1. NORMATIVA

Directiva 005 del 12 de agosto de 2005: Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital Alcaldía Mayor de Bogotá, D.C.

Ley Estatutaria 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Congreso de la Republica Decreto Ley 1151 abril de 2008: Establecen los lineamientos generales de la estrategia de gobierno en línea de la república de Colombia, se reglamenta parcialmente la Ley 962 de 2005. Manual de implementación de la estrategia de gobierno en línea Presidencia de la Republica.

Ley 1273 enero de 2009: Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Decreto 235 enero 2010: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas. Ministro del Interior y de Justicia de la República de Colombia.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales Congreso de Colombia.

Ley 1341 del 30 de julio de 2009: Por lo cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías s de la información y las comunicaciones TIC se crea la Agenda Nacional del Espectro y se dictan otras disposiciones

Ley 1437 de 2011 Capitulo IV: autorizan la utilización de medios electrónicos en el proceso administrativo en lo referente al documento público en medios electrónicos, el archivo electrónico de documentos, el expediente electrónico, la recepción de documentos electrónicos.

ISO/IEC 27001:2013: Describe cómo gestionar la seguridad de la información en una empresa Organización Internacional de Normalización (150).

ISO/IEC 27002:2013: Controles Para Seguridad de la información Organización Internacional de Normalización (150).

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones Presidencia de la Republica

Decreto 235 de 2015: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

Ley 1915 del 12 de Julio de 2018: Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos Congreso de Colombia.

Conpes 3995 de Julio de 2020: Política Nacional de Confianza y seguridad digital Consejo Nacional de Política Económica y Social.

2. ALINEACIÓN CON EL DIRECCIONAMIENTO ESTRATÉGICO

La Política de seguridad de la información de la Subred integrada de Servicios de Salud Sur ESE se articula con la Plataforma Estratégica desde el enfoque:

Misión: La Subred Integrada de Servicios de Salud Sur ESE, presta Servicios de Salud a través de un Modelo de Atención Integral en Red, bajo los enfoques de Gestión Integral del Riesgo, Seguridad, fortaleciendo la formación académica orientada a la investigación Científica e innovación, con un Talento Humano Comprometido, Humanizado y Competente que contribuya al mejoramiento de las condiciones de salud de nuestros usuarios urbanos y rurales de las localidades de Usme, Ciudad Bolívar, Tunjuelito y Sumapaz.

Visión: En el 2024 seremos una Empresa Social del Estado referente en el Distrito por la Prestación de Servicios de Salud con Estándares Superiores de Calidad, Consolidada, Sostenible, referente en investigación, Docencia e Innovación, con Enfoque Diferencial, Territorial y comunitario, que promueven el cambio, la intersectorialidad, impactando positivamente la salud y calidad de vida de nuestros usuarios.

Objetivos Estratégicos

Estratégico Nro. 1: Consolidar el Modelo de Atención Integral en Red, garantizando la prestación de Servicios Integrales de Salud, con enfoque en la gestión del Riesgo, servicios humanizados, accesibles y oportunos, impactando positivamente las condiciones de Salud de nuestros Usuarios, Familia y comunidad.

Estratégico Nro. 2: Alcanzar estándares superiores de calidad en salud, mediante la implementación de acciones progresivas que contribuyan al fortalecimiento del desempeño institucional y reconocimiento como Hospital Universitario de la Subred Sur ESE. Optimizando la atención centrada en los usuarios.

3. ENUNCIADO

La Subred Integrada de Servicios de Salud Sur ESE., se compromete a promover el uso adecuado de los recursos informáticos preservando la confidencialidad, integridad y disponibilidad de la información a través de la identificación y mitigación de los riesgos, amenazas y los impactos asociados que afecten la prestación de los servicios.

4. OBJETIVO DE LA POLÍTICA

Promover la cultura de la información para la toma de decisiones basada en hechos y datos ejecutando lineamientos de seguridad que garanticen la protección de los activos de información, preservando la confiabilidad, confidencialidad, integralidad de la información la cual, debe ser siempre protegida, cualquiera que sea su forma de ser compartida, comunicada o almacenada.

5. ALCANCE DE LA POLÍTICA

La política cubre, sin excepción, a todos los procesos de la entidad, con competencia de todos los colaboradores, personas Naturales o Jurídicas, proveedores que provean servicios o productos a la entidad.

6. DEFINICIONES

ACCESO REMOTO: Posibilidad de realizar ciertas tareas en una computadora (ordenador) sin estar físicamente en contacto con el equipo.

