QSystems SAS se compromete a proteger la información de nuestros clientes y aliados, que se genera, circula, procesa y almacena en la prestación de sus servicios.

1. OBJETIVO

Objetivo General: Salvaguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información de la empresa, minimizando el riesgo de pérdida, robo o daño de la información sensible.

Objetivos específicos:

- Establecer controles de seguridad adecuados para proteger los activos de información.
- Definir políticas y procedimientos de seguridad de la información para guiar las prácticas y comportamientos de los empleados.
- Realizar auditorías y evaluaciones periódicas para garantizar el cumplimiento de las políticas y procedimientos de seguridad de la información.
- Responder de manera eficiente y efectiva a incidentes de seguridad de la información, mitigando los impactos y restaurando la normalidad lo antes posible.
- Proporcionar concientización y capacitación en seguridad de la información a todos los empleados de la empresa.

2. ALCANCE

El proceso de seguridad de la información se aplicará a todos los activos de información y sistemas de la empresa, incluyendo datos internos y de clientes, manejo de correos electrónicos, aplicaciones de software, redes, servidores y dispositivos de almacenamiento.

3. DEFINICIONES

- **Auditoría:** Proceso por el que se lleva a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos,para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.
- **Bases de Datos:** Es un conjunto de datos interrelacionados y un conjunto de programas para accederlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.
- **Confiabilidad**: Está determinada por el posible daño, como resultado de una operación del sistema de información realizada en forma incorrecta,incompleta, impropia o inoportuna.

- **Confidencialidad**: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control de Acceso:** Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria, es una característica o técnica en un sistema para permitir o negar el uso de algunos componentes o algunas de sus funciones.
- **Contraseña o Clave:** Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos) y su longitud.
- **Desarrolladores de Sistemas:** Personal que selecciona, desarrolla y da mantenimiento a los sistemas de información.
- **Política**: Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.
- **Política de Seguridad Informática (PSI):** Una política de seguridad informática es una forma de comunicarse con los usuarios. Las políticas de seguridad informática (PSI) establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos proteger y el porqué de ello.
- **Procedimiento**: Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.
- **Funcionario**: Personal que tiene relación directa con la entidad, Ya sea empleado, contratista o Tercero
- **Software as a Service (SaaS):** Es un modelo de software basado en la nube que ofrece aplicaciones a los usuarios finales a través de un navegador de Internet.
- **Impacto**: Evaluar el grado en que una amenaza podría afectar la operación del software, considerando aspectos como la pérdida de datos, la interrupción de las operaciones y la reputación de la organización.
- **Probabilidad:** Evaluar la probabilidad de que una amenaza específica se materialice, teniendo en cuenta la exposición actual y las medidas de mitigación existentes.

4. POLÍTICAS RELACIONADAS

QSystems SAS liderará la revisión, cumplimiento y mejoramiento continuo de la seguridad informática, y generará la documentación necesaria como procedimientos, manuales, instructivos y demás elementos que sean necesarios para tal fin.

Las políticas relacionadas a la Seguridad de la Información como son el presente documento, la Política de respaldo y seguridad de la información y la Política de tratamiento de datos personales deberán ser difundidas a todo el personal involucrado en su definición.

4.1. REGLAMENTO DE SEGURIDAD INFORMÁTICA

- **RESPONSABILIDADES:**

    - **Equipo de Seguridad de la Información**: Velar por el cumplimiento de la presente política, garantizando los niveles de seguridad adecuados para el uso de la infraestructura y sistemas de información.
    - **Líder de seguridad informática:** Designar el personal idóneo para que establezca y configure los dispositivos, redes de datos, elementos de seguridad, estaciones de trabajo y demás elementos que hagan parte de la red de datos y servicios digitales de QSystems SAS, acogiendo los lineamientos de seguridad definidos en la presente política.
    - **Personal**: Hacer uso responsable de la infraestructura y aplicaciones acogiendo los lineamientos establecidos para QSystems SAS.

