

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 1 de 19
		Versión: 1

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2025

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

Iderbol [®]

VERSIÓN 1.0

**Instituto Departamental de Deporte y Recreación de Bolívar
IDERBOL**

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 2 de 11
		Versión: 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

El Instituto Departamental de Deporte y Recreación de Bolívar (IDERBOL), en cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) y las directrices establecidas en la Política de Gobierno Digital y la Política de Seguridad Digital, adopta estrategias y mecanismos que garanticen la protección, integridad, disponibilidad, confidencialidad y privacidad de la información institucional.

En el contexto de la transformación digital del sector público, la seguridad de la información se convierte en un pilar fundamental para la prestación eficiente y confiable de los servicios que ofrece IDERBOL a la ciudadanía. La implementación de un Plan de Seguridad y Privacidad de la Información responde a la necesidad de fortalecer la gestión de riesgos, establecer controles y mecanismos de prevención, y consolidar una cultura organizacional basada en la confianza digital y el uso responsable de las tecnologías de la información y las comunicaciones.

Este plan se fundamenta en normativas nacionales e internacionales, como la NTC-ISO/IEC 27001, la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1078 de 2015, el Decreto 620 de 2020 y el Esquema de Seguridad y Privacidad de la Información (ESPI) promovido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Su propósito es garantizar que los funcionarios, contratistas y terceros que interactúan con los sistemas de información de la entidad adopten las mejores prácticas en seguridad digital, minimicen los riesgos y contribuyan al fortalecimiento de la ciberseguridad institucional.

Para ello, se establecen directrices que permiten identificar amenazas, evaluar vulnerabilidades, gestionar incidentes y asegurar la continuidad de los servicios de la entidad. Asimismo, se promueve la aplicación del ciclo PHVA (Planear-Hacer-Verificar-Actuar), con el fin de garantizar el mejoramiento continuo de los procesos de seguridad de la información.

El compromiso con la seguridad y privacidad de la información no solo responde a un mandato normativo, sino que también constituye un factor clave en la consolidación de una gestión pública transparente, eficiente y confiable. La correcta implementación de este plan permitirá a IDERBOL fortalecer su gobernanza digital, proteger los datos institucionales y ofrecer servicios seguros y de calidad a la comunidad.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Garantizar la protección, integridad, disponibilidad, confidencialidad y privacidad de la información de IDERBOL mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la Política de Gobierno Digital, la Política de Seguridad Digital, el Esquema de Seguridad y Privacidad de la Información (ESPI), con el propósito de fortalecer la gestión institucional, mitigar riesgos digitales y asegurar la prestación eficiente y confiable de los servicios deportivos y recreativos en beneficio de la comunidad.

Objetivos Específicos

-

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 3 de 11
		Versión: 1

Estos objetivos contribuyen a consolidar una gestión pública moderna, segura y confiable, asegurando que IDERBOL cumpla con su misión de promover el deporte y la recreación con altos estándares de seguridad digital y protección de la información.

1.2.2. OBJETIVOS ESPECÍFICOS

- Establecer lineamientos y controles de seguridad de la información que permitan proteger los activos digitales de IDERBOL y garantizar la continuidad de los servicios institucionales.
- Implementar una cultura organizacional de seguridad digital mediante estrategias de sensibilización y formación dirigidas a funcionarios, contratistas y proveedores, promoviendo el uso responsable de las tecnologías de la información y la gestión adecuada de los datos.
- Identificar, evaluar y mitigar los riesgos de seguridad digital a través de metodologías de análisis de amenazas y vulnerabilidades, asegurando una respuesta efectiva ante incidentes de seguridad y ciberataques.
- Asegurar el cumplimiento normativo en materia de seguridad y privacidad de la información, garantizando la aplicación de las disposiciones establecidas en la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1078 de 2015, el Decreto 620 de 2020 y la NTC-ISO/IEC 27001.
- Implementar mecanismos de monitoreo y mejoramiento continuo del SGSI, mediante la aplicación del ciclo PHVA (Planear-Hacer-Verificar-Actuar), para optimizar la gestión de la seguridad digital y la resiliencia institucional frente a riesgos tecnológicos.
- Fortalecer la interoperabilidad y la gestión de datos seguros en los procesos digitales del instituto, promoviendo la transparencia y la confianza ciudadana en el uso de los servicios de recreación y deporte ofrecidos por IDERBOL.
- Desarrollar e implementar planes de respuesta y continuidad del negocio en materia de seguridad digital, garantizando la operación ininterrumpida de los sistemas de información ante eventos de riesgo o contingencias tecnológicas.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 4 de 11
		Versión: 1

1.3. JUSTIFICACIÓN

En el contexto actual de la transformación digital del sector público, la seguridad y privacidad de la información se han convertido en pilares fundamentales para garantizar la eficiencia, estabilidad y confiabilidad en la gestión institucional. IDERBOL, como entidad pública que presta servicios de recreación y deporte, depende de sistemas de información que permiten la gestión de sus procesos y la interacción con la ciudadanía, lo que hace imprescindible la implementación de mecanismos robustos de protección de datos y ciberseguridad.

