1. OBJETIVO

Establecer los lineamientos en la Organización Pajonales S.A.S para mitigar los riesgos asociados a los sistemas de información, ya sea en los aplicativos locales como en los implementados en la nube, describiendo lo que se espera de todo los proveedores y contratistas que en el desarrollo de sus funciones puedan tener acceso a la información restringida o a los sistemas de información o recursos de Pajonales, con el fin de proteger la confidencialidad, integridad y disponibilidad de su información.

2. DEFINICIONES

Activos Críticos de Información: Es toda aquella información necesaria para el negocio, que es procesada, transportada o almacenada por medios informáticos como software, hardware, redes o cualquier otro medio o formato en que ésta se encuentre, ya sea en los aplicativos locales como en los implementados en el ciberespacio. Esta definición aplica para las partes del documento donde se cite la frase Activos de Información.

Acuerdos de Niveles de Servicios: Pactos realizados entre áreas o con terceros con el fin de establecer aspectos a tener en cuenta para el intercambio de información; tales como: medios de transmisión, periodicidad, canalizador y como es este caso, las seguridades implementadas (certificación digital, cifrado, reserva, etc.).

Área Crítica: Áreas de la organización en donde la información del negocio es procesada, transportada o almacenada por medios informáticos como software, hardware, redes o cualquier otro medio o formato en que ésta se encuentre.

Código Malicioso: Software que es creado con el propósito de hacer daño. Los virus informáticos están catalogados como código o software malicioso.

Confiabilidad: Indica que la información debe ser la apropiada para la administración de la Entidad y el cumplimiento de obligaciones.

Responsable de la información: Individuo o unidad organizacional que tiene responsabilidad de clasificar y tomar decisiones de control respecto al uso de su información.

Información: Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, ya sea en los aplicativos locales como en los implementados en el ciberespacio sirve de soporte a las actividades de negocio y a la toma de decisiones. Esta definición aplica para las partes del documento donde se cite la frase Información del Negocio.

Información Restringida: Información crítica al interior de la organización o en el ciberespacio y es para uso exclusivo de un grupo específico de funcionarios, Área o División. Dicha información puede ser conocida únicamente por los funcionarios de PAJONALES relacionados con las tareas asignadas y terceros relacionados estrictamente según la operación del negocio y que al ser revelada a personas no autorizadas puede poner en riesgo la continuidad de la operación del

negocio y/o puede tener un fuerte impacto en los estados financieros, en los asuntos legales y/o en la imagen de PAJONALES.

Información de Uso Interno: Información disponible solo para funcionarios de PAJONALES la cual en caso de ser revelada a terceros representa un bajo riesgo para la operación del negocio y/o los estados financieros.

Información Pública: Información catalogada como no sensible y que puede ser conocida tanto por el personal de PAJONALES, como por terceros sin que se ponga en riesgo su imagen ni tenga impacto en los estados financieros.

Internet: Es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes.

Log: Archivo donde se registran las diversas actividades realizadas por los usuarios en el sistema (rastro).

Miembro de la Comunidad: Individuo que tiene autoridad limitada y específica del responsable de la información para ver, modificar, adicionar, divulgar o eliminar dicha información.

Modelo de Seguridad de la Información y Ciberseguridad y Ciberseguridad: Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad y ciberseguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.

Norma: Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.

Organización de Seguridad de la Información y Ciberseguridad: Estructura organizacional que soporta la Seguridad de la Información y Ciberseguridad, donde se definen roles y responsabilidades de cada uno de sus integrantes.

Perímetros o áreas seguras: Un área o agrupación dentro de la cual un conjunto definido de políticas y medidas se aplican para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar entidades con requisitos de seguridad y niveles de riesgo similares, para asegurar que cada zona se separa adecuadamente de las otras.

Política de Seguridad de la Información y Ciberseguridad: Documento donde establece las directrices y los lineamientos relacionados con el manejo seguro de la información en PAJONALES que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de la entidad y/o los prestados a través de terceros.

Procedimiento: Pasos operacionales específicos que los individuos deben tomar para lograr las metas definidas en las políticas.

