	<p>DEPARTAMENTO DE RISARALDA Secretaria Administrativa</p> <p>GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
<p>Versión.0</p>	<p>Vigencia: Junio 2015</p>

PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA

Aprobó: Comité Sistema de Gestión de Seguridad Informática
 Revisó: Ligelly Hernández Mayorga - Directora de Informática
 Frank Jhoanny Hernández Restrepo - Contratista



	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

TABLA DE CONTENIDO


INTRODUCCIÓN	5
RESUMEN	6
OBJETIVOS.....	7
Objetivo general.....	7
Objetivos específicos.....	7
PLANTEAMIENTO DEL PROBLEMA	8
Justificación	9
FORMULACIÓN DEL PROBLEMA.....	10
MARCO REFERENCIAL	11
Marco teórico.....	11
Inventario de Sistemas de Información – Proceso responsable.....	13
Inventario de bienes – Proceso responsable	14
Inventario de expedientes – Proceso responsable	14
Encuesta para determinar los sistemas de información más sensibles que operan en la Gobernación y la percepción de seguridad informática de los diferentes usuarios de la misma y aplicación de la herramienta Security Assessment Tool	¡Error! Marcador no definido.
Ficha técnica y resultados obtenidos de herramienta Microsoft Security Assessment Tool 	¡Error! Marcador no definido.
Ficha técnica encuesta interna.....	¡Error! Marcador no definido.
Resultado y análisis de la encuesta interna	¡Error! Marcador no definido.
Definición de prioridades y el Alcance del Plan de Gestión de Seguridad de la Información.	16
Política de Seguridad informática de la Gobernación de Risaralda	16
Declaración De La Política De Seguridad.....	¡Error! Marcador no definido.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
 Revisó: Ligelly Hernández Mayorga - Directora de Informática
 Frank Jhoanny Hernández Restrepo - Contratista

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Cuentas de usuario de los sistemas.....	19
Clasificación de la Información.....	20
Acuerdos de confidencialidad y derechos de propiedad intelectual.....	22
Seguridad de la red interna y perimetral	22
Buen uso de recursos informáticos.....	23
Trabajo móvil.....	24
Formación y capacitación en seguridad de la información.....	24
Escritorios y pantallas limpias	25
Seguridad en la reutilización o eliminación de equipos.....	25
Correo electrónico e Internet.....	26
Acceso físico a áreas sensibles	26
Uso de dispositivos de almacenamiento masivo de información.....	26
Incidentes de seguridad de la información	27
Administración de los riesgos de procesos ya identificados en el sistema de gestión de calidad.	¡Error! Marcador no definido.
Evaluación de Riesgos	¡Error! Marcador no definido.
Riesgos Inventario Sistemas de Información	¡Error! Marcador no definido.
Riesgos inventario de bienes.....	¡Error! Marcador no definido.
Riesgos Inventario de expedientes	¡Error! Marcador no definido.
Riesgos inventario del Recurso Humano.....	¡Error! Marcador no definido.
Plan de tratamiento del riesgo del manejo de la información.	28
Autenticación, Gestión y control de usuarios y Aplicaciones	28
Declaración de aplicabilidad	47
DISEÑO METODOLÓGICO.....	51
CRUCE DE PREGUNTAS.....	¡Error! Marcador no definido.
ANÁLISIS DE DATOS.....	¡Error! Marcador no definido.
CONCLUSIONES	52
RECOMENDACIONES	53

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

REFERENCIAS BIBLIOGRÁFICAS 54

LISTA DE ILUSTRACIONES

Ilustración 1 Plataforma de Calidad de la Gobernación de Risaralda.....	12
Ilustración 2 Inventarios de la Dirección de Informática y Sistemas	14
Ilustración 3 Archivos almacenados en el disco duro.....	15
Ilustración 4 Herramienta Microsoft Security Assessment Tool. ¡Error! Marcador no definido.	
Ilustración 5 Herramienta Microsoft Security Assessment Tool. ¡Error! Marcador no definido.	
Ilustración 6 Cuadro pregunta 7 Sistemas de Información	¡Error! Marcador no definido.
Ilustración 7 Cuadro de respuestas pregunta 7 Sistemas de Información	¡Error! Marcador no definido.
Ilustración 8 Cuadro de Riesgos	¡Error! Marcador no definido.
Ilustración 9 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 10 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 11 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 12 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 13 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 14 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 15 Plataforma de Calidad Gobernación de Risaralda	¡Error! Marcador no definido.
Ilustración 16 Propia	49
Ilustración 17 Gráfico estadístico en barras pregunta 1 Experiencia	¡Error! Marcador no definido.
Ilustración 18 Gráfico estadístico en torta pregunta 2 tipo de vinculación	¡Error! Marcador no definido.
Ilustración 19 Gráfico estadístico en torta 3d pregunta 3 Identificación de acciones en el marco del SGSI	¡Error! Marcador no definido.
Ilustración 20 Gráfico estadístico barras pregunta 4 uso de dispositivos externos	¡Error! Marcador no definido.
Ilustración 21 Gráfico estadístico en barras horizontales pregunta 5 uso del correo electrónico	¡Error! Marcador no definido.
Ilustración 22 Gráfico estadístico circular pregunta 6 formación en SGSI	¡Error! Marcador no definido.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

INTRODUCCIÓN


El siguiente documento inspira y dirige todo el Sistema de Gestión de Seguridad Informática de la Gobernación de Risaralda, expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas, directrices principales, entre otras del SGSI. Se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Gobernación de Risaralda.

Debe ser conocida y cumplida por toda la planta de personal de la Gobernación de Risaralda, tanto se trate de funcionarios públicos o contratistas, y sea cual fuere su nivel jerárquico y su situación de revista.

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

RESUMEN

Palabras claves: Sistemas de información, SGSI (Sistema de Gestión de Seguridad Informática), recursos de información, confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información, priorización, seguridad informática, usuario, política, riesgos, control, página web, ficha técnica y gestión

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

OBJETIVOS

Objetivo general

Elaborar el Plan de Gestión de Seguridad de Informática de acuerdo a los lineamientos normativos del Ministerio de las Tecnologías, específicamente en la Estrategia Gobierno en Línea para la Gobernación de Risaralda

Objetivos específicos


Elaborar un Plan de Gestión de Seguridad Informática para la Gobernación de Risaralda

Realizar una encuesta para determinar los sistemas de información más sensibles que operan en la Gobernación y la percepción de seguridad informática de los diferentes usuarios de la misma.

