República de Colombia

Gobernación de Santander

GUÍA PARA EL MANEJO Y SEGURIDAD DE LA INFORMACIÓN

Versión	Elaboración	Revisión Técnica	Revisión de Calidad
0	Lenith Granados Acuña	-	-
1	Diana Gabriela Medina	-	Alejandra Galvis Vargas

TABLA DE CONTENIDO

1 OBJETIVO

Establecer lineamientos para la implementación de estrategias de manejo y seguridad de la información con el fin de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los activos de información del Laboratorio Departamental del Salud Pública LDSP alineado a las políticas de la Gobernación de Santander.

2 ALCANCE

Aplica a todos los activos de información relacionados con los procesos del LDSP, así como a los funcionarios, contratistas, proveedores y demás partes interesadas, que en el ejercicio de sus funciones tengan relación con la información institucional sin importar su formato de presentación o medio de almacenamiento.

3 TERMINOS Y DEFINICIONES

Establecer las normas que se deben cumplir en cuanto a la clasificación, manejo y etiquetado de la información, con el fin de asegurar que reciba el nivel de protección adecuado de la información de Laboratorio de Salud Departamental de Santander.

Tabla 1: tabla definiciones

Activo	Cualquier cosa que tenga valor para la organización. [ISO/IEC 13335-1:2004].
Activo de Información	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, hardware, software, sistemas de información, edificios, personas, imagen, etc.) que tenga valor para el Ministerio de Ambiente y Desarrollo sostenible.
Confidencialidad	Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].
Control	Medida que modifica el riesgo. [ISO/IEC 27000:2018]. 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.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2018].

4 RESPONSABILIDADES

Coordinador del LDSP

- El coordinador del laboratorio debe realizar la gestión para que el laboratorio cuente con personal idóneo que pueda gestionar, controlar, verificar y ejecutar las actividades del presente documento.
- El coordinador debe asignar a una persona como responsable de Gestión de la información, que lidere la implementación de las actividades descritas en el presente documento, y debe velar siempre apuntando a una mejora continua.

Responsable de Gestión de la información

- Liderar la implementación de las actividades descritas en el presente documento.
- Revisar periódicamente el estado general de la seguridad de la información, mínimo una vez al año.
- Mantener comunicación periódica con el área de Tecnologías de Información y Comunicación (TIC's)
- Propender por el mantenimiento y fortalecimiento de la red digital del laboratorio.
- Revisar y monitorear los incidentes de seguridad de la información.
- Concertar las medidas o controles de seguridad en el procesamiento de la información.

- Atender la solicitud oportunamente a las solicitudes de asistencias técnicas y mantenimiento.

5 GENERALIDADES

El Laboratorio Departamental De Salud Pública de Santander utilizará la información suministrada única y exclusivamente para los fines indicados, por lo tanto, salvaguardará las bases de datos que contenga la información recolectada, y no permitirá el acceso a personal no autorizado, salvo las excepciones constitucionales y legales vigentes y aplicables sobre la materia.

En ese sentido tomará todas las precauciones y medidas necesarias para garantizar la reserva de la información, de conformidad con el principio de confidencialidad que trata la Ley 1581 de 2012, y demás información vigente sobre la materia. De igual manera el titular asiste los derechos que le otorga la normatividad aplicable y vigente respecto a la protección de datos y el derecho a la información.

6 DESARROLLO DE LA GUÍA

6.1 Activos de información

El LDSP debe identificar sus activos de información y para ello se debe tener en cuenta el procedimiento de Gestión de riesgos de seguridad digital de la Gobernación de Santander.

Actividad	Frecuencia	Responsable	Soporte
Identificar activos de información de las diferentes áreas del LDSP y actualizar el inventario de activos de información, y realizar su valoración de criticidad	Anual	Líderes de áreas del LDSP Responsable de Gestión de la Información del LDSP	Inventario de activos de información

6.2 Comunicaciones internas y externas

Las comunicaciones externas a la infraestructura de la entidad deben realizarse por canales seguros que garanticen la confidencialidad de los datos de acceso y la comunicación que se transfiere

6.2.1 Correos electrónicos institucionales

El LDSP cuenta con correos institucionales para cada una de las áreas del laboratorio con listado de correos institucionales de las diferentes áreas de laboratorio, y establece un sólo responsable asignado para cada correo.