Recursos de información: Dispositivos o elementos que almacenan datos, ya sea en los aplicativos locales como en los implementados en el ciberespacio, tales como: registros (formatos), archivos, Bases de Datos, equipos y el software propietario o licenciado por PAJONALES., o bajo los términos definidos con el tercero contratado para la prestación del servicio.

Riesgo: Probabilidad de que ocurra un evento en seguridad de la información y/o ciberseguridad, que cause algún tipo de pérdida a PAJONALES.

Seguridad de la información y Ciberseguridad: Protección de la información contra el acceso no autorizado accidental o intencional, su modificación, destrucción o publicación.

Seguridad física: Protección de los equipos de procesamiento de la información ya sea que se encuentren en la infraestructura tecnológica local y/o en el ciberespacio de daños físicos, destrucción o robo; asimismo, se protege al personal de situaciones potencialmente dañinas.

Trabajo Móvil: Estilo de trabajo en el que se dispone de servicios de tecnología que permiten realizar las actividades laborales desde ubicaciones diferentes a la oficina o puesto de trabajo asignado.

Llaves de cifrado: Es un elemento o pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa. Por su sensibilidad, las llaves de cifrado deben tener un nivel de seguridad mayor.

Ciberseguridad: Es el conjunto de políticas, conceptos de seguridad, recursos, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger a los activos de la entidad en el ciberespacio.

Ciberespacio: Corresponde a un ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado en dispositivos tecnológicos y redes conectadas a la red mundial, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios.

Nota: Para el presente documento, se entenderá ciberespacio como el entorno donde se establezcan los servicios de la entidad y los prestados a través de terceros.

Ciberamenaza o amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar un ciberataque contra la población, el territorio y la organización política del Estado.

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnicas de funcionamiento de las conexiones de los seres vivos y de las máquinas.

Ciberataque o ataque cibernético: Acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del ciberespacio.

Ciberiesgo o riesgo cibernético: Posibles resultados negativos asociados a los ataques cibernéticos.

Evento de ciberseguridad: Ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación de la Política de Seguridad de la Información y Ciberseguridad o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

Información en reposo: Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, bases de datos, almacenes de datos, hojas de cálculo, archivos, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

Información en tránsito: Información que fluye a través de la red pública o que no es de confianza, como Internet y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial.

Terceros críticos: Terceros con quien se vincula la entidad y que pueden tener incidencia directa en la seguridad de su información.

Riesgos Emergentes: Son los riesgos producidos por nuevos tipos de ataques o modalidades, así como por los generados por la implementación de negocios nuevos. Normalmente son desconocidos por lo que su probabilidad de ocurrencia puede ser baja, sin embargo, su impacto podría ser alto.

Nube: Es un modelo de uso de los equipos informáticos, donde se puede trasladar parte de los archivos y programas a un conjunto de servidores a los que se puede acceder remotamente a través de Internet.

3. ALCANCE

Aplica para todos los proveedores y contratistas que tienen acceso a la información restringida o acceden a los sistemas de información de Pajonales, ya sea en los aplicativos locales como en los implementados en la nube.

4. CUMPLIMIENTO

Todo el personal de proveedores y contratistas que tienen acceso a información restringida o a los sistemas de información de Pajonales, ya sea en los aplicativos locales como en los implementados en la nube, deberán cumplir con las normas de Seguridad y Ciberseguridad recogidas en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, Pajonales se reservan el derecho de veto sobre el personal externo que haya cometido la infracción, así como la ejecución de las medidas sancionatorias que se consideren pertinentes en relación con la empresa contratada, y que pueden llegar a la finalización de los contratos que se tengan vigentes.

5. NORMAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PARA PROVEEDORES Y CONTRATISTAS

Seguridad de la información y Ciberseguridad

- ✓ El proveedor o contratista protegerá y garantizará la confidencialidad, integridad, disponibilidad, auditabilidad y privacidad de la información de Pajonales, sin importar el medio, formato o presentación en que la información sea creada, almacenada o utilizada.

Confidencialidad de la información

- ✓ El personal externo que tenga acceso a información de Pajonales deberá considerar que dicha información, por defecto, tiene el carácter de restringida.