Analizar los resultados de la investigación

Actualizar la Política de Seguridad informática de la Gobernación de Risaralda, asegurando su eficacia.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

PLANTEAMIENTO DEL PROBLEMA


La información es un recurso que, como el resto de los activos, tiene valor para la Gobernación de Risaralda y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Gobernación de Risaralda.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la Gobernación de Risaralda, de los entes descentralizados, de terceros que usen al menos parte de los sistemas de información de la Gobernación de Risaralda y encargados de la difusión, consolidación y

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


cumplimiento de una Política de seguridad informática actualizada y eficiente garantizando el fin último del cumplimiento de la Misión del Departamento.

Justificación

Proteger los recursos de información de la Gobernación de Risaralda y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, mediante la elaboración del Plan de Seguridad Informática.

Igualmente viabilizar la graduación de los autores como Especialistas en Gerencia Informática.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p>DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p>GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
<p>Versión.0</p>	<p>Vigencia: Junio 2015</p>

FORMULACIÓN DEL PROBLEMA

¿Será que las políticas de seguridad de información actuales de la Gobernación de Risaralda, responden a las necesidades de información de la entidad y las expectativas de los usuarios?

Aprobó:
Revisó:

Comité Sistema de Gestión de Seguridad Informática
Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
<p>Versión.0</p>	<p>Vigencia: Junio 2015</p>


MARCO REFERENCIAL

Marco teórico

1. Identificación del inventario de activos de la información de la Gobernación de Risaralda.

Inicialmente, hacemos la socialización del mapa de procesos que hace parte de la plataforma de calidad de la entidad, esto con el fin de ubicar los procesos que tienen a cargo el inventario de activos de información dentro de la entidad.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
<p>Versión: 0</p>	<p>Vigencia: Junio 2015</p>

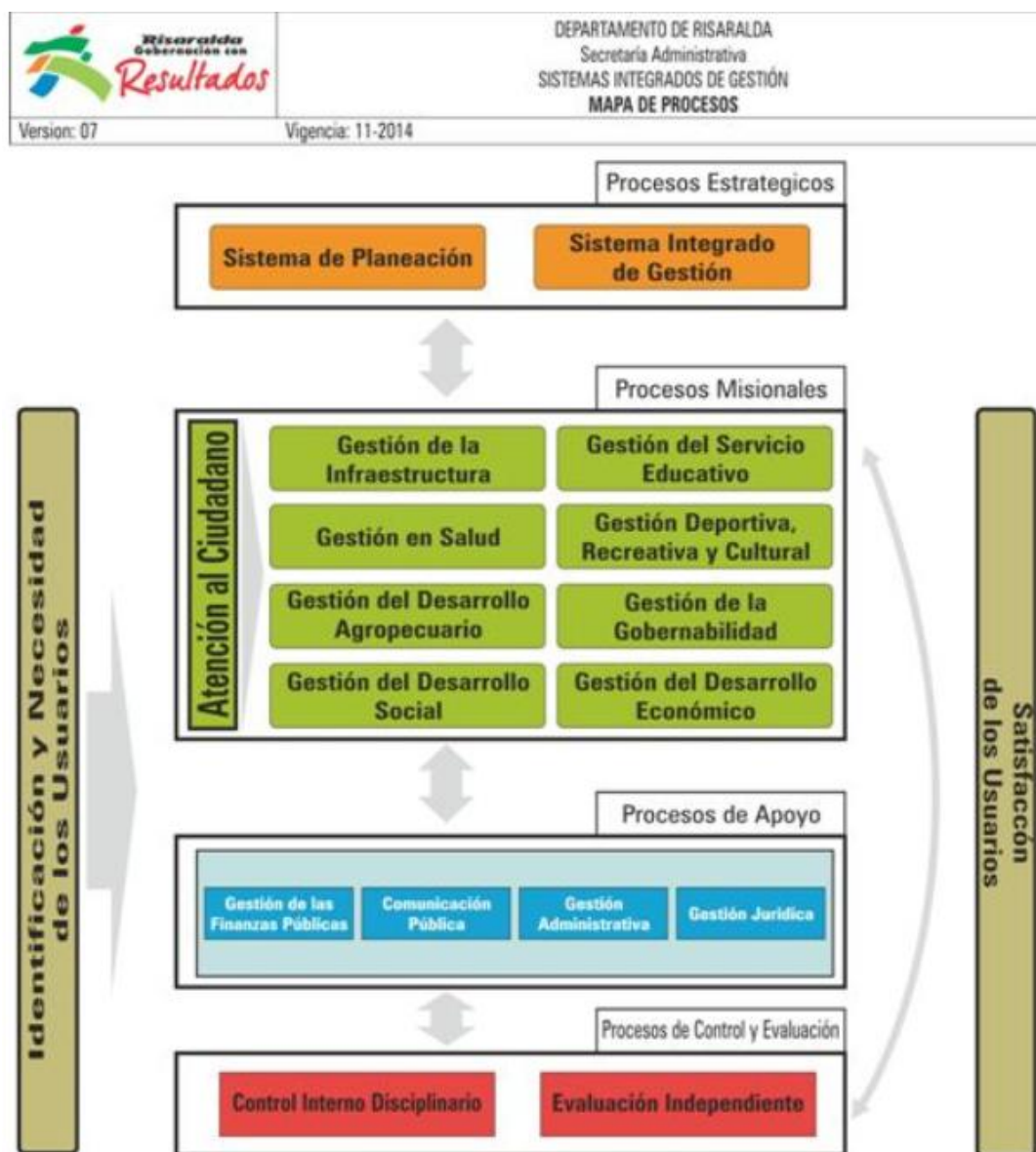



Ilustración 1 Plataforma de Calidad de la Gobernación de Risaralda

Cabe anotar que cada proceso produce información importante para la entidad mediante un sistema de información.

Aprobó:
Revisó:

Comité Sistema de Gestión de Seguridad Informática
Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

A continuación se hace la identificación del inventario de activos de la información de la Gobernación de Risaralda, clasificándolos en 4 grupos con su respectivo proceso de gestión según el sistema de Calidad de la entidad.

- a) Inventario de Sistemas de Información – Proceso responsable
- b) Inventario de bienes – Proceso responsable.
- c) Inventario de expedientes – Proceso responsable.
- d) Inventario del recurso humano – Proceso responsable.