Todos los correos institucionales deben estar asociados al correo principal del laboratorio como correo de recuperación de cuenta y/o informe de actividad inusual.

Las claves que sean asignadas a un correo deberán tener una seguridad alta por lo cual se establece que debe conformarse de mínimo 6 caracteres y estos deben contener mínimo una letra mayúscula, un carácter numérico, y un carácter especial diferente a letra o número.

Actividad	Frecuencia	Responsable	Soporte
Realizar asignación de correo electrónico institucional al funcionario asignado como responsable de su manejo.	Cada vez que se deba asignar o reasignar la responsabilidad del manejo de un correo institucional	Coordinador del LDSP Responsable de Gestión de la Información del LDSP	Control de equipos, claves y correos

Actividad	Frecuencia	Responsable	Soporte
Hacer entrega de correo institucional a funcionario que lo manejará. Si más de una persona debe acceder al correo, todas deben quedar registradas para su uso.	Cuando se asigne un correo a un responsable. Cuando ingrese un nuevo funcionario	Responsable de Gestión de la Información del LDSP con autorización previa del Responsable técnico del área o Coordinador del LDSP	Control de entrega y recepción de sistemas de información
Realizar cambio de clave de correo institucional, e informar al responsable de sistemas de información del LDSP, y realizar registro del cambio realizado.	Semestral Máximo Cada vez que el encargado de un correo abandone la institución temporal o definitivamente Cada vez que se comprometa o sea vulnerable la seguridad de la información del correo Cuando se traslade la responsabilidad a otro funcionario	Responsable del correo Responsable de Gestión de la Información del LDSP	Control de equipos, claves y correos
Hacer devolución de correo institucional y entregar la información al responsable de Gestión de la Información del LDSP	Cuando el responsable de un correo abandone la institución temporal o definitivamente Cuando se traslade la responsabilidad a otro funcionario	Responsable del correo	Control de entrega y recepción de sistemas de información

6.2.2 Correos electrónicos externos autorizados

Para el envío de informes de resultados y/o de información de interés a la red de laboratorios del Departamento de Santander y usuarios relacionados, el laboratorio cuenta con correos electrónicos que han sido previamente autorizados por cada una de las instituciones, por el período de un año, los cuales serán de preferencia institucionales.

Actividad	Frecuencia	Responsable	Soporte
Realizar solicitud de autorización de correo para envío de información a través de medios oficiales.	Anual	Líderes de área de laboratorio	Formulario de solicitud Correo electrónico
Actualizar listado de correos electrónicos autorizados del LDSP.	Anual	Líderes de área de laboratorio Responsable de Gestión de la Información del LDSP	Consolidado de correos autorizados para el manejo de la información

6.3 Control y seguridad de la información

6.3.1 Control de acceso a la información

El laboratorio Departamental de Salud Pública, buscando garantizar un adecuado control de acceso a sus activos de información, implementa mecanismos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y asignación de privilegios de acceso a los sistemas.

El laboratorio cuenta con red Wifi para el laboratorio, y otra para invitados con el fin de evitar el acceso de personas externas a la red de información del LDSP.

Con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la entidad, el responsable de Gestión de la Información del LDSP deberá conceder y restringir permisos para acceder, modificar, borrar o ejecutar actividades en los archivos, aplicativos y carpetas digitales con información sensible, así como otorgar el acceso a correos y equipos de cómputo, de acuerdo a directrices de la coordinación del laboratorio.

Para conceder permisos y accesos debe considerarse las obligaciones y responsabilidades de la persona a la cual se le otorgarán, ya que esto debe concordar con el rol que desempeña dentro del laboratorio.

El LDSP mantiene la confidencialidad de la información recibida, creada, y/o generada de acuerdo a la Guía para la gestión del riesgo de imparcialidad y la confidencialidad, en la cual se establece que todo personal que ingrese al laboratorio debe firmar un Acta de confidencialidad.