4.2. CONTROL DE ACCESO

- Cada usuario debe tener una identificación única e intransferible dentro del sistema de control de accesos. La combinación de usuario y contraseña deben ser únicos.
- Los nombres de usuario y “claves” son personales e intransferibles, y solamente deben ser utilizados por el funcionario al que le fueron asignados. Está totalmente prohibido que un funcionario autorice el uso de clave a terceros o que preste sus credenciales de acceso.
- Todo funcionario será responsable de las actividades y transacciones que sean realizadas con su “usuario y clave” de carácter confidencial.
- Los derechos de acceso de los usuarios a las transacciones específicas de cada uno de los sistemas de información deben estar formalmente autorizados por el Líder de Seguridad Informática.
- Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros usuarios.
- Al asignarse por primera vez la contraseña a un funcionario debe realizarse su cambio de forma inmediata. Para la contraseña y nombre de usuario, deberá tener en cuenta lo siguiente:
- Las contraseñas de usuario deben ser alfanuméricas, contener caracteres especiales, combinación de mayúsculas y minúsculas y una longitud no menor a 8 (ocho) caracteres.
- No deben revelarse bajo ninguna circunstancia.
- No se deben utilizar “claves” previamente utilizadas.
- El nombre de usuario y la contraseña deben ser diferentes entre sí.

- No se deben utilizar contraseñas con información fácilmente identificable como fechas de cumpleaños, nombres de familiares y apellidos, números de identificación, y/o demás información personal evidente
- La contraseña debe ser cambiada periódicamente mínimo dos veces al año.
- El Líder de seguridad informática deberá revisar al menos dos veces al año los derechos de accesos conferidos a los usuarios administradores de los sistemas bajo su responsabilidad grupos de privilegios (incluye personal de la propia oficina, personal técnico, auditor y cualquier otro que lo requiera), verificando que los derechos asignados se ajustan a las funciones y tareas de cada funcionario.
- El líder de seguridad informática es responsable de dejar deshabilitados los derechos de acceso de aquellos funcionarios que ya no tiene una relación con Qsystems SAS.
- Ante múltiples fallas de autenticación de un usuario (contraseña errónea), el usuario será bloqueado automáticamente y se deberá informar al líder de seguridad informática para restablecer el acceso.
- No se deben dejar nombres de usuario y contraseñas escritos en lugares donde puedan ser vistos o tomados por terceros (por ejemplo en la carpeta del escritorio, pantalla del equipo, bajo el teclado, etc.).
- Los usuarios no deben dejar desatendidas las estaciones de trabajo. Todo funcionario es responsable de desactivar las aplicaciones (cerrarlas) de ser necesario, cada vez que se ausente de su puesto de trabajo, y dejarla bloqueada con contraseña.

4.3. CORREOS ELECTRÓNICOS

- El correo electrónico, es una herramienta de trabajo que provee la Institución a sus funcionarios, por lo tanto, es responsabilidad de cada usuario, utilizar prudente y apropiadamente este servicio.
- Todo evento que se dé a través del uso del Correo Electrónico, será administrado, monitoreado y regulado por el área Equipo de seguridad dela información, el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de QSystems SAS.
- El contenido de los mensajes creados, enviados, recibidos y almacenados debe limitarse a los propósitos Misionales y/o Operativos de QSystems SAS, su contenido debe ser respetuoso y no debe atentar contra la imagen ni integridad moral de sus funcionarios y usuarios.
- Queda totalmente prohibido enviar mensajes de correo electrónico masivos por parte de personal no autorizado.
- Las cuentas de correo electrónico institucional deberán ser usadas solamente para fines laborales; No para suscripción de servicios y/o listas de correo relacionadas con temas personales.

- Las cuentas de correo electrónico institucional deberán ser usadas solamente para fines laborales; No para suscripción de servicios y/o listas de correo relacionadas con temas personales.
- La información que se haya definido como sensible por QSystems SAS se puede transferir por medio de correo electrónico solamente si existe la necesidad real de transferir la información.
- Los mensajes creados, enviados, recibidos o almacenados no deben ser impresos, especialmente los configurados como de carácter reservado o confidencial, salvo que sea estrictamente requerido o necesario.