Inventario de Sistemas de Información – Proceso responsable

Este inventario tiene como responsable el proceso de apoyo – Gestión Administrativa – Gestión de las tecnologías de información.

A continuación el inventario de sistemas de información localizados y administrados por la Dirección de Informática y Sistemas líderes del sub-proceso Gestión de las tecnologías de la información.

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista



DEPARTAMENTO DE RISARALDA

Secretaría Administrativa

GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA

Versión.0

Vigencia: Junio 2015

NOMBRE	DESCRIPCION	URL	EMPRESA DESARROLLADORA	BASE DE DATOS	ENTIDAD	SECRETARIA
Aplicativo Web	Entrevista de Deserción Estudiantil	http://educacion.risaralda.gov.co/sitioportal/desercion/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Educación
Aplicativo Web	Prueba de Competencias Lectoras	http://educacion.risaralda.gov.co/sitioportal/lectura/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Educación
Aplicativo Web	Sistema de Medición de Competencias Matemáticas	http://educacion.risaralda.gov.co/sitioportal/matematicas/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Educación
Aplicativo Web	Sistema de Orientación Profesional	http://educacion.risaralda.gov.co/vocacional/app/VoAplicacion/	Universidad Tecnológica de Pereira	PostgreSQL	Gobernación de Risaralda	Secretaría de Educación
Aplicativo Web	Sistema de Información de Contratación Pública	http://www.risaralda.gov.co/juridica/	Persona Natural	MySQL	Gobernación de Risaralda	Secretaría Jurídica
Aplicativo Web	Sistema de Información Financiero y de Activos	http://190.128.91.166/PCTGI/	PCT Ltda.	Oracle	Gobernación de Risaralda	Secretaría Administrativa
Aplicativo Web	Sistema de Información para Inducciones & Rendiciones	http://www.risaralda.gov.co/capacitaciones/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría Administrativa
Banco de Proyectos	Sistema de Información del Banco de Proyectos	http://intranet.risaralda.gov.co/Planeacion/Banco/	Implementación Propia	Microsoft Access	Gobernación de Risaralda	Secretaría de Planeación
Deuda Pública	Sistema de Información de la Deuda Pública	http://190.128.91.166/humano/humano/Ingresar.aspx?Ent=GoBrisaraldaWeb	Persona Natural	PostgreSQL	Gobernación de Risaralda	Secretaría de Hacienda
HumanoWeb	Sistema de Información de Gestión de Recursos Humanos – Desprendible de Pago Mensual	http://190.128.91.166/humano/humano/Ingresar.aspx?Return=UI-32/humano/32Humano	Soporte Lógico	Oracle	Gobernación de Risaralda	Secretaría Administrativa
HumanoWeb	Sistema de Información de Gestión de Recursos Humanos – Nómina	http://www.risaralda.gov.co/humano/humano/Ingresar.aspx?Return=UI-32/humano/32Humano	Soporte Lógico	Oracle	Gobernación de Risaralda	Secretaría Administrativa
Moodle	Curso de Inducción a Docentes	http://educacion.risaralda.gov.co/sitio/moodle/	Ministerio de Educación	MySQL	Gobernación de Risaralda	Secretaría de Educación
Moodle	Comunidad Virtual de Aprendizaje	http://educacion.risaralda.gov.co/sitio/capacitaciones/	Fundación Universitaria del Área Andina	MySQL	Gobernación de Risaralda	Secretaría de Educación
OCS Inventory NG	Sistema de Información de Inventario de Hardware & Software	http://monitoreo.risaralda.gov.co/OCSreports/	Implementación Propia	MySQL	Gobernación de Risaralda	Secretaría Administrativa
ODEC	Sistema de Información del Observatorio Departamental del Delito y la Convivencia	http://odec.risaralda.gov.co/	Universidad Tecnológica de Pereira	PostgreSQL	Gobernación de Risaralda	Secretaría de Gobernación
PCI	Sistema de Información Financiero y de Activos	http://intranet.risaralda.gov.co/Planeacion/PCI/	PCI Ltda.	Oracle	Gobernación de Risaralda	
Portal Web	Portal Web del Comité Interinstitucional de Control Interno de Risaralda	http://cicir.risaralda.gov.co/	Persona Natural	MySQL	Gobernación de Risaralda	Despacho del Gobernador
Portal Web	Portal Web Institucional de la Administración Departamental	http://www.risaralda.gov.co/site/main/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría Administrativa
Portal Web	Portal Web Institucional de la Asamblea Departamental	http://www.asamblearisaralda.gov.co/	Persona Natural	MySQL	Asamblea Departamental	N/A
Portal Web	Portal Web Institucional de la Promotora de Vivienda de Risaralda	http://www.pvr.gov.co/	Implementación Propia	MySQL	Promotora de Vivienda de Risaralda	N/A
Portal Web	Portal Web Institucional de la Secretaría de Deporte, Recreación y Cultura	http://deporteycultura.risaralda.gov.co/	Persona Natural	MySQL	Gobernación de Risaralda	Secretaría de Deporte, Recreación y Cultura
Portal Web	Portal Web Institucional de la Secretaría de Desarrollo Agropecuario	http://www.risaralda.gov.co/site/agropecuaria/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Desarrollo Agropecuario
Portal Web	Portal Web Institucional de la Secretaría de Desarrollo Social	http://www.risaralda.gov.co/site/social/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Desarrollo Social
Portal Web	Portal Web Institucional de la Secretaría de Educación	http://www.risaralda.gov.co/site/educacion/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Educación
Portal Web	Portal Web Institucional de la Secretaría de Hacienda	http://www.risaralda.gov.co/site/hacienda/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Hacienda
Portal Web	Portal Web Institucional de la Secretaría de Planeación	http://planeacion.risaralda.gov.co/site/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Planeación
Portal Web	Portal Web Institucional de la Secretaría de Salud	http://www.risaralda.gov.co/site/salud/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Salud
Portal Web	Sistema de Información Juvenil	http://www.risaralda.gov.co/sitio/lacuaoven/	Persona Natural	MySQL	Gobernación de Risaralda	Secretaría de Desarrollo Social
SAIA	Sistema de Administración Integral de Información	http://saia.risaralda.gov.co/	CEROK SAS	Oracle	Gobernación de Risaralda	Secretaría Administrativa
SIETE	Sistema de Información y Estadística Territorial	http://planeacion.risaralda.gov.co/sitio/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Planeación
SIG	Sistema de Información de Indicadores	http://sig.risaralda.gov.co/	Universidad Tecnológica de Pereira	PostgreSQL	Gobernación de Risaralda	Secretaría de Planeación
SIG	Visor Geográfico	http://sig.risaralda.gov.co/8080/visor_gobernacion/	Universidad Tecnológica de Pereira	PostgreSQL	Gobernación de Risaralda	Secretaría de Planeación
Biodiversidad	Sistema de Información en Biodiversidad de Risaralda (SIBIR)	http://planeacion.risaralda.gov.co/biodiversidad/	Universidad Tecnológica de Pereira	MySQL	Gobernación de Risaralda	Secretaría de Salud
B2B	Sistema de Información Comercio Agro Risaralda	http://b2b2b.risaralda.gov.co/	SISTE SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Desarrollo Agropecuario
SIG	Sistema de Información Georeferenciada	http://mvsig.risaralda.gov.co/	SISTE SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Desarrollo Agropecuario
SISAP	Sistema de Información Integrado de la Secretaría de Salud	http://saludito.risaralda.gov.co/	Sisto SAS	PostgreSQL	Gobernación de Risaralda	Secretaría de Salud