La información es un activo estratégico que, al igual que otros recursos institucionales, debe ser gestionado y protegido de manera efectiva. Debido a la necesidad de estar conectados y proveer a los Bolivarenses facilidades para acceder a tramites en línea, surgen nuevas amenazas y vulnerabilidades que pueden comprometer la confidencialidad, integridad, disponibilidad y privacidad de los datos. Por esta razón, se hace necesario adoptar un enfoque preventivo y de gestión del riesgo alineado con la Política de Seguridad Digital, la Política de Gobierno Digital, el Esquema de Seguridad y Privacidad de la Información (ESPI) y normativas como la Ley 1581 de 2012, el Decreto 1078 de 2015, y el Decreto 620 de 2020.

Este plan busca establecer una línea base que permita articular los esfuerzos institucionales en materia de seguridad digital, asegurando la implementación de controles, políticas y estrategias que mitiguen los riesgos asociados a la gestión de información en las plataformas tecnológicas de IDERBOL. Se enfoca en garantizar la protección de la información en los sistemas, redes, servicios digitales y demás herramientas tecnológicas utilizadas por la entidad, minimizando vulnerabilidades y fortaleciendo la resiliencia frente a incidentes de ciberseguridad.

Además, este plan sienta las bases para la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la protección de los datos mediante la implementación progresiva de medidas de respaldo, acceso restringido, protección contra amenazas y protocolos de respuesta ante incidentes. A través de estos lineamientos, se busca no solo dar cumplimiento a la normativa vigente, sino también promover una cultura organizacional de seguridad digital en la entidad.

Los principales beneficiarios de este plan incluyen a la Gerencia General y las Subgerencias de IDERBOL, que podrá contar con información confiable y disponible para la toma de decisiones estratégicas, y a los usuarios de los servicios tecnológicos de la entidad, quienes se verán beneficiados con plataformas más seguras, ágiles y confiables en la gestión de información. De esta manera, IDERBOL refuerza su compromiso con la transparencia, la eficiencia y la seguridad digital, asegurando la prestación óptima de sus servicios a la comunidad.

1.4. ALCANCE

El Sistema de Gestión de Seguridad de la Información (SGSI) de IDERBOL abarca la implementación de medidas, controles y procesos que garanticen la protección de los activos de información institucionales, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y privacidad. Para ello, se adoptan lineamientos basados en la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022, la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1078 de 2015, el Decreto 620 de 2020, y las directrices establecidas en la Política de Seguridad Digital y la Política de Gobierno Digital.

Este plan aplica a todos los funcionarios, contratistas y terceros que interactúan con los activos de información de IDERBOL, quienes deberán conocer, cumplir y aplicar las políticas, procesos y procedimientos establecidos en el SGSI. Se establecen controles específicos para la

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 5 de 11
		Versión: 1

protección de la infraestructura tecnológica, los sistemas de información, las bases de datos y cualquier otro componente digital o físico que intervenga en la gestión de la información institucional.

Asimismo, el alcance del plan incluye la implementación de estrategias de gestión de riesgos, respuesta ante incidentes de seguridad digital, capacitación y concienciación en ciberseguridad, así como la aplicación de un enfoque de mejoramiento continuo basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

A través de este enfoque integral, IDERBOL fortalece la seguridad digital de su entorno organizacional, asegurando que la información institucional se gestione de manera segura, confiable y conforme con la normativa vigente, en beneficio de la ciudadanía y de la prestación eficiente de sus servicios de recreación y deporte.

2. MARCO CONCEPTUAL

El presente marco conceptual establece los términos y definiciones clave en el **Plan de Seguridad y Privacidad de la Información de IDERBOL**, en alineación con la **Política de Seguridad Digital** y la **Política de Gobierno Digital** del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Estas definiciones son fundamentales para la gestión de riesgos, el aseguramiento de la información y la implementación del **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en estándares internacionales como la **NTC-ISO/IEC 27001:2022**.

Aceptación del Riesgo

Decisión formal de asumir un riesgo residual dentro de los niveles aceptables definidos por la organización. Esta decisión se toma tras evaluar las medidas de mitigación y el impacto potencial sobre la operación y los activos de información.

