirección de Plataforma Tecnológica debe mantener los mecanismos adecuados para el control de código malicioso que pueda ingresar a los equipos de cómputo y servidores de la compañía, debe disponer de monitoreo periódico que permita identificar el estado de los recursos y definir planes de acción para la mitigación de estos riesgos.

Los terceros que actúen con información que viaja a través de los recursos de Alliance Enterprise deben respetar esta política. Como mínimo se deben adoptar los siguientes mecanismos de control:

a. Todo el software será instalado a partir de copias originales, previamente escaneadas por la Dirección de Plataforma Tecnológica.
b. La Compañía mantendrá únicamente una marca de antivirus comercial, el cual debe ser aplicado a todos los equipos sin excepción.
c. Todos los terceros (proveedores, clientes) que realizan conexiones entre equipos propios y de Alliance Enterprise, deben contar con un antivirus actualizado.
d. No se debe usar software libre (shareware) sin previo escaneo por parte de un colaborador autorizado de la Dirección de Plataforma Tecnológica.
e. Los terceros que pretendan hacer demostraciones o pruebas de software, deben hacerlo en máquinas propias, ajenas a las de la Compañía antes de su instalación final.
f. Todos los servidores deben contar con un software antivirus actualizado.
g. Las copias de seguridad de los Files Servers deben ser escaneadas en busca de código malicioso

8.22 Conservación y destrucción

Directriz: Es responsabilidad del dueño del activo de información, determinar cuando la información ha dejado de ser útil para la organización de acuerdo con su valoración y acorde a la regulación que aplique.

Se deben establecer actividades relacionadas con el tratamiento de la información durante su vida útil y establecer los mecanismos de destrucción o borrado de acuerdo con el medio que la custodie.

Todos los colaboradores, deben destruir de manera segura los documentos físicos clasificados como de Uso Restringido previo a su desecho (con máquina trituradora o manualmente).

Borrado Seguro: Todos los medios de almacenamiento que contengan información de Alliance Enterprise y que vayan a ser reutilizados o dados de baja, deben seguir el procedimiento de borrado y destrucción segura de soportes de almacenamiento y la política de disposición final de residuos electrónicos RAEE.

8.23 Separación de Redes

Directriz: Todas las conexiones de red de Alliance Enterprise deben contar con un esquema de segregación, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que se preserve la confidencialidad, integridad y disponibilidad de la información de Alliance Enterprise.

Establecer parámetros técnicos para la conexión segura a cada uno de los segmentos de red.

- Producción
- Contingencia
- Certificación
- Desarrollo

Nota: Los segmentos de red se encuentran lógicamente segregados, lo que impide que los ambientes de desarrollo y certificación puedan acceder a los ambientes productivos.

8.24 Requisitos Mínimos de Seguridad en Aplicaciones

Directriz: Los desarrollos de aplicaciones al interior de Alliance Enterprise deben contar mínimo con las siguientes características de seguridad:

- Módulo de seguridad para la gestión de usuarios y accesos.
- Configuración de parámetros de contraseñas.
- Gestión, protección y tratamiento de datos personales (Definido a nivel contractual).
- Autenticación a través de múltiples factores de autenticación.
- Evaluación y Gestión de Vulnerabilidades y Pruebas de Ethical Hacking a nivel de infraestructura y software.
- Configuración de registros de log y auditoría.
- Configuración de firmas de integridad, utilizando algoritmos criptográficos AES256 sobre la información en tránsito.
- Registros ante la Dirección Nacional de Derecho de Autor de Colombia.

WEB Service

- Uso de certificados autofirmados (HTTPS)
- Autenticación básica.
- Transmisión de información firmada con algoritmo AES256-GCM vía Alliance Enterprise - cliente.

8.25 Desarrollo y mantenimiento de software (gestión de cambios)

Directriz: Se deben implementar procesos formales para controlar el desarrollo, mantenimiento e implementación de cambios en los sistemas de información. Los

cambios a los programas existentes o implementación de nuevos sistemas en el ambiente de producción deben ser sometidos a todas las pruebas que se consideren necesarias y autorizados por las instancias definidas.