Ilustración 2 Inventarios de la Dirección de Informática y Sistemas

Inventario de bienes – Proceso responsable

Este inventario tiene como responsable el proceso de apoyo – Gestión Administrativa – Gestión de bienes y servicios.

Inventario de expedientes – Proceso responsable

Este inventario tiene como responsable el proceso de apoyo – Gestión Administrativa – Gestión documental.

Existe un inventario físico clasificado de la siguiente forma


Aprobó:

Comité Sistema de Gestión de Seguridad Informática

Revisó:

Ligelly Hernández Mayorga - Directora de Informática

Frank Johanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


















 CAJAS TRASLADADAS A FIDUCENTRO	02/10/2014 04:04 ...	Carpeta de archivos
 CORRESPONDENCIA	02/10/2014 04:04 ...	Carpeta de archivos
 DECRETOS	02/10/2014 04:17 ...	Carpeta de archivos
 DEVOLUCIONES	02/10/2014 04:19 ...	Carpeta de archivos
 HISTORIAS LABORALES	02/10/2014 04:19 ...	Carpeta de archivos
 INDEPORTES	02/10/2014 04:19 ...	Carpeta de archivos
 INVENTARIO DE NOMINAS SALA 2	02/10/2014 04:19 ...	Carpeta de archivos
 INVENTARIO EDUCACION BODEGA 2	02/10/2014 04:19 ...	Carpeta de archivos
 O.P.S EDUCACIÓN	02/10/2014 04:19 ...	Carpeta de archivos
 ORDENANZAS	02/10/2014 04:20 ...	Carpeta de archivos
 PRESTACIONES SOCIALES EDUCACIÓN	02/10/2014 04:20 ...	Carpeta de archivos
 RESOLUCIONES	02/10/2014 04:32 ...	Carpeta de archivos
 TRANSFERENCIAS DOCUMENTALES	02/10/2014 04:33 ...	Carpeta de archivos
 VIRTUALES 2011-2012	02/10/2014 04:34 ...	Carpeta de archivos
 VIRTUALES 2013	02/10/2014 04:36 ...	Carpeta de archivos
 VIRTUALES 2014	02/10/2014 04:37 ...	Carpeta de archivos

Ilustración 3 Archivos almacenados en el disco duro

Igualmente un sistema de Gestión documental como parte de la plataforma SAIA, desde la vigencia 2010 que maneja todo los documentos de acuerdo a la tabla de retención documental vigente en la Gobernación. Ver anexo 2.

SAIA® es una plataforma diseñada para centralizar de forma electrónica los procesos de gestión de la Gobernación en los que se vean involucrados información, documentos y responsabilidades, permitiendo el flujo dinámico y controlado de la información, logrando reducir todos los costos administrativos asociados, diseñado de acuerdo a las directrices del Archivo General de la Nación contempladas en la ley 594 de 2000 , las sugerencias y recomendaciones de la Contraloría General de la Nación, según la Evaluación de la Función Archivística realizada en el año 2002 y el decreto 2578 de 2012, permite consultar la trazabilidad de los documentos durante el recorrido que

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

realiza internamente hasta obtener su respectiva respuesta y cierre; es un sistema con características 100% Web.

Definición de prioridades y el Alcance del Plan de Gestión de Seguridad de la Información

De acuerdo al análisis de los resultados de la investigación se definen las prioridades y el alcance del presente Plan, de la siguiente forma se identifica los sistemas de información priorizados en los procesos a los que pertenece según la estructura del mapa de procesos de la plataforma de calidad institucional.


Política de Seguridad informática de la Gobernación de Risaralda

Declaración De La Política De Seguridad

“El Departamento de Risaralda es la administración central del Departamento de Risaralda tiene como responsabilidad lo público, en el ámbito económico, social y de gestión ambiental de los 14 municipios. Conscientes de la importancia que la seguridad de la información en la construcción de una sociedad con acceso a la información y una economía basada en el conocimiento, ha decidido implantar un sistema de gestión y suscribe la presente política.

El Departamento de Risaralda establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI)

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, disponibilidad e integridad de su información así como de los sistemas que la soportan, aumentando la confianza de los ciudadanos y otras partes interesadas; junto con el cumplimiento de todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

El diseño, implantación y mantenimiento del SGSI se apoyará en los resultados de un proceso continuo de análisis y gestión de riesgos del que se derivan las actuaciones a desarrollar en materia de seguridad dentro del alcance de su misión y en coherencia con la estrategia integradora CAMEDA (Calidad, Modelo Estándar de Control interno y Desarrollo Administrativo).

El Departamento de Risaralda establecerá los criterios de evaluación del riesgo de manera que todos aquellos escenarios que impliquen un nivel de riesgo inaceptable sean tratados adecuadamente. Como parte del SGSI, el comité SGSI desarrollará, implantará y mantendrá actualizado un plan de acción acorde a las necesidades de la entidad y dimensionado a los riesgos que le afectan.