- ✓ El personal externo protegerá la información restringida a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información ejerciendo sobre ésta el mismo grado de diligencia que utiliza para proteger información restringida de su propiedad.

- ✓ El personal externo se obliga a mantener la confidencialidad absoluta sobre la documentación e información que conozca o reciba para la ejecución de sus actividades.

- ✓ El personal externo se abstendrá de fotocopiar y/o sacarle copia a la información que reciba, salvo las copias que requiera para el desarrollo de su trabajo, entendiéndose que el manejo que se le dé a tales copias está cobijado por lo definido en estas normas.

- ✓ Ningún proveedor o contratista, en proyectos o trabajos puntuales deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada por Pajonales tanto ahora como en el futuro.

- ✓ Cumplida la finalidad para la cual fue entregada la información y los documentos, el empleado del proveedor o contratista destruirá los documentos o los devolverá al responsable en Pajonales, de acuerdo con las instrucciones que ésta imparta en ese sentido.

Control de acceso físico a instalaciones de Pajonales.

- ✓ El personal del proveedor o contratista no podrá permanecer ni ejecutar trabajos en las áreas críticas sin supervisión. Sólo podrá ingresar cuando se tenga la autorización respectiva del colaborador responsable en Pajonales, e ingresar con la persona acompañante que éste designe.

- ✓ Portar siempre visible el carnet que lo identifique como funcionario de un proveedor o contratista.

- ✓ El proveedor o contratista debe mantener las áreas en donde se encuentre la información de Pajonales, con las protecciones necesarias, controles de seguridad ambientales y acceso físico adecuados, de modo tal que se garantice la conservación física y confidencialidad de esta.

- ✓ El personal del proveedor o contratista no debe comer, beber o fumar cuando se encuentre en las instalaciones de Pajonales donde se encuentre información o sistemas de información.

- ✓ No mover ni manipular equipos o información que estén en los centros de cómputo, a no ser que sea estrictamente necesario para la prestación del servicio, para lo cual deberá obtener el visto bueno del colaborador responsable en Pajonales.

- ✓ No retirar equipos, ni información de las instalaciones de Pajonales sin previa autorización del colaborador responsable.

- ✓ Permitir las actividades de revisión al ingreso y salida de los centros de cómputo o de las instalaciones, si Pajonales así lo considera necesario.

- ✓ Al finalizar las actividades, informar al colaborador responsable de Pajonales para que se verifique el buen estado de las instalaciones, de los equipos y de la información (verificación de la actividad contratada), al igual que para restringir nuevamente los accesos a estos lugares.

- ✓ El ingreso de equipos celulares, cámaras fotográficas o cámaras de video no está prohibido, sin embargo, el personal del proveedor o contratista si debe abstenerse de tomar fotografías o vídeos de los centros de cómputo y de áreas críticas.

- ✓ Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:

    - Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

    - Asegurar la confidencialidad de los documentos tanto en los puntos de recepción y envío de información (correo postal, máquinas de escáner, etc.) como en las fotocopiadoras.

Uso apropiado de los recursos

Los recursos que Pajonales pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir las obligaciones enmarcados en la relación contractual y para el propósito de la operación para la que fueron diseñados e implantados.

El personal del proveedor o contratista que use dichos recursos debe conocer que no tiene el derecho de confidencialidad en su uso y por lo tanto acepta que el uso de dichos elementos sea objeto de supervisión y monitoreo.

Queda prohibido:

- ✓ El uso de estos recursos para actividades no relacionadas con el propósito del servicio, o bien la extralimitación en su uso.

- ✓ La búsqueda o explotación de vulnerabilidades en cualquier aplicación o equipos.

- ✓ Introducir en los sistemas de información o la red corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

- ✓ Introducir cualquier tipo de malware, dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.