4.4. SISTEMAS DE INFORMACIÓN

- Todos los sistemas de información, herramientas de datos (programas, bases de datos, sistemas de información, interfaces y demás) desarrollados con o a través de los recursos de QSystems SAS se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo, incluyendo sus diseños, fuentes, documentación y demás aspectos de desarrollo.
- Todos los Sistemas de Información deberán ser desarrollados y documentados de acuerdo con la metodología estándar definida por QSystems.
- Para todos los sistemas de información, la seguridad debe ser considerada como obligatoria desde el inicio del ciclo de vida. Así mismo deben ser realizados las pruebas de vulnerabilidades y seguridad que QSystems, a través del área encargada considere pertinentes y no se pondrán en producción hasta tanto no se hayan corregido las vulnerabilidades existentes.
- Durante cada fase del proceso de desarrollo de sistemas, mantenimiento y ajustes, los aspectos de seguridad deben ser definidos explícitamente,documentados por el equipo de desarrollo y establecidos como un requerimiento de seguridad específico.
- En la fase de pruebas e implementación, las medidas de seguridad deben ser probadas adecuadamente por el líder de seguridad informática. Las pruebas deben ser documentadas en un reporte, remitidas al funcionario encargado.
- Cuando se realicen pruebas deberán de realizarse en un ambiente de prueba antes de poner la aplicación en producción y deberá considerarse el uso en paralelo del nuevo sistema y del antiguo sistema, a fin de detectar errores.
- El Comité Gerencial, deberá velar por que la aplicación desarrollada cumpla con la funcionalidad para la cual el desarrollo/Sistema de información fue contratado.
- El proceso de puesta en producción de las aplicaciones, de los sistemas o de sus actualizaciones, debe realizarse de tal forma que no deteriore los servicios a los usuarios o la operación normal, por tanto, debe coordinarse adecuadamente y realizarse con cronogramas y horarios preestablecidos.

- QSystems SAS será responsable de mantener la operatividad de los servidores y atender las fallas que estos presenten tanto a nivel del sistema operativo como a nivel de hardware, storage.
- QSystems SAS garantizará a los usuarios del servicio los recursos de almacenamiento y los respaldos de la información allí contenida.
- QSystems SAS será responsable de monitorear la utilización de los recursos de hardware en los servidores. Esto con el fin de proceder a la actualización de los mismos en el caso de ser requerido para garantizar la continuidad de los servicios.
- QSystems SAS notificará a los usuarios las ventanas de mantenimiento o la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.
- Todo código fuente, script o archivo relevante para el desarrollo de los sistemas de información deberá ser copiado y respaldado en el computador del programador que lo está elaborando y deberá alojar una versión en el repositorio de código fuente.
- Todo cambio deberá ser documentado, y de igual forma, deberá contar con una ventana de mantenimiento para su puesta en producción. Dichas ventanas de mantenimiento deben estar debidamente documentadas indicando fecha, responsable, servidor y aplicativo afectado. Se debe informar a los clientes afectados sobre la actualización.

4.5. SEPARACIÓN DE AMBIENTES

- La entidad deberá contar con ambientes separados para Desarrollo, Pruebas y Puesta en Producción de los Sistemas de Información. Bajo ningún motivo se podrá desarrollar aplicaciones en el ambiente productivo.
- Las funciones de desarrollo de aplicaciones, prueba, aceptación y producción de aplicaciones, y la custodia del software e información ligada, deben estar separadas y ser realizadas por funcionarios distintos entre sí, a efecto de asegurar una adecuada segregación de funciones.
- Cuando se realizan las pruebas del nuevo Sistema de Información deberá realizarse previamente en un ambiente de pruebas del sistema preferiblemente virtualizado, con el fin de no comprometer la información ni las bases de datos de QSystems SAS o de los usuarios.
- Las herramientas y privilegios propios del ambiente de desarrollo, que favorecen un ambiente y facilidades para las pruebas, no deben ser traspasados al ambiente de producción debido a que comprometen la seguridad de la operación normal; las pruebas deberán de realizarse en un ambiente de prueba o en paralelo.