El Departamento de Risaralda se compromete a la implantación, mantenimiento y mejora del SGSI dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso. Para ello el comité incluirá en el plan de acción actividades para la formación y concienciación del personal con la seguridad de la información. A su vez, cuando los trabajadores incumplan las políticas de seguridad el comité notificará a la autoridad competente, respetando el conducto regular con

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

el fin de aplicar las medidas disciplinarias dentro del marco legal aplicable, y dimensionadas al impacto que tengan sobre la entidad.

La responsabilidad general de la seguridad de la información recaerá sobre cada responsable del inventario de información y es responsabilidad cada usuario reportar los incidentes en materia de seguridad utilizando las directrices establecidas y debidamente socializadas.


Todo lo definido en esta política se concretará y desarrollará en normativas y procedimientos, las cuales se integrarán en la medida de lo posible con otros sistemas de gestión de la entidad, compartiendo aquellos recursos en pro de la optimización y buscando la mejora continua de la eficiencia y eficacia de la gestión de los procesos.

La presente política será de aplicación a todo el personal y recursos que se encuentran dentro del alcance del SGSI, se pone en su conocimiento y es comunicada a todas las partes interesadas.

Gobernador de Risaralda”

La información de la Gobernación de Risaralda es uno de los activos más importantes para la entidad, y por lo tanto se le debe dar un tratamiento seguro, bajo la supervisión de los Secretarios, Directores, Jefes de área y la responsabilidad de cada uno de los funcionarios de la entidad; con el fin de mantener la confidencialidad, integridad, y disponibilidad de la misma.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Cuentas de usuario de los sistemas

El acceso a los sistemas de información será controlado por medio de nombres de usuario y contraseñas personales e intransferibles. Está prohibido el préstamo de cuentas (revelación de contraseñas) de los sistemas (aplicaciones, dominio, VPN, etc.).

Sólo se crearán cuentas de usuario genéricas en los sistemas de información, si las mismas contemplan exclusivamente opciones de consulta, bajo la condición de que no se esté accediendo a información clasificada como **“Información Pública Reservada”** definida en la Ley 1712 de 2014 (Ley de Transparencia, Artículo 6 Literal c).


Los usuarios deben establecer contraseñas que no sean fácilmente identificables.

Las contraseñas de acceso a los sistemas de información no deben ser escritas en medios físicos o digitales no protegidos (deben ser memorizadas o almacenadas digitalmente: bajo técnicas de cifrado de datos, o usando archivos protegidos por contraseñas fuertes).

Cuando se produzcan cambios de funciones que impliquen la reasignación de privilegios sobre los sistemas, se deben tramitar oportunamente los cambios de permisos bajo responsabilidad de los jefes de los funcionarios.

Toda desvinculación de funcionarios de la entidad, deberá ser comunicada por el jefe del funcionario para ser notificado a la Dirección de Informática y

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Sistemas con el fin de cancelar los accesos a los sistemas de información y recuperar los activos informáticos asignados.


Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de la compañía deberán ser salvaguardados bajo custodia del Director de Informática y Sistemas o quien este delegue, en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

Clasificación de la Información

La información propiedad de la Gobernación de Risaralda se considerará por defecto como “**Interna**”, correspondiente a toda la información no “**Pública**”, o que no haya sido declarada como “**Pública**”, “**Pública Clasificada**” o “**Pública Reservada**”. (Ley 1712 de 2014 de Transparencia, Artículo 6) Sólo se podrá tener acceso a información clasificada como “**Pública Clasificada**” o “**Pública Reservada**” bajo previa aprobación del “sujeto obligado” de la información. (Art. 5 Ley 1712/2014)

De acuerdo a la Ley en Mención, la información se clasifica en:

- **Pública:** Toda obligación que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal.
 - **Pública Clasificada:** Es aquella información, que estando en poder o custodia de un sujeto obligado, pertenece al ámbito propio, particular y privado o semi privado, de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado siempre que se trate de las circunstancias
- Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la citada Ley.


- **Pública Reservada:** Es aquella información, que estando en poder o custodia de un sujeto obligado o en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el Artículo 19 de la citada Ley.

La responsabilidad de la clasificación de la información, recae sobre los Secretarios de Despacho, Directores Operativos, Asesores y Jefes de Área de cada dependencia. Se debe tomar como guía para el proceso de clasificación, lo establecido en la Ley 1712 del 2014 Artículo 6.

El primer responsable de verificar que la Información cuente con controles adecuados que eviten su pérdida, daño o divulgación no autorizada es el sujeto obligado de la Información.

El nivel de protección requerido para cada nivel de clasificación, se deberá evaluar analizando los requerimientos de Confidencialidad (la información de mayor valor para la entidad solo puede ser conocida por personas autorizadas); e Integridad (la información no debe poder ser alterada o destruida de manera no autorizada para afectar la entidad).

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Acuerdos de confidencialidad y derechos de propiedad intelectual

Mientras persista una relación laboral con la Gobernación, todos sus funcionarios cederán a la compañía los derechos de propiedad intelectual de los desarrollos que originen como parte de sus responsabilidades laborales con la compañía.

Siempre que se requiera compartir información “**Pública Clasificada**” y/o “**Pública Reservada**” con un tercero, deberá acogerse a los términos de la Ley.

Con el fin de tener acceso a los sistemas de Información institucionales de la Gobernación cada usuario deberá firmar el Compromiso de confidencialidad.


Seguridad de la red interna y perimetral

La creación de cuentas de usuario para acceso remoto a la red interna de la Gobernación a través de VPN, sólo será autorizada por el Director de Informática y Sistemas.

No está permitida la conexión a la red interna de equipos diferentes a los asignados por la Gobernación. En caso de existir la expresa necesidad de conectar un equipo de un tercero, solo podrá realizarse bajo previa autorización del Director de Informática y Sistemas.

Todas las redes inalámbricas existentes en la entidad deberán cumplir con los Estándares de Seguridad definidos por la Dirección de Informática y Sistemas.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Buen uso de recursos informáticos

Los equipos informáticos fijos y portátiles asignados por la Gobernación a sus funcionarios, son herramientas de trabajo y deben ser utilizados para fines laborales. El usuario a quien le hayan sido asignados será responsable de su buen cuidado y correcto uso.

Toda la información almacenada en los equipos de cómputo son, en principio, propiedad de la Gobernación, y debe ser clasificada de acuerdo con las normas definidas en esta Política. La información “**Personal**” almacenada en estos equipos deberá estar claramente identificada y separada de la información laboral.