- ✓ Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- ✓ Intentar distorsionar o falsear los registros “log” de los sistemas de información.
- ✓ Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
- ✓ Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, o dañar o alterar los recursos informáticos.
- ✓ Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Estos actos podrían constituir un delito, según la legislación vigente.
- ✓ Almacenar o introducir en la red corporativa o en el puesto de trabajo del usuario cualquier archivo a través de Internet, correo electrónico o cualquier otro medio, que no cumpla con los requisitos establecidos en las normas de propiedad intelectual y protección de datos personales.
- ✓ Conectar computadores no corporativos a la red de comunicaciones de Pajonales, excepto a la red habilitada para ello, disponible para visitas, proveedores, etc.
- ✓ Ningún usuario externo intentará por ningún medio vulnerar el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo**.**

Protección frente a malware

Los recursos que el proveedor o contratista utilizan para la prestación del servicio a Pajonales deberán seguir las siguientes directrices:

- ✓ Los sistemas se deben mantener al día con las últimas actualizaciones de seguridad disponibles.
- ✓ El software antivirus se deberá instalar y usar en todos los servidores y computadores donde repose información de Pajonales.
- ✓ El software antivirus deberá estar siempre habilitado; se establecerá una actualización automática de definición de virus tanto en los computadores como servidores.
- ✓ En caso de que sea detectado cualquier malware en uno de los equipos conectados a la red de Pajonales, dicho equipo será desconectado de la red sin que sea necesario aviso previo.

Intercambio de información

- ✓ Para el intercambio de información magnética se deben utilizar cuentas de correo electrónico corporativos u oficiales tanto de la empresa contratista o proveedor (si es posible) como de Pajonales.
- ✓ El intercambio de información restringida debe realizarse a través de medios seguros; para esto se deben utilizar herramientas de cifrado cuando es información digital. En caso de que

sea información física debe entregarse en sobres cerrados, y verificar su recepción por parte de la persona responsable en Pajonales.

- ✓ En relación con el intercambio de información, se considerarán no autorizadas las siguientes actividades:
    - Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias, raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
    - Transmisión o recepción de archivos que infrinjan la ley de protección de datos personales, ley de derechos de autor o directrices de Pajonales.
    - Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
    - Uso de repositorios de almacenamiento masivo públicos tipo Dropbox o Google Drive y almacenamiento de información en medios externos (CD/DVD, discos extraíbles y USB), para esto las unidades de salida estarán bloqueadas (cuando el equipo sea entregado por Pajonales).

Conectividad a internet

La utilización de internet por parte de los usuarios externos estará sujeta a las siguientes normas:

- ✓ Todas las actividades en internet deberán estar en relación con las tareas y actividades de trabajo.
- ✓ Todo el tráfico desde y hacia internet será inspeccionado en búsqueda de amenazas. En caso de que algún empleado del proveedor o contratista se encuentre accediendo a sitios clasificados como maliciosos (pornografía, juegos, etc.) o ajenos al negocio se le podrá bloquear la navegación sin que sea necesario aviso previo.
- ✓ El acceso a internet desde la red corporativa se restringe por medio de dispositivos de control incorporados en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de internet.
- ✓ La transferencia de información no relativa a estas actividades (por ejemplo, la descarga de juegos, música y contenidos multimedia) está prohibida, quedando expresamente prohibido el uso de software tipo P2P o torrents.

Responsabilidad sobre el usuario y la contraseña asignada

Cada empleado del proveedor o contratista será responsable de sus credenciales de acceso y todo lo que de él se derive, por lo que es imprescindible que esta información sea personal e intransferible.

Por lo anterior, los usuarios externos asumen las siguientes responsabilidades:

- ✓ Cuando el usuario recibe sus credenciales de acceso a los sistemas de Pajonales se considera que acepta formalmente las normas de Seguridad de la Información y Ciberseguridad dadas en este documento.

- ✓ El usuario será responsable de todas las acciones registradas en los sistemas informáticos de Pajonales ejecutadas con su usuario.

- ✓ Los usuarios no deben revelar bajo ningún concepto sus credenciales de acceso a otra persona ni mantenerla por escrito a la vista ni al alcance de terceros.

- ✓ Los usuarios deberán seguir las directivas definidas en relación con la gestión de las contraseñas establecidas en el dominio de Pajonales (cambio periódico, complejidad, historial).

- ✓ Los usuarios deberán asegurar que los equipos quedan protegidos cuando estén desatendidos, es decir deben bloquearlos al ausentarse del puesto de trabajo.

Uso de software

- ✓ El software que se utilice durante la ejecución debe cumplir con los requerimientos legales que faculten su utilización.