ACTIVO DE INFORMACIÓN: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Subred Sur ESE y, en consecuencia, debe ser protegido.

ACUERDO DE CONFIDENCIALIDAD: Es un documento en los que los colaboradores y contratistas de la Subred Sur ESE o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Subred Sur ESE, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

ATI - ADMINISTRADORES DE TECNOLOGÍAS DE INFORMACIÓN: Responsables de la administración de los equipos de cómputo, sistemas de información y redes de la Subred Sur ESE. Velan por todo lo relacionado con la utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

AUTENTICACIÓN: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

CAPACITY PLANNING: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

CENTROS DE CABLEADO: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

CENTRO DE CÓMPUTO: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

CIFRADO: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para a los repositorios de información. Prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido CRIPTOGRAFÍA: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

CUSTODIO DEL ACTIVO DE INFORMACIÓN: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el SGS1 de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la

justificación tanto de su selección corno de la exclusión de controles incluidos en el anexo A de la norma

DERECHOS DE AUTOR: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

DISPONIBILIDAD: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

DISPOSITIVOS LOT: consiste en un objeto al que se le ha dotado de conexión a Internet y cierta inteligencia software, sobre el que se pueden medir parámetros físicos o actuar remotamente y que por tanto permite generar un ecosistema de servicios alrededor del mismo.

EQUIPO DE CÓMPUTO: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

GUÍAS DE CLASIFICACIÓN DE LA INFORMACIÓN: Directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

HACKING ÉTICO: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar danos en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

IDENTIFICACIÓN DEL RIESGO: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Subred Sur, que ponen en riesgo la Confidencialidad, Integridad y Disponibilidad de los Activos de Información, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

INCIDENTE DE SEGURIDAD: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo). INGENIERÍA SOCIAL: En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

INTEGRIDAD: Es la protección de la exactitud y estado completo de los activos.

INVENTARIO DE ACTIVOS DE INFORMACIÓN: Es una lista ordenada y documentada de los activos de información pertenecientes a la Subred Sur ESE.

LICENCIA DE SOFTWARE: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MEDIO REMOVIBLE: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

PERFILES DE USUARIO: Son grupos que concentran varios usuarios con similares necesidades de

información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

PROPIEDAD INTELECTUAL: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

PROPIETARIO DE LA INFORMACIÓN: Es la unidad organizacional o proceso donde se crean los activos de información.

RECURSOS TECNOLÓGICOS: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de La Subred Sur ESE.

REGISTROS DE AUDITORIA: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de La Subred Sur ESE. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

RESPONSABLE POR EL ACTIVO DE INFORMACIÓN: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por La Subred Sur ESE ❑ de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

SISTEMAS DE CONTROL AMBIENTAL: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

SOFTWARE MALICIOSO: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

TERCEROS: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

TRABAJO EN CASA: Trabajo que se realiza en un lugar alejado de las oficinas centrales, de las instalaciones de producción o del cliente que lo contrata, mediante la utilización de las nuevas tecnologías de la información y la comunicación.

USUARIO: En el presente documento se emplea para referirse a directivos, colaboradores, contratistas,

terceros y otros colaboradores de la Subred Sur ESE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Subred Sur ESE y a quienes se les otorga un nombre de usuario y una clave de acceso.

VULNERABILIDADES: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Subred Sur ESE (amenazas), las cuales se constituyen en fuentes de riesgo.

7. DESARROLLO

La Subred Integrada de Servicios de Salud Sur E.S.E, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La protección de la información busca la disminución del impacto que se puede generar sobre sus activos, los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de valor identificados.

De acuerdo con lo anterior, esta política aplica según como se define en el alcance, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema General de Seguridad de la Información estarán determinadas por los siguientes aspectos:

Fortalecer la cultura de seguridad de la información en colaboradores, personas jurídicas o naturales, proveedores, que provean servicios o productos a la entidad, garantizando la continuidad del negocio frente a incidentes.

La Subred Integrada de Servicios de Salud Sur E.S.E, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de la Subred Integrada de Servicios de Salud Sur ESE:

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios y personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

La Subred Integrada de Servicios de Salud Sur E.S.E, protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej: proveedores o clientes), o como resultado de un servicio interno en outsourcing

La Subred Integrada de Servicios de Salud Sur E.S.E protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales

debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

La Subred Integrada de Servicios de Salud Sur E.S.E, protegerá su información de las amenazas originadas por parte del personal.

La Subred Integrada de Servicios de Salud Sur E.S.E, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La Subred Integrada de Servicios de 'Salud Sur E.S.E, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Subred Integrada de Servicios de Salud Sur E.S.E, implementará control de acceso de la información, sistemas y recursos de red.