La información pública de la Gobernación no debe ser copiada en equipos personales.

No está permitida la instalación de ningún software adicional al aprobado por la Dirección de Informática y Sistemas.

El usuario es responsable de realizar las copias de seguridad requeridas para proteger la información almacenada en los equipos asignados, a través de las herramientas que el área de la Dirección de informática y Sistemas le provea.

Ningún usuario está autorizado para compartir información de su equipo a todos los usuarios de la red sin establecer restricciones.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Trabajo móvil


Al retirar un equipo informático de las instalaciones de la entidad, el funcionario a quien éste le haya sido asignado será responsable de extremar su cuidado. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la ley para tal fin.

La información Publica Clasificada o Publica Reservada de la entidad no puede ser copiada en medios externos con excepción de aquellas autorizadas por la Ley, en dispositivos asignados por la Dirección de informática y Sistemas para el respaldo de la misma, los cuales sólo deberán ser empleados para este fin. En caso de ser estrictamente necesaria la copia de esta información en medios adicionales y previa autorización del Sujeto Obligado de la información, ésta deberá ser grabada de forma segura: bajo técnicas de cifrado de datos, o como mínimo comprimiéndola con herramientas suministradas por la compañía y estableciendo una contraseña fuerte.

Formación y capacitación en seguridad de la información

Todos los funcionarios de la Gobernación de Risaralda deben recibir capacitación sobre las Políticas de Seguridad de la Información definidas, cuando se les de la inducción y reinducción.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Escritorios y pantallas limpias

Cuando un funcionario se retire de su puesto de trabajo, deberá asegurar que la información clasificada como “**Publica Clasificada**” o “**Publica Reservada**” no quede expuesta a terceros no autorizados.

Todos los funcionarios deberán mantener sus equipos de cómputo limpios y aseados, cuando se requiera de mantenimiento especializado se debe solicitar a la Dirección de informática y Sistemas.


Ningún funcionario debe consumir alimentos ni ingerir líquidos en el sitio donde se encuentre el equipo de cómputo.

Seguridad en la reutilización o eliminación de equipos

Antes de reasignar un equipo de cómputo de un funcionario que almacene en éste información clasificada como “**Publica Clasificada**” o “**Publica Reservada**” (cuando no se trata del mismo cargo y por lo tanto la información que se maneja es diferente), se debe garantizar un borrado seguro de tal forma que los datos no puedan ser recuperados.

Todo dispositivo de almacenamiento de información que sea dado de baja debe ser destruido. Antes de realizar la venta y/o donación de equipos de cómputo se deben extraer sus medios de almacenamiento. (Norma ISO 27001:2013)

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Correo electrónico e Internet

Los servicios de correo electrónico e Internet, son herramientas de trabajo brindados por la Gobernación y deben ser usados para fines laborales.

Los mensajes de correo electrónico transmitidos a través de las cuentas de correo suministradas por la Gobernación no se considerarán correspondencia privada, ya que éstas tienen como fin primordial la transmisión de Información relacionadas con las actividades ordinarias de la Gobernación. Proceso responsable del tema Gestión Documental.

Dentro de los horarios de oficina, el Internet deberá ser empleado exclusivamente para fines laborales.


Acceso físico a áreas sensibles

Las áreas definidas como sensibles por su nivel de procesamiento de información (centros de cómputo), deberán contar con controles físicos que impidan el acceso de personal no autorizado. Los terceros siempre deberán permanecer acompañados por un funcionario de la Dirección de informática y Sistemas.

Uso de dispositivos de almacenamiento masivo de información

El uso de dispositivos que permitan el almacenamiento masivo de información en medios externos, como es el caso de equipos de conexión USB y unidades

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


de escritura de CD/DVD, estará restringido debido a que constituye una amenaza que incrementa el riesgo de pérdida de integridad de la información de la entidad (Infecciones de Software Malicioso) y pérdida de confidencialidad de la misma (fuga masiva de información “**Publica Clasificada**” o “**Publica Reservada**”). Sólo aquellos funcionarios con claras necesidades tendrán habilitados estos dispositivos con la previa autorización.

Incidentes de seguridad de la información

El Ingeniero de Seguridad de la Información o el Director de informática y Sistemas verificará el cumplimiento de las Políticas de Seguridad de la Información apoyado en las herramientas informáticas implementadas en la Gobernación. Cuando se identifique un Incidente de Seguridad de la Información, éste será reportado al sujeto obligado de la Información.

Los usuarios de los sistemas de información no deben, bajo circunstancia alguna, intentar probar una supuesta debilidad de seguridad de la plataforma informática de la compañía, por cuanto esta acción será interpretada como una falta grave que será analizada de acuerdo con lo establecido en el código de ética.

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Plan de tratamiento del riesgo del manejo de la información.

En observancia al resultado de la encuesta y al alcance propuesto a continuación se realiza un plan de tratamiento del riesgo del manejo de la información que apunta a impactar en los mayores riesgos que tiene en inventario de sistemas de información.

Autenticación, Gestión y control de usuarios y Aplicaciones

7.1.1. Objetivos

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red de la Gobernación de Risaralda y otras redes públicas o privadas.


Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

7.1.2. Alcance

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


El control de acceso definido en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Gobernación de Risaralda, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

7.1.3. Responsabilidad

El comité de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
 - Definir pautas de utilización de Internet para todos los usuarios.
 - Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
 - Controlar la asignación de privilegios a usuarios.
 - Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
 - Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración
- Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.

- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
 - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
 - Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
- Aprobar y solicitar la asignación de privilegios a usuarios.
- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Los Secretarios de despacho, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Área de Gestión de Tecnologías de la Información, cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de “enrutadores” o “gateways” adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.


El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

7.1.4. Requerimientos para el Control de Acceso

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- b) Identificar toda la información relacionada con las aplicaciones.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


- c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes
- d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

7.1.5. Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

- a) Indicar expresamente si las reglas son obligatorias u optativas
- b) Establecer reglas sobre la premisa “Todo debe estar prohibido a menos que se permita expresamente” y no sobre la premisa inversa de “Todo está permitido a menos que se prohíba expresamente”.
- c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario
- d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
- e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

7.2.6. Administración de Accesos de Usuarios


Con el objetivo de impedir el acceso no autorizado a la información se exigirá el procedimiento formal para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información, basados en solicitudes por su jefe directo o supervisor en el caso de contratistas en la plataforma SAIA.