Todas las actividades de implementación y mantenimiento de los sistemas de información se deben realizar bajo un modelo de administración que asegure una adecuada segregación de funciones.

Alliance Enterprise debe disponer de 4 ambientes independientes para el desarrollo de software dispuestos de la siguiente forma:

- Ambiente de desarrollo.
- Ambiente de pruebas QA.
- Ambiente de certificación con clientes.
- Ambiente de producción.

En todo caso, el desempeño y la seguridad de un ambiente no podrán influir en los demás ambientes.Los cambios de emergencia que deban hacerse directamente sobre el ambiente de producción deben ser aprobados por el comité de cambios, y deben ser debidamente documentados de acuerdo a los procesos existentes.

Los pasos a los ambientes de producción deben contar con los soportes definidos en los procesos y con las autorizaciones respectivas.

Nota: Ver **Política de Desarrollo Seguro**.

8.26 Propiedad intelectual

Directriz: Todo material desarrollado mientras exista una relación o vinculación laboral con Alliance Enterprise se considera de propiedad intelectual de la Compañía y es de uso exclusivo para las labores propias del negocio, por lo tanto, su utilización o publicación no autorizada será considerada un incumplimiento de la presente política.

La propiedad intelectual se define como cualquier patente, derecho de autor, desarrolló, invención o información que es propiedad de Alliance Enterprise.

Nota: Todas los desarrollos de Alliance Enterprise se encuentran registrados en la Dirección Nacional de Derechos de Autor.

8.27 Contratación con terceros

Directriz: Los contratos de servicios con proveedores externos, deberán contener la cláusula de confidencialidad de la información y acuerdos de niveles de servicios SLA, y de requerirse extensiva a sus empleados. Aplica para proveedores críticos.

Las áreas que requieran la contratación de servicios con proveedores deberán velar por la inclusión de la cláusula de confidencialidad de la información y acuerdos de niveles de servicios SLA en sus contratos.

La aplicación de esta política incluye a los terceros y proveedores, como a su personal; sobre el uso de la información de Alliance Enterprise, siguiendo los lineamientos de seguridad durante su tratamiento, procesamiento, almacenamiento y destrucción. Ver **Procedimiento Manejo de Proveedores.**

8.28 Infraestructura de Seguridad

Directriz: La alta dirección debe proporcionar la infraestructura de seguridad requerida para gestionar los riesgos asociados a los activos de información bajo los principios de confidencialidad, integridad, y disponibilidad.

8.29 Pruebas de Vulnerabilidades y Ethical Hacking

Directriz: Alliance Enterprise debe realizar pruebas controladas de intrusión a la plataforma tecnológica (Ethical Hacking) al menos una vez al año con el fin de identificar vulnerabilidades y debilidades de configuración que puedan poner en riesgo la seguridad de la información. Cabe anotar, que estas pruebas se pueden realizar con una mayor periodicidad, dependiendo de las necesidades del negocio o de que la regulación así lo requiera. Así mismo, para las vulnerabilidades encontradas y explotadas de manera exitosa se deberán definir los planes de acción y cerrar de acuerdo a su criticidad en los periodos de tiempo establecidos.

La realización de las pruebas de Ethical Hacking pueden ser ejecutadas por personal interno de Alliance Enterprise con las certificaciones que lo acrediten para realizar este tipo de pruebas o seleccionando un proveedor. Ver P**rocedimiento para la Gestión de Vulnerabilidades y Ethical Hacking.**

La gestión de los hallazgos se realizará con la siguiente prioridad de acuerdo al su clasificación

- Para Críticos: Se debe evaluar el cierre en mes y medio, preferiblemente.
- Para Altos: Se debe evaluar el cierre en los siguientes 3 meses.
- Para Medias y bajas: Mayor a 6 meses.