El responsable de Gestión de la Información del LDSP será el encargado de bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software o control que mejor se ajuste a la necesidad.

6.3.2 Claves de equipos y sistemas de información

El laboratorio cuenta con equipos informáticos físicos (hardware), en los cuáles se conserva la información digital recibida y generada. Estos equipos deben, siempre que sea posible, tener acceso restringido a través de claves; para ellos el Responsable de Gestión de la información del LDSP deberá crear usuarios, y establecer accesos con claves en estos equipos.

Así mismo, las bases de datos de resultados de análisis solo podrán permitir el acceso a través de una clave.

Se deben asignar responsables de cada equipo informático, usuario, aplicativo y/o base de datos de acuerdo a las directrices dadas por la coordinación del laboratorio.

Si los usuarios y claves son asignadas por una entidad externa, por ser un aplicativo o base de datos externa, ésta también deberá ser contemplada dentro de los sistemas de información del laboratorio para su control.

Actividad	Frecuencia	Responsable	Soporte
Realizar asignación de usuario, equipo, aplicativo y/o base de datos al funcionario que se designe como responsable de su manejo.	Cada vez que se deba asignar o reasignar la responsabilidad del manejo de un correo institucional, por salida de la entidad, cambio de cargo o rol, o desistimiento.	Coordinador del LDSP Responsable de Gestión de la Información del LDSP	Control de equipos, claves y correos
Hacer entrega de usuario, equipo, aplicativo y/o base de datos a funcionario que lo manejará. Si más de una persona debe acceder, todas deben quedar registradas para su uso.	Cuando se asigne a un responsable. Cuando ingrese un nuevo funcionario al área	Responsable de Gestión de la Información del LDSP con autorización previa del Responsable técnico del área o Coordinador del LDSP	Control de entrega y recepción de sistemas de información
Realizar cambio de clave usuario, equipo, aplicativo y/o base de datos, e informar al responsable de sistemas de información del LDSP, y realizar registro del cambio realizado.	Semestral Máximo Cada vez que el encargado abandone la institución temporal o definitivamente Cada vez que se comprometa o sea vulnerable la	Responsable del correo Responsable de Gestión de la Información del LDSP	Control de equipos, claves y correos

	seguridad de la información. Cuando se traslade la responsabilidad a otro funcionario		
Hacer devolución de clave usuario, equipo, aplicativo y/o base de datos y entregar la información al responsable de Gestión de la Información del LDSP	Cuando el responsable de un correo abandone la institución temporal o definitivamente Cuando se traslade la responsabilidad a otro funcionario	Responsable del correo	Control de entrega y recepción de sistemas de información

6.3.3 Copias de seguridad (Back up) de la información digital

Con el fin de disminuir los riesgos de pérdida de los activos de información ubicada en los equipos de cómputo, el laboratorio realiza copias de seguridad de la información de cada una de las áreas de laboratorio.

Actividad	Frecuencia	Responsable	Soporte
Realizar back up (copia de seguridad) de bases de datos de las áreas y carpetas con informes de resultados, en el servidor del laboratorio.	Mínimo dos veces por semana	Líderes de área de laboratorio Responsable de Gestión de la Información del LDSP	Reporte registro de back up base de datos LDSP
Realizar segundo back up de respaldo en disco duro externo con el fin de salvaguardar la información de riesgos en los equipos internos del laboratorio	Semanal	Responsable de Gestión de la Información del LDSP	Reporte registro de back up base de datos LDSP

6.3.4 Verificación de fórmulas y cifras significativas

Se hace necesario que el laboratorio verifique que la formulación de hojas de cálculo utilizadas para establecer los valores de un resultado de análisis es correcta, y no genera errores en el parámetro que se mide. Igualmente es importante el manejo de correctas cifras significativas en las bases de datos, con el fin de dar buen manejo a la incertidumbre de los resultados.