Activo de Información

Cualquier recurso, tangible o intangible, que tiene valor para la organización y requiere protección. Esto incluye datos, sistemas de información, infraestructuras tecnológicas, documentos físicos o digitales, servicios y el conocimiento de las personas.

Alerta de Seguridad Digital

Notificación formal de un evento o incidente de seguridad que puede comprometer la confidencialidad, integridad o disponibilidad de la información y que requiere acciones inmediatas de mitigación.

Amenaza Digital

Causa potencial de un incidente de seguridad que puede ocasionar un impacto negativo en los sistemas de información, la infraestructura tecnológica o la continuidad de la operación.

Análisis de Riesgos

Proceso sistemático para identificar amenazas, vulnerabilidades y evaluar el impacto y la probabilidad de materialización de los riesgos que afectan la seguridad de la información.

Aplicaciones

Conjunto de programas o sistemas de software utilizados en la gestión de la información institucional y que deben cumplir con los estándares de seguridad digital.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 6 de 11
		Versión: 1

Autenticación

Proceso mediante el cual se verifica la identidad de un usuario, sistema o entidad antes de permitir su acceso a la información o recursos digitales.

Confidencialidad

Principio de seguridad que garantiza que la información solo esté disponible para personas, sistemas o procesos autorizados, previniendo accesos no autorizados o divulgación indebida.

Ciberespacio

Entorno digital compuesto por redes interconectadas, sistemas informáticos, dispositivos y servicios en línea donde se desarrolla la actividad digital de la sociedad, incluyendo la infraestructura tecnológica de IDERBOL.

Control de Seguridad de la Información

Medida implementada para mitigar riesgos, garantizar la protección de los activos de información y cumplir con las políticas y normativas aplicables.

Custodio del Activo de Información

Persona, cargo o unidad responsable de implementar y administrar los controles de seguridad definidos por el propietario del activo, asegurando su adecuada protección.

Datos Abiertos

Información pública, accesible y reutilizable sin restricciones, que promueve la transparencia y facilita la innovación y el desarrollo de servicios digitales.

Datos Biométricos

Información personal basada en características físicas únicas, como huellas dactilares, reconocimiento facial o voz, utilizadas para la autenticación e identificación de individuos.

Datos Personales Sensibles

Información que afecta la intimidad del titular y cuyo tratamiento indebido puede generar discriminación, incluyendo datos sobre origen racial, orientación política, religión, salud y biometría.

Disponibilidad

Propiedad de la información que garantiza que esté accesible y utilizable cuando se requiera por entidades o individuos autorizados.

Gestión de Incidentes de Seguridad Digital

Proceso estructurado para detectar, reportar, analizar y responder a incidentes de seguridad de la información, minimizando su impacto en la operación.

Gestión de Riesgos de Seguridad Digital

Conjunto de actividades para identificar, evaluar, tratar y monitorear riesgos de seguridad de la información, asegurando la continuidad de las operaciones y la protección de los activos digitales.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 7 de 11
		Versión: 1

Habeas Data

Derecho fundamental que garantiza el acceso, actualización y corrección de la información personal contenida en bases de datos, conforme a la **Ley 1581 de 2012** sobre protección de datos personales.

Incidente de Seguridad Digital

Evento inesperado que compromete la seguridad de la información y puede afectar la confidencialidad, integridad o disponibilidad de los activos digitales de la organización.

Integridad

Propiedad que garantiza la exactitud y confiabilidad de la información, evitando alteraciones o modificaciones no autorizadas.

No Repudio

Mecanismo de seguridad que impide que un usuario niegue haber realizado una acción o transacción digital, garantizando la trazabilidad y autenticidad.

Plan de Continuidad del Negocio

Estrategia que define las acciones necesarias para mantener la operación de la organización en caso de incidentes o crisis que afecten la seguridad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI)

Conjunto de políticas, procedimientos, recursos y controles implementados para gestionar la seguridad de la información de manera estructurada y alineada con la normativa vigente.

Trazabilidad

Capacidad de registrar y auditar todas las acciones realizadas sobre los activos de información, asegurando la rendición de cuentas y la seguridad en su gestión.

Vulnerabilidad

Debilidad en un sistema, procedimiento o control de seguridad que puede ser explotada por una amenaza, poniendo en riesgo la integridad de los activos de información.