8.30 Interfaces

Directriz: Las soluciones tecnológicas que requieran el uso de interfaces de datos deberán contar con esquemas de seguridad acordes al nivel de criticidad de la información con el fin de guardar los principios de seguridad de la información.

Deben estar claramente establecidos los objetivos, alcances y funcionamiento de las interfaces, así como los controles de seguridad de acuerdo con la criticidad de los activos de información.

Se deben establecer y formalizar mecanismos estándar para la transmisión de datos entre los aplicativos de la organización, agrupados de acuerdo con el nivel de seguridad y de criticidad de la información que se transmite con base en lo siguiente:

- Información Confidencial o Restringida: Transmisiones seguras y cifradas o con controles de acceso sobre los activos de información.
- Información de uso interno: Transmisión en archivos planos centralizados y protegidos por contraseña.
- Información Pública: Transmisión de archivos de texto distribuidos.

8.31 Protección de hojas de cálculo

Directriz: Los procesos aquí descritos son aplicados a todas las aplicaciones que no son soportadas por TI y que son utilizadas dentro de Alliance Enterprise, para apoyar procesos críticos.

Procesos de Finanzas definidos Críticos: Aquellos en los cuales se realizan cálculos o consolidación de información financiera que es utilizada para emitir reportes al regulador o a áreas internas. Cualquier tipo de información que no pueda ser obtenida de los sistemas de Alliance Enterprise, y que sea considerada como crítica en los procesos.
Procesos complejos que se desarrollen por fuera de los sistemas soportados por TI.
Para la presente política, se hacen las siguientes aclaraciones:

- Se consideran aplicaciones no soportadas por TI:
  - Hojas de cálculo Excel
  - Bases de datos de Access, o cualquier otra base de datos que no esté administrada por la Dirección de Plataforma tecnológica.

  Nota: En caso de duda sobre las aplicaciones manejadas por las áreas, por favor verificar con la Dirección de Plataforma Tecnológica si esta es soportada.
- Toda información relacionada con estas aplicaciones, debe residir en un sitio en Google drive designado para cada área o en su defecto en el espacio el en file server designado, con el fin de que quede un respaldo de esta información. Esta información no debe residir en las estaciones de usuario final. Adicionalmente, el acceso a estas aplicaciones debe ser autorizado a los funcionarios designados, de acuerdo a las instrucciones recibidas por parte del dueño del activo de la información.
- El dueño del activo de la información, deberá documentar la información de la aplicación y su clasificación de acuerdo a la metodología establecida para la administración de los activos de información.
- Las hojas de cálculo que utilicen fórmulas, así como aquellas que contengan información crítica para Alliance Enterprise, deberán ser protegidas y su password debe ser conocido por el dueño del activo de la información y por el gerente del área que lo administra, esto con el fin de que en caso de ausencia del operador de la aplicación no se generen inconvenientes en el proceso.

8.32 Restricciones para captura de imágenes y toma de fotos

Directriz: Está prohibida la toma de fotos, captura de imágenes con dispositivos móviles sobre las estaciones que puedan visualizar la información de clientes. Cualquier incumplimiento de esta directriz que resulte comprometiendo la confidencialidad, integridad y disponibilidad de la información podrá generar una sanción disciplinaria de acuerdo a lo establecido en el contrato laboral, el reglamento interno de trabajo y el **Código de Ética y Conducta** respectivamente.

9 Excepciones a la presente política

Directriz: Las excepciones requeridas por los colaboradores a la presente política, deberán estar justificadas como requerimientos organizacionales y deben contar con las autorizaciones de los gerentes o directores de la compañía. Estas excepciones deben ser revisadas anualmente para garantizar su adecuado uso. Cabe anotar que estas excepciones deben estar recopiladas y a cargo del Analista de Seguridad de la Información.

Realizó	Revisó	Aprobó
Gerente de Riesgos y Procesos	Analista de Procesos	Gerente de Riesgos y Procesos