4.6. GESTIÓN DE RECURSOS HUMANOS

- Antes de empezar a ejecutar las funciones por las cuales se adquiere vínculo con QSystems SAS, el personal deberá ser capacitado en las políticas con las cuales adquiere

responsabilidad y los sistemas de información con los cuales tendrá contacto; se deberá dejar evidencia de dichas capacitaciones en los formatos destinados para tal fin.

- Se deberá realizar reinducción permanente (mínimo una vez al año) en las temáticas de políticas de seguridad de la Información y Seguridad Informática.
- El líder de seguridad informática es responsable de dejar deshabilitados los derechos de acceso y los recursos de aquellos funcionarios que ya no tiene una relación con Qsystems SAS.
- En caso de finalizar el vínculo entre la persona y QSystems SAS , se deberá hacer entrega de la información a la cual tuvo acceso; esto deberá ser informado al supervisor del contrato y reposar en actas.

4.7. POLÍTICA DE COPIA DE SEGURIDAD O BACKUP

- La información sobre esta política y procedimiento puede encontrarse en el documento P - PROCESO DE BACKUP DE BASES DE DATOS Y ARCHIVOS INDEXADOS.

4.8. EVALUACIÓN DE RIESGOS

El propósito de una Evaluación de Riesgos es proporcionar una visión general de la planificación, implementación y mejora continua de los controles y medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de sistemas de información asociados dentro de QSystems S.A.S.

- **IDENTIFICACIÓN DE AMENAZAS**

Amenazas Internas: son aquellas que pueden originarse dentro de la organización o el entorno que administra los recursos e infraestructura de Qsystems SAS. Estas pueden incluir:

- **Error Humano**: Registrar posibles escenarios en los que los usuarios o administradores del software puedan cometer errores que afecten la integridad de los datos o la funcionalidad.
- **Abuso de Privilegios**: Identificar áreas en la infraestructura donde los usuarios pueden tener acceso a privilegios que no corresponden a sus roles, lo que podría llevar a actividades maliciosas o errores involuntarios.Descrito anteriormente en la sección de Control de acceso.

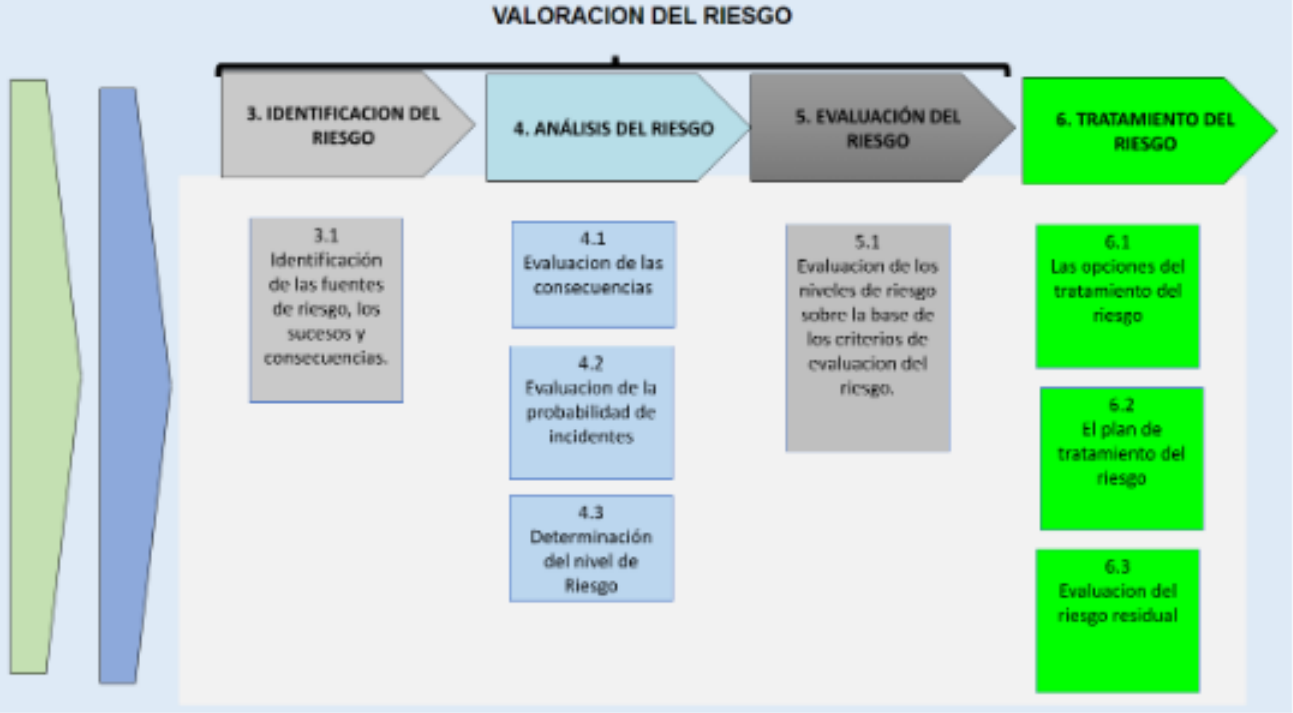
Amenazas Externas: son aquellas que provienen de fuentes externas a la organización y pueden incluir:

- **Ataques Cibernéticos:** Identificar posibles vectores de ataque, como intrusiones, malware, ataques de phishing o ataques de fuerza bruta, que podrían comprometer la seguridad y la confidencialidad de la información en custodia de QSystems SAS.

- **Brechas de Seguridad:** Analizar y evaluar la vulnerabilidad de los sistemas e infraestructura frente a las últimas amenazas de seguridad y posibles brechas que podrían exponer datos críticos o permitir el acceso no autorizado.
- **Fallos en Terceros**: Investigar la relación con terceros, proveedores o socios que puedan tener acceso o influencia en el software QS, identificando posibles debilidades en sus sistemas que podrían repercutir en la seguridad del software. Descrito anteriormente en la sección de Control de acceso y Sistemas de información.

- **EVALUACIÓN DE RIESGOS**

QSystems SAS basa la gestión del riesgo en el enfoque que parte del modelo definido por la norma ISO 31000, para ello se emplea el siguiente modelo:



Una vez que se han identificado las amenazas, es esencial evaluar su impacto potencial y su probabilidad de ocurrencia.

- **METODOLOGÍA DE APRECIACIÓN DEL RIESGO:**

Para la definición del nivel de riesgo (valoración), emplea un método cualitativo a partir de una matriz de calificación, compuesta por una serie de 5 columnas que definen la probabilidad de

materialización del riesgo; en el eje vertical aparecen 5 dimensiones de impacto. Con la participación de un grupo de expertos de cada proceso, entrenados en la metodología, se realiza la valoración de los riesgos, ubicando cada uno en uno de los cuadros de la Matriz de calificación del riesgo, como se muestra a continuación:

	Probabilidad muy baja	Baja probabilidad	Probabilidad media	Alta probabilidad	Muy alta probabilidad
Muy bajo impacto	0	1	2	3	4
Bajo impacto	1	2	3	4	5
Mediano impacto	2	3	4	5	6
Alto impacto	3	4	5	6	7
Muy alto impacto	4	5	6	7	8

- **Criterios de evaluación:** Luego de determinado el nivel de riesgo, se realiza la evaluación, en la cual se define su tratamiento y prioridad, según los criterios establecidos en la matriz de calificación (umbrales), el costo, la facilidad y el impacto del tratamiento.Para ello se analizan estos aspectos con las áreas encargadas.
- **Umbrales de evaluación:**
  - 0, 1 ó 2: Nivel de riesgo bajo. Se admite.
  - 3, 4 ó 5: Nivel de riesgo medio. Se analiza según el costo, facilidad e impacto del tratamiento. El equipo de la seguridad de la información define si se trata.
  - 6, 7 u 8: Nivel de riesgo alto. Se debe tratar, definir un plan de tratamiento acorde al caso, lo definen con la gerencia
- **Análisis y tratamiento de Riesgos:** Para realizar el análisis y tratamiento de riesgos se debe utilizar el siguiente formato (F - MATRIZ Y TRATAMIENTO DE RIESGOS - SEGURIDAD INFORMÁTICA):