3. MARCO NORMATIVO.

El **Plan de Seguridad y Privacidad de la Información de IDERBOL** se enmarca en la legislación vigente en Colombia, garantizando el cumplimiento de las normativas aplicables en materia de seguridad digital, protección de datos personales y gestión de la información. Este marco normativo se fundamenta en la **Constitución Política de Colombia de 1991**, así como en leyes y decretos que regulan la protección, acceso, uso y gestión de la información en el sector público.

Normativa General

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 8 de 11
		Versión: 1

1. Constitución Política de Colombia (1991)

Establece el derecho fundamental a la intimidad (Artículo 15), el acceso a la información pública (Artículo 20) y la obligación del Estado de garantizar la protección de los datos personales.

Normativa Específica en Seguridad y Protección de la Información

2. Ley 527 de 1999

Regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales. Define las entidades de certificación y establece disposiciones sobre la seguridad y autenticidad de la información digital.

3. Ley 594 de 2000 (Ley General de Archivos)

Reglamenta la gestión documental en entidades públicas, asegurando la conservación, acceso y organización de los documentos en formatos físicos y electrónicos.

4. Ley 603 de 2000

Obliga a las empresas a declarar en sus informes de gestión si utilizan software legal, promoviendo el respeto por los derechos de autor en el ámbito digital.

5. Ley 962 de 2005

Busca la simplificación de trámites administrativos y establece parámetros de seguridad en la información electrónica de entidades públicas, asegurando su integridad, autenticidad y confidencialidad.

6. Ley 1150 de 2007

Fortalece la seguridad de la información en los procesos de contratación pública en línea, garantizando la transparencia y protección de los datos utilizados en las plataformas de compras estatales.

7. Ley 1266 de 2008 (Ley de Habeas Data)

Regula la administración de bases de datos personales en el sector financiero, crediticio y comercial, estableciendo principios de seguridad, confidencialidad y acceso a la información.

8. Ley 1273 de 2009

Modifica el Código Penal para incluir delitos informáticos y fortalecer la protección de los sistemas que utilizan tecnologías de la información y las comunicaciones. Penaliza accesos no autorizados, interceptación de datos y daño informático.

9. Ley 1341 de 2009 (Ley TIC)

Define los principios de la sociedad de la información, regula la organización de las Tecnologías de la Información y las Comunicaciones (TIC) y establece el marco regulatorio del sector.

10. Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo)

Regula el acceso a la información pública, estableciendo principios de transparencia y mecanismos para garantizar el derecho a la información en entidades del Estado.

11. Ley 1474 de 2011 (Estatuto Anticorrupción)

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 9 de 11
		Versión: 1

Fortalece los mecanismos de control en la gestión pública, incluyendo disposiciones sobre seguridad de la información y transparencia en la administración de recursos digitales.

12. Ley 1581 de 2012 (Régimen General de Protección de Datos Personales)

Establece principios y derechos en el tratamiento de datos personales en Colombia, obligando a las entidades a implementar medidas de seguridad para la protección de la información de los ciudadanos.

13. Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública)

Regula el derecho de acceso a la información pública y establece la obligación de las entidades estatales de garantizar la disponibilidad, integridad y accesibilidad de la información.

14. Decreto 1078 de 2015

Compila y reglamenta la estrategia de **Gobierno Digital**, estableciendo directrices para la implementación de seguridad digital, gestión documental electrónica y estándares de interoperabilidad.

15. Decreto 620 de 2020

Reglamenta la seguridad de la información en entidades públicas, definiendo lineamientos para la gestión de riesgos digitales, respuesta a incidentes y protección de datos personales.

16. CONPES 3701 de 2011 (Política Nacional de Seguridad Digital y Ciberseguridad)

Establece la estrategia nacional en seguridad digital, definiendo roles y responsabilidades en la protección de infraestructuras críticas, ciberseguridad y gestión de incidentes digitales.

4. ESTRATEGIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Estrategia de Seguridad y Privacidad de la Información

La estrategia de seguridad y privacidad de la información de IDERBOL se fundamenta en la necesidad de proteger los activos digitales de la organización, alineándose con la **Política de Seguridad Digital** y el marco normativo vigente en Colombia. Su propósito es garantizar la **confidencialidad, integridad y disponibilidad** de la información, fortaleciendo los mecanismos de gestión de riesgos, cumplimiento normativo y protección de datos personales en todos los procesos institucionales.

Para lograr este objetivo, se establecerá un enfoque basado en la **gestión de riesgos** mediante la aplicación de la metodología **MAGERIT**, complementada con estándares internacionales como **ISO 27001 y el marco NIST de ciberseguridad**. Se iniciará con un diagnóstico detallado de los sistemas de información, donde se identificará y clasificará cada activo digital según su nivel de criticidad. Posteriormente, se llevará a cabo un análisis de amenazas y vulnerabilidades que permitirá determinar los riesgos existentes y definir las medidas de mitigación adecuadas.