Actividad	Frecuencia	Responsable	Soporte
Verificación de fórmulas en hojas de cálculo utilizadas para emisión de resultados de análisis.	Mensual	Líderes de área de laboratorio	Consolidado de verificación de fórmulas y bases de datos
Verificación de uso de cifras significativas en bases de datos para emisión de resultados de análisis.	Mensual	Líderes de área de laboratorio Responsable de Gestión de la Información del LDSP	Consolidado de revisión de fórmulas y bases de datos

6.3.5 Mantenimiento y soporte de Hardware y Software

El laboratorio debe contar con un programa de mantenimiento para los equipos informáticos donde se manipule y guarde información, así como aquellos que sirvan de respaldo para el funcionamiento de los equipos (estabilizadores, UPS, etc.), y que sean propiedad de la entidad departamental. Dentro de este mantenimiento se debe contemplar la revisión y mantenimiento, así como instalación y eliminación de programas de software, así como gestionar la protección antivirus de equipos que lo requieran.

Cuando un funcionario del laboratorio requiera soporte en hardware y/o software que se encuentre en las competencias de los ingenieros y técnicos de sistemas que se encuentran dentro del laboratorio, este deberá ser solicitado a través correo electrónico o verbalmente, y la ejecución del soporte deberá ser diligenciada en el formato de Reporte de servicio de mantenimiento preventivo y correctivo de equipos de cómputo

Actividad	Frecuencia	Responsable	Soporte
Definir el programa de mantenimiento de los equipos del LDSP	Anualmente	Responsable de Gestión de la Información del LDSP	Programa de mantenimiento de los equipos informáticos
Realizar mantenimiento preventivo y/o correctivo (si es requerido y se tiene personal con la competencia)	Según lo establecido en el programa de mantenimiento.	Responsable de Gestión de la Información del LDSP Coordinador LDSP	Informe de mantenimiento de equipos
Realizar soporte de Equipos de cómputo u otros informáticos relacionados	Según sea requerido	Ingenieros y/o técnicos de sistemas o informáticos	Reporte de servicio de mantenimiento preventivo y correctivo de equipos de cómputo

Cuando un equipo requiera intervenciones que deban ser realizadas por personal externo, el responsable de Gestión de la Información del LDSP deberá informar a la coordinación del laboratorio esta necesidad para ser incluida en el presupuesto anual de compras, y la gestión necesaria para cumplir con el programa de mantenimiento.

Todos los productos de Software que se adquieran e instalen en los equipos de cómputo de la entidad deben contar con su respectiva licencia de uso.

6.4 Reportes de resultados

A través de los sistemas de información que se manejan en el laboratorio, se generan reportes de resultados, y a partir de ellos se consolidan estadísticas, que tienen importancia en la vigilancia epidemiológica del Departamento. Esta información generada en el laboratorio es comunicada así

6.4.1 Manejo y transferencia de información de vigilancia por laboratorio de los eventos de interés en salud pública y vigilancia y control sanitario

INFORMACIÓN	MÉTODOS DE COMUNICACIÓN,	SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN
Boletines Epidemiológicos, Circulares, lineamientos técnicos departamentales	De acuerdo al comportamiento de eventos de interés en Salud Pública priorizados, se realiza cruce de información de bases de datos entre el grupo de epidemiologia y demografía y el Laboratorio Departamental de Salud pública, se verifica concordancia en notificación de casos y resultados de laboratorios y se valida información a ser incluida en boletines epidemiológicos, circulares, lineamientos, que incluya algoritmos, casos confirmados por laboratorio, vigilancia virológica, centinela, etc.	La información se verifica con personal autorizado del grupo de epidemiologia y demográfica, el envío de bases, reportes de laboratorio e información se hace a través de correos institucionales a correos autorizados.
Estudios de Vigilancia Epidemiológica.	En caso de realizarse estudios de vigilancia epidemiológica a nivel territorial o nacional, el laboratorio suministrará información necesaria a los interesados, entre ellos el grupo de epidemiológica y	Deberá contar con autorización del responsable de la dirección, coordinador del laboratorio, la información se suministrará

INFORMACIÓN	MÉTODOS DE COMUNICACIÓN,	SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN
	demografía del Departamento de Santander, Instituto Nacional de Salud e INVIMA.	a través de correos institucionales a correos autorizados, en caso de que aplique se deberán firmar actas de confidencialidad de la información.
Comité de Vigilancia epidemiológica (COVE)	El laboratorio participa en COVES departamentales o municipales (según aplique), realizando presentación de la vigilancia por laboratorio, protocolos, algoritmos, casos confirmados por laboratorio, instituciones y municipios participantes en programas de control de calidad con el LDSP.	La información se consolida y analiza, para presentación al personal autorizado en el COVE.
Eventos de interés en Salud Pública y Control Sanitario	El laboratorio comunica los resultados de análisis de acuerdo a lo descrito en el procedimiento para la emisión de resultados para diagnóstico, vigilancia y/o control de calidad, se realiza cruce de información de bases de datos entre el grupo de epidemiologia y demografía y el Laboratorio Departamental de Salud pública, se verifica concordancia en notificación de casos y resultados de laboratorios y se valida información de eventos priorizados, en el caso de información de vigilancia y control sanitario se remiten resultados al grupo de salud ambiental de la Secretaria de Salud de acuerdo a oportunidad de entrega de resultados establecida y se valida cargue de información en SIVICAP. Los eventos definidos como resultados de alerta son notificados inmediatamente al personal responsable de la UPGD, municipio, Secretaría de Salud, INS o INVIMA según aplique.	La información se verifica con personal autorizado del grupo de epidemiologia y demográfica, el envío de bases, reportes de laboratorio e información se hace a través de correos institucionales a correos autorizados.
Proyectos de Investigación de eventos de interés en salud pública, vigilancia y control sanitario	El laboratorio gestiona propuestas con la participación de otras áreas de la Secretaría de Salud, grupos de investigación de instituciones o universidades de acuerdo a temas de interés, con el fin de generar información para la toma de decisiones en salud pública.	Se debe contar con autorización por parte del Director, Secretario de Salud o Gobernador (según aplique). Se definirá alcance y participación del LDSP, criterios de seguridad y confidencialidad de información, consentimientos informados para participación en investigación y reconocimiento de créditos en publicaciones y artículos emitidos.

6.4.2 Modificación de resultados

Ya emitidos los reportes de resultados, es posible encontrar que se cometieron errores. Los informes de resultados no son susceptibles de cambios y/o modificaciones, sin previa autorización, por lo tanto, se establece:

Cargo, Rol y/o Responsabilidad	Autorización
Analista de área	Reportar resultados. No está autorizado para modificaciones a reportes de resultados.
Responsable técnico de área	Realizar cambio en reportes de resultados, o solicitar a aplicativos externos el cambio, previa comunicación al coordinador del LDSP

6.5 Recomendaciones a los usuarios de sistemas de información

6.5.1 Uso de Correo electrónico institucional

- Es responsabilidad del usuario realizar constantemente la depuración de su correo electrónico, tanto a los correos enviados como los recibidos y los que se encuentran en la papelera de reciclaje.
- Ningún usuario debe permitir a otro usuario enviar correos electrónicos utilizando su cuenta. Las cuentas asignadas son únicas e intransferibles. Cada servidor público o contratista es responsable del alcance de las acciones o uso de cada una de ellas.
- El mantenimiento del buzón de correo electrónico y la lista personal de direcciones de correo en cada computador, será responsabilidad del usuario.
- La cuenta de correo electrónico institucional asignada al usuario, sólo podrá ser utilizada para el desempeño de las funciones en la entidad en el marco del cumplimiento de los objetivos institucionales.
- Los mensajes y la información contenida en los buzones de correo electrónico, así como los archivos adjuntos, son propiedad laboratorio Departamental de Salud Pública de Santander y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones laborales.
- No se debe utilizar la dirección de correo electrónico de la organización, como punto de contacto en redes sociales, comerciales o cualquier otro sitio que no esté directamente relacionado con las actividades laborales.
- No está permitido crear o enviar cadenas de correo electrónico, mensajes con contenido religioso, político, racista, pornográfico, publicitario no institucional, o que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promuevan cualquier partido político, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, sin que los mismos estén autorizados a ser tratados, por los titulares de la información de conformidad con Ley 1581 de 2012, y demás normas que las adicionen, aclaren y modifiquen.
- No está permitido el envío de archivos que contengan extensiones ejecutables (aplicaciones, apk, instaladores).
- No está permitido el envío de archivos de música y videos exceptuando la necesidad de suplir comunicaciones institucionales.
- La información enviada como resultados, diagnósticos, información sobre visitas técnicas a terceros debe estar relacionada con correos autorizados para remitir información, que son propiedad laboratorio Departamental de Salud Pública de Santander.

6.5.2 Uso adecuado del Software

Los usuarios no deben efectuar ninguna de las siguientes actividades:

- Copiar software licenciado de la institución para utilizar en sus computadores personales o en cualquier tipo de dispositivo diferente a los autorizados por el LDSP o la Gobernación de Santander, cualquiera sea su ubicación.
- Intentar instalar un software no autorizado, en cualquier computador o servidor de la organización, sin autorización.
- Introducir programas maliciosos en las redes o a los servidores (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, phishing, pharming, ataques DDOS, keyloggers o cualquier otro tipo de malware).

6.5.3 Uso de equipos

- Ubicar el equipo en un área donde la conexión al suministro eléctrico sea regulada y tanto el cableado como la ubicación del mismo no represente riesgo de accidente al personal o afectación del equipo.
- No trasladar el computador sin la autorización de coordinación del LDSP.
- Ubicar el computador sobre escritorios y muebles estables, especialmente diseñados para ello.
- Asesorarse debidamente para garantizar una correcta conexión a la red eléctrica. La energía de corriente eléctrica regulada (110 voltios y con polo a tierra) se identifica por las tomas de color naranja.
- Apagar los equipos de cómputo al momento de terminar las labores diarias, incluidos los monitores, las impresoras y escáneres.
- No colocar ganchos, clips, bebidas y comida encima del equipo, que puedan caer accidentalmente dentro del equipo y dañar sus partes.
- No fumar cerca a los equipos de cómputo.
- Utilizar los tamaños adecuados de papel según los requerimientos de las impresoras, no forzar las bandejas de papel o los rodillos después de un atasco.
- No romper los sellos de garantía para acceder y reparar los equipos por cuenta propia. Siempre solicitar el servicio de soporte a través de los medios autorizados.
- No permitir el uso de los equipos a personas ajenas al proceso, salvo con autorización del superior inmediato o para actividades de soporte, mantenimiento y revisión realizadas por el responsable de Gestión de la información o asignado.

A medida que se avance en la mejora del sistema de seguridad de la información, se deberá garantizar una comunicación eficiente con el área de Tecnologías de Información y Comunicación (TIC´s) de la Gobernación de Santander, con el fin de acoplar los sistemas de información y gestionar mejores estrategias de respaldo de la información.

Esta guía debe ser revisada anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

7 CONTROL DE CAMBIOS

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**APROBÓ**
0	13/12/2019	Emisión inicial del documento	Sandra Bayona Vergel **Coordinador Grupo LDSP** Javier Orejarena Pinilla **Director de Salud Integral**	Luis Alejandro Rivera Osorio **Secretario de Salud de Santander**
1	29/08/2023	Actualización total del documento	Alba Rocío Orduz Amézquita **Líder Grupo LDSP** German Eduardo Marín Cárdenas **Director de Salud Integral** Diego Sánchez Báez **Coordinador Grupo de Apoyo a la Gestión y Calidad** César Ernesto Sánchez Aranda **Director de Planeación y Mejoramiento en Salud**	Javier Alonso Villamizar Suarez **Secretario de Salud de Santander**

Versión	Elaboración	Revisión Técnica	Revisión de Calidad
0	Lenith Granados Acuña	-	-
1	Diana Gabriela Medina	-	Alejandra Galvis Vargas