- **MITIGACIÓN DEL RIESGO**

Con base en la evaluación de riesgos, se deben desarrollar estrategias de mitigación adecuadas. Esto incluye:

- Implementación de Controles de Seguridad: Establecer medidas de seguridad para reducir la probabilidad de ocurrencia de amenazas, como firewalls, sistemas de detección de intrusiones y autenticación.

- Políticas y Procedimientos: Desarrollar políticas y procedimientos internos que guíen el uso seguro de los sistemas de información e infraestructura y definir roles y responsabilidades claras.
- Análisis de Vulnerabilidades mediante Pruebas de Penetración: La empresa llevará a cabo análisis de vulnerabilidades mediante pruebas de penetración en la aplicación y la infraestructura del software QS por un proveedor externo por lo menos una vez al año. Estas pruebas identificarán posibles puntos débiles y brechas de seguridad, permitiendo la corrección proactiva de problemas antes de que se conviertan en amenazas reales. Una vez al año, se realizará una auditoría externa para análisis de vulnerabilidades completo. (P- PROCEDIMIENTO DE AUDITORÍA DE SEGURIDAD PARA SERVIDORES Y APLICACIONES).
- Capacitación y Concientización: Proporcionar formación a los funcionarios en temas de seguridad para minimizar errores humanos y mitigar los riesgos de falla.
- Auditorías y Monitoreo Continuo: Establecer un sistema de auditoría internas y externas y monitoreo constante para detectar y abordar rápidamente cualquier amenaza o brecha de seguridad.
- Esta incorporación del análisis de vulnerabilidades mediante pruebas de penetración fortalece la estrategia de mitigación al permitir la identificación proactiva y la revisión de posibles debilidades de los sistemas de información y su infraestructura, garantizando un nivel más alto de seguridad y robustez.

4.9. MEJORA DE LOS CONTROLES DE SEGURIDAD

Como parte de nuestro compromiso continuo con la seguridad de nuestros sistemas de información, hemos implementado una serie de mejoras significativas en nuestros controles de seguridad. Estas mejoras incluyen las siguientes acciones:

- Acceso controlado: esto garantiza que solo los usuarios autorizados tengan acceso a las funciones y datos críticos del sistema.
- **Política de copias de seguridad diarias:** estas copias se hacen con una periodicidad de 24 horas y de forma automática para proteger los datos esenciales de la empresa contra pérdidas accidentales o ataques cibernéticos.
- Auditorías regulares de análisis de vulnerabilidades: estas auditorías internas y externas se realizan en los sistemas de información y su infraestructura, para identificar y abordar proactivamente cualquier posible debilidad o riesgo de seguridad.

Estas medidas nos permiten mantener un entorno seguro y confiable para nuestros clientes, asegurando la integridad y la disponibilidad de los datos de mantenimiento.

5. FORMATOS

- P- PROCEDIMIENTO DE AUDITORÍA DE SEGURIDAD PARA SERVIDORES Y APLICACIONES
- L- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
- M- ANÁLISIS Y TRATAMIENTO DE RIESGOS
- F - MATRIZ Y TRATAMIENTO DE RIESGOS - SEGURIDAD INFORMÁTICA
- P - PROCESO DE BACKUP DE BASES DE DATOS Y ARCHIVOS INDEXADOS
- L- POLÍTICA DE FILTRADO EN TRANSMISIÓN DE DATOS
- L- POLÍTICA ACCESO Y AUTENTICACIÓN
- P- PROCESO MANEJO DE INCIDENTES DE SEGURIDAD
- P- PROCEDIMIENTO DE MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

CONTROL DE CAMBIOS

Versión	Cambio Realizado	Vigente a partir de:
1	Documento inicial	10/06/2023