7.2.7. Registro de Usuarios

Todo registro de usuarios se deberá realizar por el procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas en la plataforma SAIA, bases de datos y servicios de información multiusuario, el cual debe comprender:

- a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Gobernación de Risaralda, por ejemplo que no compromete la separación de tareas.
- d) Entregar a los usuarios un detalle electrónico (link) de sus derechos de acceso.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Gobernación de Risaralda o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- Cancelar identificadores y cuentas de usuario redundantes
- Inhabilitar cuentas inactivas por más de 30 días

En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.


j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

7.1.8. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Se deben tener en cuenta los siguientes pasos:

- a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados.


Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

- d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

- e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

7.1.9. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal uso de la plataforma SAIA, mediante el cual deben respetarse los siguientes pasos:

- a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad. Ver anexo 3 Compromiso de Confidencialidad
- b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
- c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
- d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e) Configurar los sistemas de tal manera que:
 - Las contraseñas tengan combinación de letras (mayúsculas y minúsculas) y números, no menor a 8 caracteres,

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


- Suspendan o bloqueen permanentemente al usuario luego de tres (3) intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda),

7.1.10. Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.

f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad.

7.1.11. Responsabilidades del Usuario Uso de Contraseñas


Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- a) Mantener las contraseñas en secreto.
- b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
 1. Sean fáciles de recordar.
 2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

g) Notificar cualquier incidente de seguridad relacionado con sus contraseñas a la Dirección de Informática y Sistemas:

Pérdida, robo o indicio de pérdida de confidencialidad.


Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

7.1.12. Control de Acceso a la Red - Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Gobernación de Risaralda.


Para ello, se debe realizar una solicitud formal por la plataforma SAIA si es usuario interno con el respectivo aval del jefe de área o comunicado externo para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- a) Identificar las redes y servicios de red a los cuales se permite el acceso.
- b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

7.1.13. Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Gobernación de Risaralda. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos debe llevarse a cabo utilizando:

a) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que se implementara un procedimiento que incluya:

- Establecimiento de las reglas con el usuario.
- Establecimiento de un ciclo de vida de las reglas para su renovación.

b) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.


Los procedimientos y controles de re-llamada, o dial-back, brindan protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la Gobernación de Risaralda.

Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado de la Gobernación de Risaralda.

7.1.14. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Gobernación de Risaralda. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la Gobernación de Risaralda.

7.1.15. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el secretario o director de área a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.


Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares.

Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto “Compromiso de Confidencialidad”. Para ello, el Responsable de Seguridad Informática junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de “firewalls”, “proxies”, etc.

7.1.16. Control de Conexión a la Red

Sobre la base de lo definido en el punto “Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red.

Entornos a las que deben implementarse restricciones son:

- a) Correo electrónico.
- b) Transferencia de archivos.
- c) Acceso interactivo.
- d) Acceso a la red fuera del horario laboral.

7.1.17. Control de Ruteo de Red


En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de la Gobernación de Risaralda, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

7.1.18. Seguridad de los Servicios de Red

El Responsable de Seguridad Informática junto con el Responsable del Área Informática definirá las pautas para garantizar la seguridad de los servicios de red de la Gobernación de Risaralda, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad


Informática.

7.1.19. Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la Gobernación de Risaralda, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las PC's, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

7.1.20. Monitoreo del Acceso y Uso de los Sistemas - Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.


Los registros de auditoría deberán incluir:

- a) Identificación del usuario.
- b) Fecha y hora de inicio y terminación.
- c) Identidad o ubicación de la terminal.
- d) Registros de intentos exitosos y fallidos de acceso al sistema.
- e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

7.1.21. Factores de Riesgo

Entre los factores de riesgo que se deben considerar se encuentran:

- a) La criticidad de los procesos de aplicaciones.
- b) El valor, la sensibilidad o criticidad de la información involucrada.
- c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
- d) El alcance de la interconexión del sistema (en particular las redes públicas).


Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

Declaración de aplicabilidad

El Gobernador de Risaralda, los Secretarios de despacho, gerentes de entidades descentralizadas, Directores, funcionarios posesionados o contratistas y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Gobernación de Risaralda, cualquiera sea su situación

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

de vinculación, el área a la cual se encuentre afectada y cualquiera sea el nivel de las tareas que desempeñe.


Las máximas autoridades de la Gobernación de Risaralda aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información de la Gobernación de Risaralda, procederá a revisar y proponer a la máxima autoridad de la Gobernación de Risaralda para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la Gobernación de Risaralda y coordinar el proceso de administración de la continuidad de las actividades de la Gobernación de Risaralda

Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad de la Gobernación de Risaralda compartida por los Secretarios de despacho, gerentes de entidades

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

descentralizadas o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Conformación del Comité de Seguridad de la Información


Secretaría / Dirección	Representante
Planeación Departamental	Bleymirk Vargas Purgarin
Coordinación de Calidad	Lina María Alzate Castaño
Archivo General	Jhon Jairo Jiménez Valencia
Dirección de Recursos Físicos	Nicolai Andrei Vallejo Cano
Dirección de Informática y Sistemas	Ligelly Hernández Mayorga
Dirección de Informática y Sistemas	Frank Jhoanny Hernández
Asistencia legal	Invitad@
Control Interno	Invitad@

Ilustración 4 Propia

Este Comité tendrá entre sus funciones:


- Revisar y proponer a la máxima autoridad de la Gobernación de Risaralda para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro de la Gobernación de Risaralda.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información de la Gobernación de Risaralda frente a interrupciones imprevistas.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


DISEÑO METODOLÓGICO

Este documento por ser institucional en cumplimiento de la implementación del eje del tema temático Seguridad y privacidad de la información “Datos ciudadanos guardados como un tesoro, gracias a la seguridad de la información”, de la Estrategia Gobierno en línea, está dirigido a las personas que laboran en la Administración ya sean funcionarios o contratistas que en virtud de sus funciones deben interactuar con los diferentes sistemas de información institucionales.

La encuesta interna, se dirigió a 447 funcionarios y aproximadamente 100 contratistas que prestan sus servicios en el Edificio Departamental, para un total de 547 personas que conforman la población original, teniendo en cuenta que la encuesta fue diligenciada por 124 personas, se puede concluir que aproximadamente el 23% conforman la muestra de los encuestados.