- ✓ El proveedor o contratista se abstendrá de instalar software en los equipos de Pajonales, sin la previa autorización por parte de éste. El contratista o proveedor garantizará que ha obtenido las licencias y autorizaciones respectivas de los propietarios del software que instale con la autorización de Pajonales en sus equipos.

Conexión a la red

Sobre la conexión a la red se establecen los siguientes principios:

- ✓ Pajonales se reserva el derecho de, sin aviso previo, bloquear, suspender, alterar o monitorear los servicios soportados en su red informática y puestos a disposición del personal externo, cuando se detecten actividades que contravengan los principios y normas expresados en el presente documento.

- ✓ No se deberá conectar a los recursos de Pajonales ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

- ✓ Nadie deberá conectarse a la red corporativa a través de otros medios que no sean los definidos.

- ✓ Se prohíbe la captura de tráficos de red por parte de los usuarios externos, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas por el área de seguridad de la Información y Ciberseguridad de Pajonales.

- ✓ El proveedor o contratista deberá notificar al responsable del servicio en Pajonales, todos los cambios habidos en cuanto a las personas, identidades y equipos que estén conectados a los sistemas de información de Pajonales, ya sea en los aplicativos locales como en los implementados en la nube, Además, el responsable de Pajonales tiene la obligación de solicitar la modificación de estos accesos de acuerdo con los procedimientos internos establecidos para este fin.

Propiedad intelectual

En relación con la propiedad intelectual se aplicarán las siguientes normas:

- ✓ Las entidades externas que acceden a internet a partir de la red informática y equipos de cómputo de Pajonales son responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.

- ✓ Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

- ✓ Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

- ✓ Pajonales únicamente autorizarán el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

Incidentes de Seguridad de la Información y Ciberseguridad

En caso de detectarse algún incidente relacionado con los sistemas de información y/o ciberseguridad se deben seguir las siguientes normas:

- ✓ El proveedor o contratista debe reportar el incidente al colaborador de Pajonales manteniendo estricta confidencialidad sobre la ocurrencia de tal incidente, para lo cual deberá hacer uso de los canales de comunicación seguros definidos por Pajonales.

- ✓ El proveedor o contratista deberá acatar las recomendaciones que Pajonales haga en relación con el manejo de dicho incidente de seguridad, dentro de los plazos determinados.

- ✓ El proveedor o contratista no deberá ejecutar actividades que permitan generar incidentes de seguridad y/o Ciberseguridad que puedan afectar la confidencialidad, integridad, disponibilidad, privacidad y auditabilidad de la información de Pajonales. Además, deberá mantener la integridad de las evidencias, generadas como consecuencia de una violación a las normas de seguridad de la información y Ciberseguridad.

- ✓ Cualquier usuario podrá informar al área de Seguridad de la Información y Ciberseguridad sugerencias y/o debilidades, que pueda tener relación con la Seguridad de la Información y Ciberseguridad, y las directrices contempladas en el presente documento.

Seguimiento y control

- ✓ Con el fin de velar por el correcto uso de los mencionados recursos, a través de los mecanismos formales y técnicos que se considere oportunos, Pajonales comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos por todos los usuarios. En caso de apreciar que alguien utiliza incorrectamente aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, se le comunicará tal circunstancia y se le facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.

- ✓ En caso de apreciarse mala fe en la incorrecta utilización de las aplicaciones y/o datos, principalmente, así como cualquier otro recurso informático, Pajonales ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

- ✓ En caso de que el servicio contratado sea prestado en instalaciones diferentes a las de Pajonales y según ésta lo considere necesario, el proveedor o contratista debe permitir la ejecución de revisiones o auditorías periódicas para la verificación de los acuerdos pactados en el contrato, contando con una programación y coordinación previa la visita.

DOCUMENTOS REFERENCIA

- ✓ Política de Seguridad de la Información y Ciberseguridad – PLT-SIC-001
- ✓ Formulario Único de Conocimiento de Terceros - FR-CMP-022

IDENTIFICACIÓN DE CAMBIOS			
Versión	**Página**	**Numeral**	**Descripción del cambio**
01	11	N. A	Se cambia código de la política de seguridad de la información y ciberseguridad