La implementación de controles de seguridad se estructurará en tres niveles: **técnico, organizativo y normativo**. Desde la perspectiva técnica, se establecerán mecanismos como el cifrado de datos, autenticación multifactor, monitoreo de eventos de seguridad y segmentación de redes para minimizar riesgos de accesos no autorizados. A nivel organizativo, se adoptarán políticas de seguridad de la información que definirán lineamientos para el acceso, uso y tratamiento de los datos, acompañado de programas de capacitación para funcionarios y contratistas con el fin de fortalecer la cultura de ciberseguridad. En el ámbito normativo, se garantizará el cumplimiento de regulaciones como la **Ley 1581 de 2012 sobre protección de datos personales**, la **Ley 1273 de 2009 en delitos informáticos** y el **Decreto 1078 de 2015 en Gobierno Digital**, asegurando la transparencia y el adecuado manejo de la información pública.

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 10 de 11
		Versión: 1

En cuanto a la **gestión de incidentes de seguridad**, se estructurará un **Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)** que aplicará protocolos basados en el estándar **NIST 800-61**. Esto permitirá una detección temprana de amenazas, una respuesta efectiva ante incidentes y la recuperación eficiente de los sistemas afectados. Se implementará un sistema de reporte y análisis de incidentes que facilitará la toma de decisiones y la mejora continua de los controles de seguridad.

La protección de datos personales será un pilar fundamental dentro de la estrategia, adoptando el enfoque de **“Privacidad por Diseño”** en cada proceso que implique tratamiento de información sensible. Se formalizará la designación de un **Oficial de Protección de Datos**, encargado de supervisar el cumplimiento de la normativa y de establecer medidas como la amonificación de información y la gestión de consentimientos.

Para garantizar la eficacia de la estrategia, se establecerá un sistema de monitoreo y evaluación con indicadores clave de desempeño que medirán el nivel de madurez en seguridad de la información, la efectividad de los controles implementados y la reducción de incidentes. Se realizarán auditorías periódicas que permitirán la mejora continua y la actualización de la estrategia en función de los cambios tecnológicos y regulatorios.

El compromiso con la seguridad de la información no solo es un requisito normativo, sino una necesidad estratégica para garantizar la continuidad operativa y la confianza en la gestión institucional. A través de esta estrategia, IDERBOL fortalecerá su resiliencia digital y garantizará la protección de la información, promoviendo una cultura organizacional basada en la seguridad y la transparencia.

4.1. PLAN DE ACCIÓN.

FASE	ACTIVIDADES	RESPONSABLES	PLAZO
Diagnóstico y evaluación de riesgos	Identificación de activos, análisis de amenazas y cálculo de riesgos	Asesor TIC, Planeación y Control Interno	3 Meses
Implementación de Controles	Adopción de medidas técnicas y organizativas según ISO 27001	Asesor TIC, Subgerencia Administrativa y Financiera	6 meses
Gestión de Incidentes	Creación de protocolos de respuesta y formación del CSIRT	Asesor TIC	4 meses
Protección de Datos Personales	Implementación de políticas y designación de Oficial de Protección de Datos	Asesor TIC y Jefe Jurídico	3 Meses
Monitoreo y mejora continua	Auditorías, reportes de seguridad y actualización de planes	Asesor TIC, Planeación y Control Interno	Permanente

	FORMATO PLANES INSTITUCIONALES	Código:
		Fecha:
		Página 11 de 11
		Versión: 1

REFERENCIAS

Manual de Gobierno Digital – MINTIC.

Modelo de Seguridad y Privacidad de la Información – MINTIC.

CONPES No. 3701 del 2011 “Lineamientos de Políticas para la Ciberseguridad y Ciberdefensa”

CONPES No. 3854 de 2016 “Política Nacional de Seguridad Digital”

CONPES No. 3995 de 2020 “Política Nacional de Confianza y Seguridad Digital”

Decreto 767 de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital” del Ministerio de las Tecnologías de la información y las Comunicaciones.

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5

Adicionalmente se utilizó IA mediante Prompts específicos guiados por la experiencia del Asesor TIC

CONTROL DE CAMBIOS.

Versión	Fecha y número de Acta y/o Acto Administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1	Acta Comité Institucional de Gestión y Desempeño No.001-2025	Rudy Joel Nieto Henriquez	Edgardo Olarte, Steffi Chalave	Ariel Zambrano	Creación del documento.

