

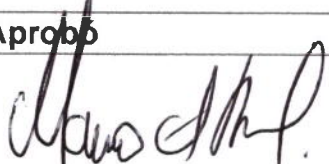
	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 1 de 16	

POLÍTICA DE DESARROLLO E IMPLANTACION DE LOS SISTEMAS DE INFORMACION



SERVICIUDAD E.S.P
DOSQUEBRADAS

Elaboró	Revisó	Aprobó
 Harrison González Santa Técnico grado 3 sistemas	 Wilson Arias Castaño Profesional especializado	 Mauricio Andrés Rodas T Subgerente Planeación (e)
Fecha: 26/11/2021	Fecha: 29/11/2021	Fecha: 29/11/2021



	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implementación de los Sistemas de Información	Página 2 de 16	

TABLA DE CONTENIDO

INTRODUCCIÓN	2
1. DEFINICIONES	3
2. NORMATIVIDAD RELACIONADA	4
3. OBJETIVO	5
4. ALCANCE DE LA POLÍTICA	6
6. ARQUITECTURA DE REFERENCIA	8
7. ELEMENTOS DE LA POLÍTICA	10
7.1. POLÍTICA DE DESARROLLO E IMPLANTACIÓN DE LOS SISTEMAS DE INFORMACIÓN	10
7.1.1. Política de ejecución de proyectos de TI.....	10
7.1.2. Política de liberación y despliegue.....	11
7.2.3 Validación y pruebas del servicio.....	13
7.2. POLÍTICAS GENERALES PARA EL DESARROLLO DE SISTEMAS DE INFORMACIÓN	14
SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA	17
CONSIDERACIONES FINALES	18

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 3 de 16	

INTRODUCCIÓN

El desarrollo e implantación de sistemas de información, deben ser las etapas primordiales para identificar, documentar y aprobar los diferentes requerimientos que se detallan durante la ejecución e implementación de proyectos tecnológicos especialmente de software en SERVICIUDAD E.S.P, por lo cual se deben gestionar canales de comunicación adecuados con proveedores y desarrolladores de los sistemas de información contratados a la medida o alquilados, para realizar adecuadamente el proceso de ejecución de proyectos, validación y pruebas del diseño del proyecto y su liberación y despliegue, lo cual permitirá una adecuada operación de los sistemas de información y su ubicación dentro del catálogo de servicios de TI.

1. DEFINICIONES

Política: Instrucciones mandatorias que indican la intención de la alta gerencia respecto a la operación de la organización.


Procedimiento: Documento que contiene las fases secuenciales donde se describe detalladamente cómo se lleva a cabo una actividad determinada.

Recurso Informático: Elementos informáticos (base de datos, sistemas operativos, redes, sistemas de información y comunicaciones, equipos computacionales) que facilitan servicios informáticos.

Proyecto tecnológico: Creación, modificación o adaptación de un producto específico o servicio gracias al empleo de la tecnología. El producto tecnológico, que es el resultado del proceso, tiene como función satisfacer una necesidad, demanda o servicio.

Sistema de información: Es el conjunto de instrucciones, órdenes y reglas que un equipo de cómputo debe ejecutar, orientados al tratamiento y administración de datos e información. El concepto de *software* abarca todo lo intangible en una computadora o lo que no es físico ni se puede tocar. Ejemplos de *software* son los programas de computación o sistemas operativos de los equipos de cómputo.

Usuario: Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que utilicen recursos informáticos para desarrollar sus funciones y actividades asignadas.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 4 de 16	

Liberación y Despliegue: Es una etapa que mediante procedimientos estandarizados permite desplegar nuevos servicios tecnológicos o modificaciones a los servicios tecnológicos existentes en producción de manera segura y confiable.

2. NORMATIVIDAD RELACIONADA

LEY 1273 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.

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

Ley 44 de 1993: por la cual se modifica y adiciona la ley 23 de 1982 "Sobre los Derechos de Autor" y se modifica la ley 29 de 1944.


Decreto 1008 de 2018: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

3. OBJETIVO

Definir las directrices para el diseño e implantación de los Sistemas de Información desarrollados por la Oficina de TI, contratados a la medida o alquilados, como soporte de las capacidades de TI de SERVICIUDAD E.S.P

4. ALCANCE DE LA POLÍTICA

Las políticas definidas en el presente documento aplican a todos los colaboradores de SERVICIUDAD E.S.P, incluyendo contratistas, practicantes universitarios, aprendices SENA y otras personas relacionadas a terceras partes, que utilicen recursos informáticos de la Entidad.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 5 de 16	

5. PRINCIPIOS DE LA POLÍTICA

Los principios definidos para la Política de Implantación y Desarrollo de los sistemas de Información de **SERVICIUDAD E.S.P** son los siguientes:

Responsabilidad: Todos los usuarios, sin excepción, son responsables por los accesos, acciones y demás situaciones que se realicen en los diferentes sistemas de información donde se implique el uso de código de usuario y contraseña, así como en el uso de las cuentas de correo electrónico corporativo.

Cumplimiento: Es deber de los usuarios acatar las normas, procedimientos administrativos y técnicos establecidos por la Entidad para el uso de los sistemas de información, así como la aplicación de las instrucciones para la protección de la información.


Ética: Se debe mostrar y aplicar una buena conducta en la utilización de los sistemas de información, los cuales han sido destinados únicamente para los servicios prestados por la Entidad, respetando la propiedad intelectual del software, diseños e información, como también el adecuado uso de la información contenida en ellos.

Propiedad: La Entidad es la propietaria de todos los recursos informáticos instalados y entregados a los usuarios para su utilización, entre los que se destacan los siguientes: computadores de escritorio y/o portátiles, dispositivos móviles (celular Smartphone, Tablet, entre otros), correo electrónico y la información resultante en los servicios prestados sobre ellos.

Vigilancia: La Entidad se reserva el derecho de vigilar el uso de los recursos informáticos y acceder a la información contenida en los mismos de ser necesario, procurando la no violación de las normas y principios establecidos por la organización, en especial la información que no tenga relación con las funciones inherentes al cargo del usuario o aquella que no esté debidamente autorizada para su acceso, la cual podrá ser retenida por la Entidad en caso de ser hallada durante una revisión.

6. ARQUITECTURA DE REFERENCIA

Para el desarrollo e implantación de los sistemas de información, todo proyecto deberá ser basado en la Arquitectura de Referencia de la AE diseñada para **SERVICIUDAD E.S.P**, en la cual se determinan los parámetros y estándares de TI necesarios para que los sistemas diseñados sean implantados apropiadamente en la infraestructura de TI de la Entidad.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 6 de 16	

COMPONENTE	DESCRIPCIÓN
Usabilidad y Accesibilidad	Los sistemas de información de SERVICIUDAD E.S.P deben cumplir con el Manual de usuario y Accesibilidad definido para tal fin
Arquitectura	Los sistemas de información de SERVICIUDAD E.S.P deben estar desarrollados bajo las capas de presentación (Esta capa reúne todos los aspectos del Software que tiene que ver con las interfaces y la interacción con los diferentes tipos de usuarios humanos, incluyen el manejo y aspecto de las ventanas, el formato de los reportes, menú, gráficos y elementos multimedia en general.) y la capa de repositorio (Esta capa reúne todos los aspectos del software que tienen que ver con el manejo de los datos persistentes, por lo que también se le denomina la capa de las Bases de Datos)
Documentación	La documentación mínima que debe contener un sistema de información debe estar alineada con la Metodología de referencia para el desarrollo de sistemas de información.
Tecnologías	<p>Los sistemas de información desarrollados para SERVICIUDAD E.S.P deben utilizar tecnologías estándar y ampliamente difundidas en el mercado.</p> <p>Aplicaciones</p> <p>Lenguajes de programación:</p> <p>Android Studio</p> <p>HTML5</p> <p>Java</p> <p>Delphi</p> <p>php</p>



SERVICIUDAD E.S.P

Código
SPOT 32


Versión
01

Política de Desarrollo e
implantación de los Sistemas de
Información

Página 7 de 16

	Servicios WEB:
	php
	HTML5
	Datos:
	Firebird
	MYSQL
Trazabilidad de los sistemas de información	<p>Los sistemas de información deben manejar los siguientes niveles de trazabilidad:</p> <ul style="list-style-type: none"> · Auditoria a nivel de base de datos: El usuario de acceso a la base de datos configurado en el sistema de información desarrollado, debe tener un registro de auditoria en base de datos de las acciones que realice en la misma. · Auditoria a nivel de sistemas de información: Cada sistema de información debe tener un registro de los eventos que realicen los usuarios en el sistema a través de la base de datos. Dichos eventos deben contener información acerca de las acciones ejecutadas en las diferentes funcionalidades del sistema implementadas. · Log del sistema de información: Cada sistema de información debe registrar los eventos en nivel de error que se presenten; lo anterior para realizar un seguimiento adecuado a las fallas que disminuyan la calidad de los servicios prestados. Estos logs del sistema pueden ser almacenados en archivos planos o en la base de datos.

Fuente: Ver documento Arquitectura de Referencia SERVICIUDAD.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implementación de los Sistemas de Información	Página 8 de 16	

7. ELEMENTOS DE LA POLÍTICA

La política de desarrollo e implantación de sistemas de información de SERVICIUDAD E.S.P se desarrolla bajo los siguientes elementos:


7.1. POLÍTICA DE DESARROLLO E IMPLANTACIÓN DE LOS SISTEMAS DE INFORMACIÓN

7.1.1. Política de ejecución de proyectos de TI

Todo proyecto que incluya componente tecnológico en la Entidad, deberá ser sometido a las políticas y procedimientos determinados por la Oficina de TI para su desarrollo y puesta en funcionamiento deseado. A continuación, se enuncian las directrices de necesario cumplimiento para la ejecución de proyectos:

Plan de ejecución del proyecto:

- I. Todo Proyecto de desarrollo informático estará sujeto a los estándares dispuestos por la Oficina de TI de SERVICIUDAD E.S.P y a las directrices planteadas en el presente documento.
- II. Lo dispuesto en la presente política será de observancia general y obligatoria de todas las dependencias de la Entidad que, en cumplimiento de los objetivos estratégicos, desarrollen proyectos con componentes tecnológicos.
- III. La Oficina de TI deberá determinar los recursos informáticos necesarios para llevar a cabo los proyectos con componente tecnológico que sean requeridos por la Entidad.
- IV. Los derechos de autor de todo Proyecto con componente tecnológico desarrollado con recursos propios, pertenecerán a SERVICIUDAD E.S.P, Se deben incluir dentro de los contratos con Ingenieros de Sistemas, Desarrolladores o Programadores las cláusulas que permitan verificar y controlar esto.
- V. La Oficina de TI pondrá a disposición de acuerdo a los niveles de acceso y roles, un repositorio con los expedientes de todos los proyectos a fin de ser utilizados como referencia en nuevos proyectos.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 9 de 16	


- VI. Todo Sistema informático deberá ser desarrollado atendiendo la Arquitectura de Referencia determinada en la AE de la Entidad.
- VII. Todo proyecto con componente de TI deberá ser incorporado al Catálogo de Servicios de la Oficina de TI.

Control de cambios:


- I. Todo proyecto de TI que sea sometido a cambios, deberá ser actualizado de acuerdo a: Alcance, Recursos, Cronograma, Procedimientos, Costos, Documentación, Calidad u Otros.
- II. Todo cambio deberá ser documentado según su CAUSA/ORIGEN, relacionando como mínimo: reparación o defecto, acción correctiva, acción preventiva, actualización, modificación de documento.
- III. El control de cambios deberá contener una descripción detallada y justificación de la propuesta de cambio.
- IV. Toda propuesta de cambio deberá contener las implicaciones de recursos (Materiales y Capital Humano) a utilizar, así como los Riesgos del Cambio, ya sean económicos, operativos, tecnológicos o de cumplimiento.
- V. Toda propuesta de cambio deberá informar de manera detallada el impacto del cambio: alcance, cronograma, costo, calidad.
- VI. Toda propuesta de cambio deberá ir firmada con el responsable encargado y con su compromiso frente al cambio solicitado.

7.1.2. Política de liberación y despliegue

Todo proyecto de la Entidad que tenga componente de TI, deberá ser sometido a un procedimiento de liberación y despliegue, en el cual se deberán informar aspectos como:

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 10 de 16	

- I. Todo proyecto de TI deberá ser sometido a un protocolo de despliegue y liberación, el cual deberá ser definido, documentado y registrado en el Sistema de Gestión de Calidad de la Entidad.
- II. Todo proyecto deberá contener una Lista de chequeo de liberación y despliegue.
- III. Todo proyecto de TI deberá contener una CMDB (Base de Datos de la Gestión de la Configuración) como repositorio que contiene todos los "elementos de configuración" del sistema de información o servicios de TI y sus relaciones. La CMDB deberá incluir tanto la descripción del servicio ofrecido, así como sus requerimientos de Arquitectura de TI (máquinas, servidores, routers, periféricos, etc.), personas involucradas, redes, software, documentación, proveedores, etc.
- IV. En todos los proyectos de TI se deberán documentar las lecciones aprendidas en los formatos establecidos en el Sistema de Gestión de Calidad de la Entidad determinados para tal fin.
- V. Una vez terminado el proceso de documentación de lecciones aprendidas, todo proyecto debe contener en su expediente documental, un acta de cierre del proyecto, en la cual, las partes involucradas validan y aprueban el desarrollo e implantación de los sistemas de información.
- VI. La Oficina de TI deberá emitir la liberación del Sistema informático para su puesta en el Ambiente de producción con base en el resultado de la liberación y despliegue.
- VII. La Oficina de TI deberá verificar periódicamente que existan copias útiles y actualizadas de la información que considere relevante o necesaria para la operación y recuperación de los Sistemas informáticos y que hayan sido liberados.
- VIII. La Oficina de TI deberá asegurar que los expedientes y documentación del procedimiento de liberación y despliegue, se encuentren actualizados conforme a la última versión liberada de los Sistemas informáticos.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 11 de 16	

7.2.3 Validación y pruebas del servicio

La validación y pruebas del servicio tiene como objetivo asegurar la calidad de los productos del Proyecto de desarrollo y el cumplimiento de los Requerimientos del sistema.


- I. El Plan de validación y pruebas a los sistemas informáticos deberán incluir los siguientes tipos:
 - ✓ Pruebas de código
 - ✓ Entradas y salidas
 - ✓ Funcionales o de usuarios
 - ✓ De rendimiento
 - ✓ De seguridad
 - ✓ Validación, funcionalidad y operación en el Ambiente de producción
 - ✓ Escenario
 - ✓ Caso de prueba
 - ✓ Aspecto verificado

- II. Si durante el proceso de pruebas se detecta la necesidad de realizar modificaciones que impacten en el programa de actividades, cronogramas, calendario de tareas y demás recursos definidos en la documentación entregada a la Oficina de TI, se notificará mediante el documento de control de cambios los requerimientos establecidos.

- III. El procedimiento de validación y pruebas del servicio será un documento que refiere los distintos tipos de pruebas que se aplicarán a un sistema en desarrollo, los ambientes en que se llevarán a cabo y los responsables de realizarlas y por ende hará parte integral del expediente documental del proyecto.

7.2. POLÍTICAS GENERALES PARA EL DESARROLLO DE SISTEMAS DE INFORMACIÓN

Diseño: En cuanto a los componentes de seguridad de los sistemas de información, se deben desarrollar controles y registros adecuados de trazas de auditorías, validando parámetros como:

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 12 de 16	

I. Verificación según lista de requerimientos del sistema.

II. Validación de interfaces entre sistemas cuando sea requerido.

III. Validación completa de los requerimientos funcionales y no funcionales por cada sistema de información

Integridad de comunicaciones: Cuando un sistema de información de la Entidad, realice intercambio de información con otros sistemas externos, se deben ejercer controles criptográficos¹, dispuestos por la norma ISO 27001.


Validación de Datos de Salida: Para garantizar la seguridad de la información en los SI de la Entidad, los proveedores de software deben ejercer controles sobre la salida de datos, que garanticen la verificación del resultado esperado de los requerimientos funcionales definidos para cada proyecto tecnológico de la Entidad.

Administración de Claves: Todos los sistemas de información deberán contar con mecanismos de protección de claves, que permitan asegurarlas contra acciones de modificación, destrucción y copia o divulgación no autorizada; mediante almacenamiento cifrado en las bases de datos.

Protección de los Datos de Prueba del Sistemas: Para las pruebas de los sistemas, se utilizarán datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas que contemplen lo siguiente:

- I. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.


¹ 10.1 Controles criptográficos: Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas. Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización. Sería necesario el desarrollo adicional de procedimientos y asignación de funciones respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado. El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en técnicas de descifrado. Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos y, en algunas ocasiones, podría ser necesario asesoramiento legal para establecer acuerdos especiales que respalden su uso. Tomado de: http://www.iso27000.es/iso27002_10.html

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 13 de 16	

- II. Eliminar inmediatamente, y una vez completadas las pruebas, la información operativa utilizada.
- III. Los datos del ambiente operativo en este sistema de pruebas, no deben permanecer más de un mes en pruebas. Una vez cumplido este periodo deberán ser borrados.

Control de Acceso a los Códigos Fuente: Para reducir la probabilidad de alteración de programas fuentes, se aplicarán las siguientes normas:

- I. Proveer a la Oficina de TI los códigos fuente solicitados para su modificación, manteniendo en todo momento la correlación programa fuente /ejecutable.
- II. Llevar un registro actualizado de todos los programas fuente en uso, Indicando nombre del programa, versión, fecha de última modificación, fecha/hora de compilación y estado (en modificación o en producción).
- III. Administrar las distintas versiones de un sistema de información.
- IV. Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- V. Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuente.
- VI. Realizar las copias de Seguridad y pruebas de restauración de los programas fuente, cumpliendo los requisitos de seguridad establecidos por la entidad en los procedimientos que surgen del presente documento.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 14 de 16	


Desarrollo Externo de Software: Para el caso que se considere la tercerización del desarrollo de software, se establecerán las siguientes normas:

- I. Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual transferidos a SERVICIUDAD E.S.P
- II. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- III. Garantías de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos.

7.3. DOCUMENTACIÓN CODIGO

En el de uso de los sistemas de información, se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:


- I. SERVICIUDAD E.S.P respeta los derechos de propiedad intelectual asociados con su propio hardware, software y documentación; en consecuencia, ningún usuario de sus sistemas de información ni cualquier otra persona puede reproducirlos por cualquier medio, comercializarlos o hacerlos públicos.
- II. Si los derechos de propiedad intelectual se infringen por medio de un abuso deliberado o por negligencia, la persona involucrada puede ser procesada según las leyes aplicables.
- III. Se considera como software autorizado, tanto los Sistemas Ofimáticos como Sistemas de gestión de la Entidad, los instalados por la Oficina de TI, previo visto bueno para su adquisición por el Director de la Oficina de TI y con la autorización legal del proveedor para su uso.
- IV. Toda área podrá utilizar UNICAMENTE el software que la Oficina de TI haya instalado en sus equipos de cómputo para el desarrollo de sus funciones.
- V. Toda necesidad de software adicional, debe ser solicitada por escrito a la Oficina de TI.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 15 de 16	

- VI. Todo software que utilice la Entidad será adquirido con normatividad vigente y siguiendo sus procedimientos específicos de adquisiciones.
- I. Sin excepción, no se permitirá la instalación de software sin la debida autorización y/o participación de la Oficina de TI. De hacerlo, la acción será considerada como una violación a las normas de la Entidad.
 - II. Todo el software de manejo de datos utilizado por la Entidad dentro de su infraestructura informática, deberá contar con la recomendación y/o aprobación de la Oficina de TI, siendo ésta la única responsable de su instalación y verificación del cumplimiento de las políticas de Seguridad de la Información.
 - III. Se debe socializar y sensibilizar a los usuarios sobre las implicaciones que tiene instalar software ilegal en los computadores de la Entidad, fomentando una cultura de seguridad de la Información.
 - IV. Mantener un inventario de las licencias del software instalado en la Entidad, permitiendo su adecuada administración, control y actualización, logrando de esta manera evitar posibles sanciones por instalación de software no licenciado.

SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA

- a. Cuando se trate de una falta que afecte directamente el normal funcionamiento del recurso tecnológico o infrinja leyes del ámbito jurídico, se aplicarán también todas las normas vigentes, informando por escrito al Área del usuario infractor y la Oficina de control interno Disciplinario para tomar las medidas y sanciones correspondientes.
- b. Cuando por consecuencia de una violación de las normas se suspendan privilegios de los servicios computacionales a un usuario, para reactivar los servicios la Subgerencia de área del usuario infractor debe solicitar por escrito el levantamiento de la restricción ante la Oficina de TI
- c. La reincidencia de una falta SIMPLE la convierte en GRAVE.

	SERVICIUDAD E.S.P	Código SPOT 32	Versión 01
	Política de Desarrollo e implantación de los Sistemas de Información	Página 16 de 16	

CONSIDERACIONES FINALES

Por todo lo anterior, se solicita la gestión de todos los colaboradores para conservar un ambiente seguro en los sistemas de información y recursos informáticos de la Entidad, informando de cualquier irregularidad observada en los procesos que se lleve en los sistemas de información, o al uso dado de los recursos informáticos.

SERVICIUDAD
ACUEDUCTO DE SAN CARLOS (S.A.)