La encuesta se compone de 8 preguntas y el análisis de las respuestas obtenidas reposa en las instalaciones de la Dirección de informática y sistemas

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

CONCLUSIONES

Con el fin de proteger los recursos de información de la Gobernación de Risaralda y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, se ha elaborado el presente Plan.


Se realizó basados en la normatividad vigente sobre la Estrategia Gobierno en Línea en su Eje Seguridad y Privacidad de la información, en la metodología de la investigación por medio de una herramienta técnica aportada por Microsoft y por una encuesta interna en la Administración donde se determinó los sistemas de información más sensibles que operan en la Gobernación y la percepción de seguridad informática de los diferentes usuarios de la misma y las necesidades puntuales en el tema seguridad de la información.

Lo anterior con el fin de identificar prioridades a tener en cuenta y establecer etapas de avance.

Igualmente se actualizó la Política de Seguridad informática de la Gobernación de Risaralda, asegurando su eficacia.

.

Aprobó:	Comité Sistema de Gestión de Seguridad Informática
Revisó:	Ligelly Hernández Mayorga - Directora de Informática
	Frank Jhoanny Hernández Restrepo - Contratista


	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
<p>Versión.0</p>	<p>Vigencia: Junio 2015</p>

RECOMENDACIONES

Para lograr el cumplimiento de las actividades propuestas en este documento, este debe ser oficializado en la plataforma de calidad de la Gobernación de Risaralda, debidamente socializado para todo el personal que labora en la entidad.

Se debe hacer un plan de acción de implementación con el comité SGSI institucional y hacerle seguimiento a su ejecución.

Aprobo: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015


REFERENCIAS BIBLIOGRÁFICAS

El nuevo Decreto de Gobierno en línea 2573 de 2014 que se puede consultar en el siguiente link:
<http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf>

El nuevo manual de Gobierno en línea que se puede consultar en el link <http://estrategia.gobiernoonlinea.gov.co/623/w3-propertyvalue-8011.html> (aún no disponible en PDF).

Adicionalmente se adjunta la presentación que se realizó a entidades del orden nacional y que se profundizará a nivel territorial en el esquema de acompañamiento que se habilitará en el mes de junio.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista


	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Ley 1712 de 2014 de Transparencia y de Acceso a la información que se puede consultar en el siguiente link

<http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf>

Decreto 103 de 2015 que reglamenta la Ley 1712 de 2014.
<http://www.archivogeneral.gov.co/sites/default/files/NoticiasAdjuntos/DECRETO%20103%20DEL%2020%20DE%20ENERO%20DE%202015.pdf> Es importante tener en cuenta que la ley 1712 y el decreto 103 tienen relevancia para la estrategia ya que contienen parámetros de información o secciones nuevas.

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

Anexo 2 Acta Compromiso de Confidencialidad

ACTA DE COMPROMISO DE CONFIDENCIALIDAD

En la ciudad de Pereira, Departamento de Risaralda, en mi calidad de servidor público y/o contratista de la administración central del Departamento de Risaralda a través de la presente acta, me comprometo a respetar las normas vigentes en materia de la información pública e implementar la responsabilidad por la **CALIDAD** de los datos y de la información y la **RESERVA** de la misma con fundamento en lo siguiente:

La Constitución de 1991 establece en su artículo 74 que *“Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”*. Y bajo este mismo entendido la Ley 1712 de 2014 estableció en su artículo 2 que *“Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley”*.


Dicha Ley 1712 de 2014 o de transparencia y acceso a la información en Colombia, plantea que se conocerá como información reservada aquella que afecte intereses públicos (artículo 19) y como clasificada aquella que afecte intereses particulares (artículo 18).

La Constitución Nacional establece que toda información del Estado es pública excepto aquella que por disposición legal sea reservada en aras de la seguridad y defensa del Estado. Así mismo en la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Que la Ley 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, establece en su artículo 4o. principios de la administración de datos que en el desarrollo,


Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

interpretación y aplicación de la presente ley, se tendrá en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

- a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;
- b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;
- c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos. Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;
- d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;
- e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Revisó: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p style="text-align: center;">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p style="text-align: center;">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p style="text-align: center;">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

CARACTERÍSTICAS GENERALES


- Toda información es pública, salvo disposición constitucional o legal.
- Es gratuito, salvo costo de expedición de copias.
- Debe ser oportuna, veraz, completa, reutilizable, procesable y estar en formatos accesibles. (Procedimientos de Gestión Documental).
- Hacer uso de procesos archivísticos que garanticen la disponibilidad en tiempo de documentos auténticos. (Archivo General de la Nación)
- Ámbito de aplicación. Todas las entidades públicas (3 Ramas del poder, nivel central y descentralizado), personas naturales y jurídicas que cumplen función pública, partidos o movimientos políticos.
- La información debe estar disponible en medios físicos, remotos o locales de comunicación electrónica (canales de atención). Asistir frente a los trámites y servicios que los requieran.

En conocimiento de lo anterior el uso de:

Soportes físicos. Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para modificar o almacenar los datos como documentos, oficios, formularios impresos, a mano o a máquina, fotografías, carpetas, expedientes, entre otros.

Soportes electrónicos. Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su

Aprobó: Comité Sistema de Gestión de Seguridad Informática
Reviso: Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista

	<p align="center">DEPARTAMENTO DE RISARALDA Secretaría Administrativa</p> <p align="center">GESTIÓN ADMINISTRATIVA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN</p> <p align="center">PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA GOBERNACIÓN DE RISARALDA</p>
Versión.0	Vigencia: Junio 2015

contenido para modificar o almacenar los datos como, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros), usb, correos electrónicos, almacenamiento en la nube y demás medios de almacenamiento masivo no volátil. Será sólo para uso dentro de la institución para fines administrativos, otro tipo de manejo será responsabilidad exclusiva del usuario que ingrese al sistema de Información, de tal forma que la institución queda exenta de toda responsabilidad en el caso del mal uso de la misma.

El uso inadecuado de la información y el incumplimiento de los procesos para publicar o entregar la información a terceros, parte del usuario será responsabilidad del usuario y queda exento el Departamento de toda consecuencia.

El servidor público y/o contratista comprometido:

Nombre del Usuario, cédula y cargo	
Firma	

Aprobó:
Revisó:

Comité Sistema de Gestión de Seguridad Informática
Ligelly Hernández Mayorga - Directora de Informática
Frank Jhoanny Hernández Restrepo - Contratista