La Subred Integrada de Servicios de Salud Sur E.S.E, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La Subred Integrada de Servicios de Salud Sur E.S.E, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La Subred integrada de Servicios de Salud Sur E.S.E, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La Subred Integrada de Servicios de Salud Sur E.S.E, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

8. NIVELES DE RESPONSABILIDAD SOBRE EL SEGUIMIENTO Y EVALUACIÓN

A partir de las líneas de defensa establecidas dentro del Modelo Integrado de Planeación y Gestión, se define las siguientes responsabilidades con respecto a la gestión, seguimiento y evaluación:

Línea Estratégica: A cargo de la Gerencia: define el Marco General de la Política y supervisa su cumplimiento.

Primera línea de defensa: jefe sistemas de información TICS, su rol principal es divulgar e implementar la política de Seguridad de la información, realizar seguimiento a las acciones definidas desde el autocontrol, además del diligenciamiento de la autoevaluación en el marco del Modelo Integrado de Planeación y Gestión.

Segunda línea de defensa: Oficina Asesora de Desarrollo institucional, su rol principal es realizar el monitoreo a la implementación de la política, medición de indicadores, evaluar la implementación de las estrategias y gestión de la primera línea.

Tercera línea de defensa: A cargo de la Oficina de Control Interno, quien provee una evaluación objetiva y de aseguramiento a la entidad a través del proceso de auditoría interna sobre la efectividad de las políticas, su implementación y la adecuada operación del Sistema de Control Interno.

9. INDICADORES

OBJETIVO QUE SE DESEA ALCANZAR CON EL CUMPLIMIENTO DE LA POLÍTICA	METAS PARA DAR CUMPLIMIENTO AL OBJETIVO ESPECÍFICO DE LA POLÍTICA	INDICADOR DE EVALUACIÓN		
		NOMBRE DEL INDICADOR	FÓRMULA	PERIODICIDAD DE MEDICIÓN
Realizar seguimiento, monitoreo y evaluación a las actividades definidas en el Plan *de* Seguridad de la información.	Cumplir mayor o igual 90% de las actividades definidas en el plan Seguridad de la Información.	Porcentaje de cumplimiento del Plan de Seguridad de la Información	Número de actividades ejecutadas de acuerdo al cronograma definido / Total de actividades programadas *100	Trimestral

10. PUNTO DE CONTROL

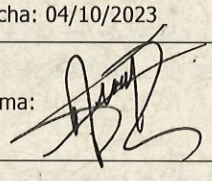
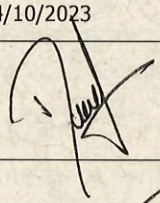
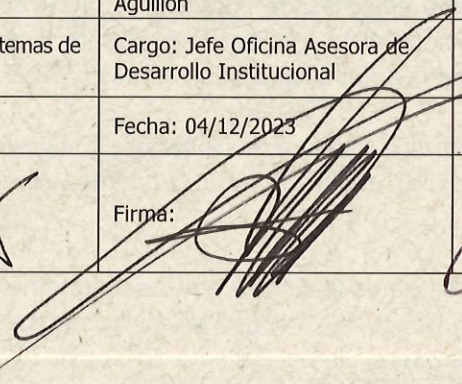
Seguimiento de los indicadores de acuerdo a su periodicidad a través de la mesa Acreditación Gerencia de la Información Comité Seguridad de la Información.

11. RESPONSABLE

Jefe de Oficina Sistemas de Información TICS.

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	05/11/2019	Articulación con los lineamientos de MIPG.
2	27/07/2021	Articulación con la Plataforma estratégica 2020-2024, Inclusión de los controles definidos por el Ministerio de las Tics. Definición de los indicadores que soportan el plan de Seguridad de la Información.
3	04/10/2023	Actualización de la normativa y enfoque del objetivo de la política de seguridad.

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrés Felipe Cubillos García	Nombre: Diana Carolina Ussa Ruiz	Nombre: Gloria Libia Polania Aguillón	Nombre: Luis Fernando Pineda Ávila
Cargo: Profesional especializado seguridad informática e información	Cargo: Jefe Oficina Sistemas de Información TIC	Cargo: Jefe Oficina Asesora de Desarrollo Institucional	Cargo: Gerente
Fecha: 04/10/2023	Fecha: 04/10/2023	Fecha: 04/12/2023	Fecha: 04/12/2023
Firma: 	Firma: 	Firma: 	Firma: