PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

GOBERNACIÓN DE RISARALDA
2020

NÚMERO DE VERSIÓN

Versión	Responsable	Notas	Fecha
1.0	Equipo Secretaría TIC	Generación del documento	Octubre/2016
2.0	Equipo Secretaría TIC	Actualización marco normativo	Enero/2020

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

MARCO NORMATIVO

1. Decreto 1078 de mayo de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
2. Decreto 415 del 2016, "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".
3. Ordenanza 006 de mayo 26 de 2016. "Por la cual se adopta el Plan Departamental de Desarrollo para el periodo 2016–2019, *Risaralda verde y emprendedora*, y se dictan otras disposiciones"
4. Decreto 1413 de 2017, "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales".
5. Decreto 1008 de 14 de junio de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
6. Ley 1955 del 25 de mayo de 2019, "Por el cual se expide el plan nacional de desarrollo 2018-2022. "PACTO POR COLOMBIA, PACTO POR LA EQUIDAD""
7. Ley 1978 del 25 de julio de 2019 "por el cual se moderniza el sector de las tecnologías de la información y las comunicaciones –TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones"

INTRODUCCIÓN

El continuo uso de las tecnologías de información y comunicaciones trae consigo retos permanentes, lo cual conlleva al aumento de los delitos electrónicos, constituyendo como prioridad del mundo globalizado la protección de la información, por esto el gobierno nacional a través del ministerio de la tecnologías de información y comunicaciones (TIC) en su estrategia del gobierno en línea (GEL), plantea dentro de su estrategia la seguridad de la información, así mismo para la gobernación del Risaralda y teniendo en cuenta que hoy día la información se considera como un bien prioritario y se debe garantizar su acceso y protección al ciudadano, en consecuencia se crea el presente documento que será denominado “Plan del Sistema de gestión de seguridad de la información (SGSI V1)” versión uno. El cual contempla las estrategias para para ejercer la labor de control y protección frente a cualquier amenaza o incidente que pueda comprometer la información.

OBJETIVOS

Objetivo general

Fortalecer la gobernación del Risaralda para enfrentar las amenazas que atente contra la seguridad y tratamiento de la información.

Objetivos específicos

1. Crear instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional;
2. Diseñar y ejecutar planes de capacitación especializada en Seguridad de la información;
3. Fortalecer las políticas y verificar el cumplimiento de las normas en seguridad de la información

JUSTIFICACIÓN

Las Tecnologías de la Información y las Comunicaciones están en constante renovación y evolución, por ende, en la Ley 1978 de 2019 o Ley TIC se uestrna idhcas renovaciones dichas renovaciones De acuerdo a lo establecido por el ministerio de las TIC, plan de gobierno en línea GEL Decreto 2573 de 2014 Lineamientos generales de la Estrategia de Gobierno en línea 2015 Decreto 1078 de 2015 Decreto Único Sectorial. Donde los componentes son:

TIC para el Gobierno Abierto: Busca construir un Estado más transparente y colaborativo, donde los ciudadanos participan activamente en la toma de decisiones gracias a las TIC.
TIC para servicios: Busca crear los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos.
TIC para la gestión: Busca darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa.
Seguridad y privacidad de la información: Busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

Así mismo la ley 1273 de 2009 donde se crea el bien denominado “DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE DATOS” y la ley 1341 de 2009 “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC”, la ley 1712 de 2014 “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información Pública nacional” y según resolución 213 de 2014, la gobernación del Risaralda, se compromete a tener un sistema de gestión de Seguridad de la información actualizado.
Al mismo tiempo revisamos la diferencia entre seguridad de la información y seguridad informática con el fin de justificar el cambio de nombre del documento.

Seguridad Informática: su objetivo es resguardar las bases tecnológicas y de comunicación que soportan el movimiento en una empresa; el análisis de riesgos se centra en vulnerabilidades del hardware o software y pretende llevar a la organización a un el nivel de riesgo aceptable.

Seguridad de la información tiene como propósito proteger la información de una organización, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen. Recordando los principios fundamentales de la información como son: ***Confidencialidad,*** ***Integridad*** *y* ***Disponibilidad***.

Su radio de acción cubre Análisis de Riesgos, Seguridad del Personal, Seguridad física y del entorno, Gestión de comunicaciones, Desarrollo y Mantenimiento de Sistemas, Control de Accesos, Gestión de Incidentes, y Continuidad de Negocio entre otros (de acuerdo a la ISO27000). En este caso el riesgo de la gestión de la información se debe conservar en un nivel por debajo del asumible por la gobernación.

Por medio de la siguiente gráfica podemos diferenciar con mayor claridad el alcance de seguridad de la información y seguridad informática. Todas las áreas aquí ilustradas según ISO 27000, se encuentran dentro del alcance de la seguridad de la información, pero las áreas con color amarillo son las que se encuentran dentro del alcance de la seguridad de la informática (dependiendo de los recursos con los que cuente la Organización); Se puede evidenciar que el alcance de la seguridad de la información es mucho más amplio que el de la seguridad informática.

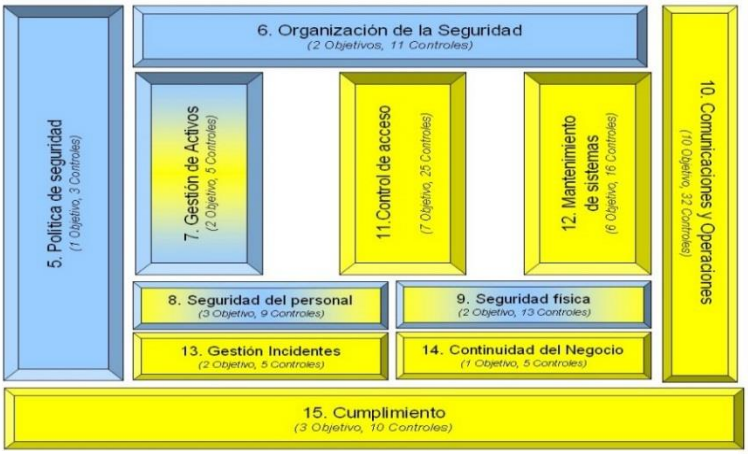

Ilustración 1, Seguridad Información & Seguridad informática

Fuente: Seguridad de la información en Colombia. 2010

FORMULACIÓN DEL PROBLEMA

El riesgo de información tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad.

El riesgo puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel. Se debe tener en cuenta que toda empresa tiene estos tipos de vulnerabilidades.

La Seguridad Física

Se define como la aplicación de barreras y procedimientos tanto físicos como lógicas frente a amenazas al hardware, así mismo son los controles y elementos de seguridad que garanticen desde la permanencia de los equipos en los sitios de trabajo hasta la buena conservación de estos.

Las amenazas más importantes que se prevén en este tipo de seguridad son:

1. Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
2. Amenazas ocasionadas por el hombre como robos o sabotajes
3. Disturbios internos y externos deliberados.

La Seguridad Lógica:

La Seguridad Lógica se refiere a la ejecución de protecciones y rutinas para proteger el acceso parcial o total de la información y que este sea restringido según los requerimientos del usuario en los sistemas. Así mismo es la protección de la información contra virus, robo de datos, alteración de la información, intrusiones no autorizadas o copias de seguridad no confiables

La seguridad lógica debe funcionar en conjunto con la seguridad física para mantener el bien más preciado en una organización como es la información.

Los puntos más importantes a considerar son:

- Agujeros de seguridad en: sistemas operativos, aplicaciones
- Error en la configuración de los sistemas de información.
- La falta de conocimiento de las políticas de seguridad por parte de los usuarios.
- Ataques frecuentes a los sistemas de información y sistemas operativos.

Riesgos causados por el Factor humano

El tercer nivel y el más crítico dentro de las empresas, dada su naturaleza impredecible, es la causada por el recurso humano. Las medidas a este nivel deberían ser más procedimentales, ligadas a la regulación y concienciación. Según varios estudios publicados, más del 75% de los problemas inherentes a la seguridad se producen por fallos en la configuración de los equipos o por un mal uso por parte del personal de la propia organización.

ALCANCE

El del sistema de gestión de Seguridad de la información (SGSI) es un manuscrito de alto nivel que expresa el compromiso del Gobernador del Departamento con la seguridad de la información. Este plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyada en el uso adecuado de TIC

Este plan es de aplicación en todas las Secretarías, direcciones, y dependencias que componen la Gobernación del Risaralda; a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal de Gobernación, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

Responsabilidades

La gobernación del Risaralda mediante resolución 0213 del 29 de agosto del 2014 creó el comité de seguridad de la información del departamento (CSIDR), el cual dentro de sus funciones tiene las siguientes:

- ✓ Revisar, aprobar y actualizar las políticas y estándares del SGSI
- ✓ Generar recomendaciones para la formulación y adecuación de las políticas, planes, programas y proyectos en materia de seguridad de la información y controles específicos de la seguridad para la implementación de nuevos sistemas o servicios.
- ✓ Realizar revisiones al SGSI, por lo menos dos (2) veces al año y según los resultados definir las acciones a seguir
- ✓ Planificar un análisis de la evaluación de los riesgos sobre seguridad de la información que se encuentran establecidos en el aplicativo SAIA, cada semestre
- ✓ Monitorear y revisar el plan de acción para mitigar y/o eliminar riesgos en seguridad de la información.

El Gobernador del Departamento de Risaralda aprueba la política de seguridad de la información y es responsable de la aprobación y adopción de las actualizaciones de dicha política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma integral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.
Al vincularse un funcionario a la gobernación contratista o funcionario dentro de la inducción, deberá ser notificado respecto al cumplimiento de las Políticas de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información.

Identificación, clasificación y valoración de activos de información.

Cada área o dependencia de la Entidad, con la colaboración del encargado de seguridad de la Información, y con base en el inventario de activos de la información, debe mantener un inventario de estos activos con la que se cuenta, ya sea procesada o producida. La forma y medios en donde se incorpore la clasificación, valorización, ubicación y acceso de la información, se especifican por medio del Comité de Seguridad de la Información, correspondiendo a la Dirección de informática y sistemas brindar herramientas que permitan la administración eficiente del inventario de información por cada área o dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos.

Seguridad de la información en el Talento Humano

Los servidores públicos de la Gobernación del Risaralda, independiente del tipo de vinculación laboral o contractual, la dependencia o área a la cual se encuentre adscrito y el nivel de funciones, tareas o actividades que desempeñe debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Dirección de Informática y Sistemas (DIS) debe mantener un directorio completo y actualizado de los perfiles creados. Así mismo deben cumplir con las políticas específicas para la prestación de servicio y salvaguardar la información.

Responsabilidades del personal de la Gobernación

Los servidores públicos de la Gobernación del Risaralda, independiente del tipo de vinculación laboral o contractual, secretaría o dependencia, a la cual se encuentre adscrito y las tareas o labores que desempeñe deben cumplir con las políticas establecidas para el manejo de la información institucional.

Los procedimientos para obtener los perfiles y las características de cada uno de los usuarios deben ser mantenidos y actualizados por cada departamento, secretaría o dependencia, de acuerdo a los lineamientos establecidos por DIS, en cuanto a los dispositivos de hardware y los elementos de software.

La gobernación del Risaralda en su plan de inducción y, en coordinación con DIS se encargará de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que proyecte la socialización y concientización individual y colectiva en temas de seguridad de la información en todo el personal.

La dirección de informática y sistemas deberá publicar en medios impresos y virtuales como intranet, correo electrónico, entre otros, información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de documentos, archivos, buenas prácticas, amenazas de seguridad, entre otros.

DIAGNÓSTICO

En esta etapa se pretende identificar el estado actual de la gobernación con respecto a los requerimientos de SGSI, se hará desde tres puntos de vista diferentes: diagnostico interno, perimetral (hacking ético), y de recursos humanos (encuesta a usuarios finales). Los resultados permitirán determinar las vulnerabilidades del sistema y el nivel de madurez de la seguridad y privacidad de la información en los usuarios de la gobernación. Así mismo medir el nivel de conocimiento de los temas de seguridad por parte de los usuarios de la Gobernación.

Diagnóstico Interno

Se iniciará con la visualización del mapa de procesos que se encuentra en 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 institución.

Además, de acuerdo a la priorización de los sistemas de información existentes realizada en SGSI V0, en la cual se priorizaron los sistemas de información a través de encuesta aplicada a los usuarios, de los cuales la siguiente tabla muestra los primeros cinco clasificados.

NOMBRE	DESCRIPCIÓN	MUY IMPORTANTE	IMPORTANTE	NO TAN IMPORTANTE	(en blanco)
Aplicativo Web	Sistema de Información de Contratación Pública – SECOP	84	29	4	7
SAIA	Sistema de Administración Integra de Información	80	34	4	6

NOMBRE	DESCRIPCIÓN	MUY IMPORTANTE	IMPORTANTE	NO TAN IMPORTANTE	(en blanco)
HumanoWeb	Sistema de Información de Gestión de Recursos Humanos – Nómina, Desprendible de Pago Mensual	70	47	4	3
Banco de Proyectos	Sistema de Información del Banco de Proyectos	68	45	4	7
SISAP	Sistema de Información Integrado de la Secretaría de Salud	61	42	11	10

Ilustración 2, priorización sistemas de información

Fuente: Plan de Gestión de la seguridad informática V0

El Aplicativo Web SECOP: es un instrumento de apoyo a la gestión contractual de las entidades estatales, que permite la interacción de las entidades contratantes, los proponentes, los contratistas, la comunidad y los órganos de control, que entre otras funcionalidades, permite a las entidades estatales cumplir con las obligaciones de publicidad de los diferentes actos expedidos en los procesos contractuales y a los interesados en participar en los procesos de contratación, proponentes, veedurías y a la ciudadanía en general, consultar el estado de los mismos.

La gobernación del Risaralda cuenta con el software de gestión documental **SAIA** que se diseñó con el fin de **centralizar** electrónicamente los **procesos** de gestión de la entidad. En los que se ven involucrados **información, documentos y responsabilidades,** permitiendo el flujo dinámico y controlado de la información, logrando **reducir** todos los **costos** administrativos asociados. Este software está 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 2568 de 2012, permite consultar la trazabilidad de los documentos durante el recorrido que **realiza internamente hasta obtener su respectiva respuesta y cierre; es un sistema con características** 100% Web. En este mismo software se maneja la parte de Peticiones Quejas y Reclamos PQR, lo cual cumple con la ley 1755 del 2015, Así mismo este software por el mismo módulo se reciben los requerimientos de acceso a la información, el cual cumple con la ley 1712 del 2014. Es de aclarar que frecuentemente se hace auditorías por parte de control interno del software.

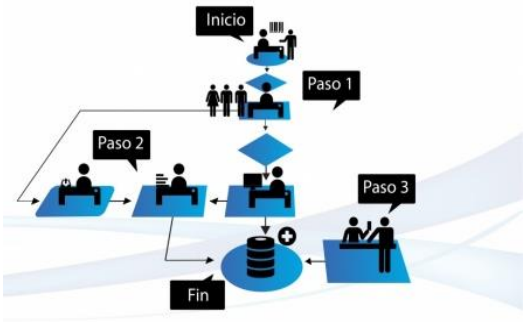

Ilustración 3, Sistema de Administración de información SAIA

Humano Web: Recursos Humanos es un área encargada de recopilar los datos de cada trabajador relativos a su historial y características personales, sus competencias y capacidades, hasta los datos más accesibles tales como sus remuneraciones y sus labores en la empresa. La cuantificación de estos datos y la sistematización para su tratamiento permite su manejo posterior por sistemas automatizados, reduciendo el tratamiento manual de las operaciones, costosa fuente de errores.

El Sistema de Información HUMANO es la base tecnológica que soporta la gestión integral de los procesos de Recursos Humanos en las entidades tanto del sector privado como público. la empresa Soporte Lógico Ltda. Presta servicios de soporte TI y soporta el software Humano web, el cual se encuentra funcionando en la gobernación desde el 2001 contando

actualmente con soporte técnico y actualizaciones permanentes según la legislación Colombiana.

SISAP: el Sistema de Información de Salud Pública SISAP es una solución informática desarrollada por la empresa Punto EXE, compuesta por varios módulos que se adaptan a las necesidades de los entes territoriales de Salud. Con estos módulos La gobernación puede tener el control vía web de la información del estado de la salud de la Población mediante la consolidación de Rips Validados, Informes Trimestrales de acciones de detección temprana y protección específica generada por los prestadores, Sistemas de Seguimiento a la Cohorte de Vacunación, TBC y otros pacientes de interés en Salud Pública, Valoración Nutricional, Gestión integral en Atención Primaria, Estado Actualizado de los sujetos de Inspección, Vigilancia y Control, Gestión integral y Auditoría de Base de Datos Única de Afiliados, SISBEN al Día, Gestión Integral y Auditoría para prestación de Servicios, Control de operaciones entre prestadores y entidades responsables de pago en la entidad, y la Gestión de sus funcionarios en las respectivas actividades tanto individuales como colectivas.

Diagnóstico Perimetral

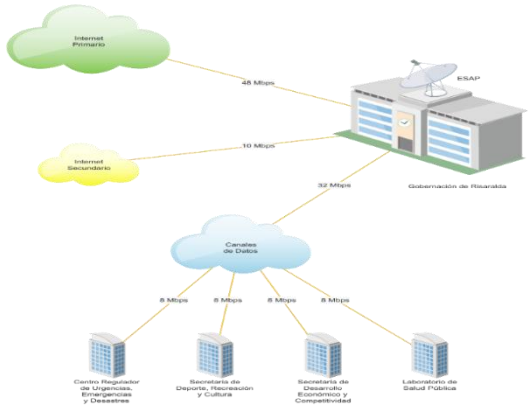

Ilustración 4, Plataforma de comunicaciones
Fuente: Plan Estratégico de Tecnología de la Información 2016

En esta parte describiremos la plataforma de comunicaciones de la gobernación la cual cuenta con un canal primario de 48 Mbps, uno secundario de 11 Mbps y otro de 32 Mbps con el cual interconecta las cuatros sedes externas como son el Centro Regulador de Urgencias Emergencias y Desastres (CRUED), secretaria de deportes recreación y cultura, la

secretaria de desarrollo económico y el laboratorio de salud pública como se visualiza en la ilustración 4.

La gobernación cuenta con un dispositivo UTM Fortigate 300C el cual tiene como objetivo optimizar la seguridad perimetral, implementando las mejores prácticas de seguridad mediante los servicios del equipo actualmente instalado, sin arriesgar la calidad y estabilidad del servicio. Este equipo cumple con las siguientes funciones:

- Servicio de navegación para aproximadamente 1200 usuarios concurrentes, aplicando políticas de firewall y perfiles de UTM, tales como Antivirus, Filtrado Web, control de aplicaciones, entre otros.
- Conexión con 4 sedes remotas a través de un canal de datos de 32Mps, es decir, 8Mbps por sede, a través de la cual se brindan servicios locales e internet a cerca de 100 usuarios.
- Publicaciones de servicios a través de Internet, con IPS en casi todas las publicaciones.
- Controlador Wireless de 12 AP actualmente y 3 SSID para el auditorio, empleados y visitantes.

La sede cuenta con una red completamente plana sin embargo, del fortigate 300C se usan 9 de las 10 Interfaces disponibles para separar servicios y aplicar políticas entre los segmentos de red físicos de la Gobernación de Risaralda.
En cuanto a la configuración actual el equipo éste está registrado a nombre de gerencia telemática hasta el 16 de noviembre del presente año como lo muestra la gráfica, la versión del firmware es 5.0, la utilización de recursos está por debajo del 80%.

Los servicios de seguridad habilitados son antivirus (AV), Data Leak Prevention (DLP), Intrusion Protection (IPS), Web Filter, Application Control y explicit Proxy). Tiene los siguientes puertos de gestión:

En las rutas estáticas están configuradas las salidas por los dos canales de internet, las conexiones SSLVPN, los accesos a las 4 sedes remotas y hacia el Cloud UNE-ETP.
El controlador de Wireless tiene 12 AP configurados, de los cuales 10 están activos, 3 SSID configurados similarmente, seguridad WPA/WPA2 – Personal encripción AES, pero con contraseñas diferentes.
El fortigate tiene configuradas 149 políticas de seguridad, pero no todas tienen perfiles de seguridad aplicados tales como Antivirus, Webfilter, Application Control, Intrusión Protection System, Data Leak Prevention y DoS. Las alertas son por detección de intrusos y cambios de configuración, las cuales se envían a la dirección de correo fortigate@risaralda.gov.co.

Diagnóstico del Recurso Humano

Para el diagnóstico del recurso humano se realizó una encuesta a usuario finales en la gobernación, para medir el nivel de conocimiento de seguridad de la información de usuarios y manejo de políticas de seguridad de contratistas. Es de aclarar que con esta encuesta se pretende verificar la información que tienen los usuarios acerca de la seguridad de la información y con ello generar nuevas políticas de capacitación o asistencia.
La presente encuesta sobre seguridad en los sistemas de Información institucionales, estuvo dirigida a todo el personal de la gobernación: funcionarios. Contratistas y aprendices SENA, es así que la población objeto fue de 1.057 personas, de los cuales el 39% respondió la encuesta lo que conlleva a tomar como población base en esta encuesta de 411 personas en adelante se denominará población.
Se compone de 16 preguntas organizadas bajo los siguientes temas:

- Identificación del usuario 3 preguntas.
- Estado de conocimiento frente al tema de seguridad informática 2 preguntas.
- Estado de conocimiento frente al tema de las políticas sobre seguridad de la información publicadas en la plataforma de calidad 6 preguntas.
- Aplicabilidad de la Ley 1712 del 2014 5 preguntas

Primera Pregunta

Para Usuario Final

¿Cuánto tiempo lleva laborando en la Gobernación de Risaralda?

Seis (6) meses Un (1) año Más de un (1) año otro

Segunda Pregunta

¿Qué tipo de vinculación tiene con la Gobernación de Risaralda?

Funcionario Contratista Aprendiz Sena

Tercera Pregunta

A qué secretaría de despacho está adscrit@?

SECRETARIA	**#**	**SECRETARIA**	**#**
Despacho Del Gobernador	20	Administrativa	59
Deporte, Recreación Y Cultura	17	Desarrollo Agropecuario	9
Desarrollo Económico Y Competitividad	13	Desarrollo Social	16
Educación	56	Gobierno	16
Hacienda	44	Infraestructura	20
Planeación	23	Salud	107
Jurídica	11	**TOTAL**	**411**

Ilustración 5, Encuestados por dependencia

Las tres primeras preguntas miden junto con el tipo de empleado, el tiempo que lleva laborando la persona en la gobernación relacionándola con la secretaria a que pertenece. Se concluye que de la población total el 66% son de la secretaría de Salud los cuales obtienen el porcentaje más alto de interacción con la encuesta, en contraste con el despacho del gobernador donde solo el 24% la diligenciaron. En conclusión en esta encuesta se denota más compromiso por los funcionarios que lleva más tiempo laborando en la gobernación y que pertenecen a la secretaría de salud que los contratistas o aprendices SENA.

Cuarta Pregunta

Ha recibido inducción en el último año?

Sí _____ No_____

Quinta Pregunta

Tiene conocimiento de las políticas y buenas prácticas en el uso de Internet y los recursos informáticos?

Sí _____ No_____

Estas dos preguntas las enlazamos para medir el conocimiento de las políticas de seguridad de la información y la inducción recibida en el último año, según la respuesta esta relación no es directamente relacionada ya que el 91% de la población de la encuesta dice tener conocimientos de seguridad, pero solo el 59% de estos han recibido inducción y/o reinducción en este año. Estas preguntas se analizaron juntas ya que se pretende generar como política, que en las futuras inducciones se hable sobre la seguridad informática.

Sexta Pregunta

Tiene usted una clave para uso de uno o más aplicativos en la gobernación?

Sí _____ Que aplicativos _____ No_____

Séptima Pregunta

Usa o ha usado claves de otras personas para ejecutar labores propias de su cargo

Sí _____ No_____

Octava Pregunta

Alguna vez le ha prestado su contraseña a otro funcionario para que trabaje en un sistema de información:

Sí _____ Que sistema: _____ No_____

Novena Pregunta

Abre usted correos de origen desconocido?

Sí _____ No_____

Décima Pregunta

Descarga usted información desde internet?

Sí _____ Que tipo de información No_____

Undécima Pregunta

¿Tiene usted información de la gobernación almacenada en dispositivos externos (USB, Disco Duro, CD's) ?

Sí _____ Que dispositivos No_____

Estas preguntas están relacionadas con las políticas sobre seguridad de la información publicadas en la plataforma de calidad, la respuesta debe ser congruentes con el desconocimiento de dichas políticas el cual es solo del 9%, este desconocimiento es congruente con el 10% que no cumplen con estas políticas. Debemos recordar que los mayores ataques de seguridad se presentan en el interior de la entidad y no por fuera, Así mismo analizaremos que las políticas que más se violan son la descarga de información desde internet y guardar información de la entidad en medios externos 40% y 34% respectivamente. Con esto entendemos que debemos generar una mayor concientización de usuarios finales.

Duodécima Pregunta

Sabe usted clasificar la información que maneja en: Pública clasificada o Pública reservada?

Sí _____ No_____

Decimotercera Pregunta

Maneja datos públicos reservados?

Sí _____ No_____

Decimocuarta Pregunta

¿Realiza copia de seguridad de la información manejada?

Sí _____ No_____

Decimoquinta Pregunta

Considera que se le ha socializado sobre la seguridad de la información por parte de la Gobernación?

Sí _____ No_____

Decimosexta Pregunta

Le gustaría recibir información acerca de seguridad en la información?

Sí _____ No_____

Las últimas cinco preguntas son sobre seguridad de la información, es de aclarar que con esta indagación se pretende, verificar la formación de los usuarios acerca del manejo de información y con ello generar nuevas políticas de capacitación o asistencia en el manejo adecuado de ésta. Igual se visualiza que el 44% del usuario no tiene conocimiento sobre la clasificación de la información, mientras el 73% dice no manejar datos públicos reservados, también pudimos evaluar que el 52% no realiza copia de seguridad de su información contrastando con el 59% que dice haber recibido información sobre seguridad de la información.

En general con los resultados de la encuesta podemos visualizar que a pesar de que los funcionarios de la gobernación tienen algún conocimiento de seguridad, Es necesario crear mecanismos de difusión para una mayor apropiación por parte del personal que labora en la institución.

CLASIFICACIÓN DE LA INFORMACIÓN

La información propiedad de la Gobernación de Risaralda se considerará por defecto, correspondiente a toda la información "**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 información 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 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).

Acuerdos de confidencialidad y derechos de propiedad intelectual

Mientras persista una relación laboral con la Gobernación, todos sus funcionarios y contratistas ceden a la entidad los derechos de propiedad intelectual de los desarrollos que originen como parte de sus responsabilidades laborales y contractuales con la institución.

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 que se encuentra implementado en la herramienta SAIA..

ADMINISTRACIÓN DE LOS RIESGOS YA IDENTIFICADOS EN EL SISTEMA DE GESTIÓN DE CALIDAD.

Clasificación	Tipo	Riesgo	Tratamiento
Inventario Sistemas De Información	Software	Pérdida de Información	Aplicar control
Inventario De Bienes	Bienes	Bienes no Asegurados	Aceptado
	Almacenamiento de elementos	Falta de controles sobre los bienes almacenados	Aplicar control
Inventario De Expedientes	Documentos	Uso inadecuado de SAIA	Aplicar control
	Expedientes	Pérdida de expedientes	Aplicar control
Inventario Del Recurso Humano	Historias laborales	Pérdida o sustracción	Aplicar control
Manejo Inadecuado de Sistemas De información	Humano	Uso inadecuado de SAIA	Aplicar control

Ilustración 6, Cuadro de riesgos

Evaluación de Riesgos

Se realiza identificación y evaluación de las amenazas y vulnerabilidades relativas a los activos de información ya sean sistemas de información, infraestructura, bienes o de recurso humano, la probabilidad de que ocurran y su potencial impacto en la operación de la Gobernación de Risaralda. Se realiza la siguiente clasificación por activo.

Riesgo	Área Responsable	Tipo de Riesgo	Probabilidad Nivel	Impacto Nivel	Riesgo No.
Pérdida de Información	Despacho de la Secretaría de Salud	De tecnología	1: Raro	4: Mayor	1
	Secretaria de infraestructura Dirección técnica	Operativo	4: Probable	3: Moderado	4
Bienes no Asegurados	Dirección de recursos físicos	Financieros	1: Raro	3: Moderado	1
Falta de controles sobre los bienes almacenados	Dirección de recursos físicos	Financieros	1: Raro	3: Moderado	2
Uso inadecuado de SAIA	Archivo del Departamento	Operativo	3: posible	2: Menor	3
Pérdida o sustracción	Dirección de Recursos Humanos	Operativo	1: Raro	3: Moderado	15
Pérdida y/o posible daño de documentación	Archivo del departamento	Operativo	1: Raro	3: Moderado	1
Conservación inadecuada de los documentos	Archivo del departamento	Operativos	3:Posible	3: Moderado	4

Ilustración 7, análisis de riesgos

Gráfica sobre los riesgos relacionados con seguridad de la información

PROBABILIDAD	IMPACTO				
	Insignificante -1	Menor -2	Moderado -3	Mayor -4	Catastrófico -5
Raro (1)	B	B	**Riesgo 1 y 2 Recursos Físicos Riesgo 15 Recursos Humanos Riesgo 1 Archivo**	**Riesgo 1 Salud**	
Improbable (2)	B	B	M	A	E
Posible (3)	- -	**Riesgo 3 Archivo**	**Riesgo 4 Archivo**		E
Probable (4)	-	A	**Riesgo 4 Infraestructura**	E	E
Casi seguro (5)	A	A	E	E	E

B: Zona de riesgo baja: Asumir el riesgo

M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo

A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Ilustración 8, Gráfica de Riesgos

La gráfica muestra el conjunto de riesgos relacionados con Seguridad de la información, concluyendo que la pérdida de información para la Secretaría de salud e infraestructura y la conservación inadecuada de los documentos en Archivo, están en la zona de riesgo alta es de anotar que cuando el riesgo se encuentra en esta zona se deben tomar medidas preventivas para minimizarlo o trasladarlo como manda la norma. Igualmente se deben

revisar y generar controles de los demás riesgos ya que todos se encuentran en la zona de riesgo moderado

La gráfica individual y el seguimiento de cada uno de los riegos se pueden visualizar en la plataforma de calidad de la Gobernación en la sección de “riesgos”.

Otras dependencias como presupuesto, tesorería, contabilidad tienen riesgos del manejo de información con mayor énfasis en el área financiera, lo que genera en algunos casos la elaboración de información errada para el público. De esta manera, el manejo de la información se convierte en una prioridad para nuestra institución.

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

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.

Alcance

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.

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 Gateway, 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 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.

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 identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticación de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad de operación.
- 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 dirección de control interno 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.

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.
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.

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.

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, este procedimiento se encuentra descrito en las 'políticas de operación de administración de sistemas de información' la cual está publicada en el proceso de Gestión de tecnología de la información – Políticas de operación del proceso.

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.
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.

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 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.

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

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 justificaran 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 se comparta la responsabilidad o en su defecto en ausencia de un usuario, el otro pueda ejecutar la acción requerida.

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.
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.

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) Cambiar la contraseña siempre que exista un posible indicio de compromiso del sistema o de su respectiva clave.
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.
    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.

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 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.

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 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, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
   - Asignación de la herramienta de autenticación.
   - Registro de los poseedores de autenticadores.
   - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
   - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
   - Establecimiento de las reglas con el usuario.
   - Establecimiento de un ciclo de vida de las reglas para su renovación.
c) 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, pueden brindar 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.

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 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. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definiran y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso, el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad Informática, el esquema más apropiado a implementar.

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”, “proxis”, etc.

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

Algunos ejemplos de los 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.

Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Organismo, 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.

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:

- 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.

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.

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.

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.

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 de vinculación, el área a la cual se encuentre afectado 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 descentralizadas o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de algunas secretarías, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Conformación del Comité de Seguridad de la Información

Secretaría / Dirección	Representante
Planeación Departamental	José Bleymirk Vargas Purgarin
Coordinación de Calidad	Lina María Álzate Castaño
Archivo General	Jhon Jairo Jiménez Valencia
Dirección de Recursos Físicos	Juan Guillermo López Montoya
Dirección de Informática y Sistemas	Ligelly Hernández Mayorga
Dirección de Informática y Sistemas	Nubia Estella Gallego C.
Asistencia legal	Invitad@
Control Interno	Invitad@

Ilustración 10, Integrantes comité de seguridad

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.
- 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.

POLÍTICAS DE LA DIRECCIÓN DE INFORMÁTICA

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.

La red interna deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red de la Gobernación.

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.

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.

Trabajo remoto

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 Pública Clasificada o Pública 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.

Para ingresar remotamente a los equipos de la gobernación, solo se hará con la previa autorización del usuario encargado de la base de datos y bajo estricta supervisión, previo conocimiento de la labor que se adelante. las claves para dicho accesos solo deben ser conocidas por el delegado de la dirección de informática y por la persona o entidad que

ingrese a nuestro sistema, estas claves son total responsabilidad del área de sistemas y debe ser una c

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, esta será implementada en la inducción y/o reinducción, la cual se hará por lo menos una vez cada año.

Escritorios y pantallas limpias

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

Todos los funcionarios deberán mantener sus equipos de cómputo limpios, aplicaciones cerradas al retirarse del equipo por más de diez minutos, todas las aplicaciones deben quedar cerradas y la información en el equipo o escritorio debidamente salvaguardada, 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 re-asignar un equipo de cómputo de un funcionario que almacene en éste información clasificada como "**Pública Clasificada**" o **"Pública 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).

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 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 "**Pública Clasificada**" o **"Pública 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 a la persona encargada de la Información.

Los usuarios de los sistemas de información no deben, bajo ninguna circunstancia, 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.

Para la implementación del presente plan y con el fin de atenuar los riegos se crearon algunas políticas y se actualizaron otras, las políticas que se deben cumplir para asegurar la información en la gobernación son:

- Políticas de operación de tecnologías de la información
- Políticas de operación de soporte de usuarios
- Políticas de operación de administración informática
- Políticas de operación seguridad informática
- Políticas de operación para la seguridad de la información aplicables al personal de la Dirección de Informática y Sistemas
- Políticas de operación para el uso de tarjetas de proximidad del centro de datos.

Estas políticas se deberán revisar periódicamente y realizar un seguimiento para lo cual se tendrán formatos y plantilla que se requerirán cuando se realice seguimiento al presente plan. Estas políticas se encuentran en la plataforma de calidad – Gestión de tecnologías de la información – Políticas de operación de proceso. A continuación se muestra la política de seguridad de la información de la gobernación.

Política de Seguridad de la información de la Gobernación de Risaralda

Declaración De La Política De Seguridad

La Gobernación de Risaralda es la administración central del Departamento 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 decido implantar un sistema de gestión y suscribe la presente política.

Política De Seguridad De La Información

El Departamento de Risaralda establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) encaminados a mejorar su seguridad, entendiéndose 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 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.

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.

Cuentas de usuario de los sistemas

El acceso a los sistemas de información será controlado por medio de nombre 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 Trasparencia, Articulo 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 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.

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.
Adicionalmente se crean las siguientes recomendaciones por puntos particulares.

Seguridad física:

- Modernizar el acceso físico en la institución, este podría incluir el uso de sistemas biométricos y vigilantes para acceso en áreas específicas.
- Generar controles a nivel de equipos, tales como ubicación y protección, seguridad y actualización del cableado estructurado.
- Gestionar medios de almacenamiento removibles.
- Controlar las vulnerabilidades técnicas.

La Seguridad Lógica:

- Restringir el acceso a los programas y archivos para usuarios y administradores, se deben crear claves adecuadas de consulta, este caso es evidente en SAIA donde dicha clave permite bajar documentación de la gobernación y no realizar una consulta como el software lo específica.
- Asegurar que se estén utilizados los datos, archivos y programas correctos y por el procedimiento correcto.
- Revisar que la información transferida sea la correcta y recibida sólo por el destinatario al cual ha sido enviada.

- Verificar la existencia planes de contingencia para comunicaciones entre diferentes puntos.
- Controles de acceso lógico con la gestión de usuarios, perfiles y privilegios para acceso a aplicaciones y gestión de contraseñas.
- Controles de acceso a la red interna y externa, segregación en redes y controles para asegurar servicios de la red.
- Instalar protocolos para intercambio y cifrado de información.
- Monitoreo de los sistemas, sincronización de relojes y protección sobre registros.
- Verificar que se tengan tiempos de conexión a aplicativos y cierres de sesión por inactividad.
- Crear VLANS de acuerdo a grupos de usuarios
- Crear un firewall de contención interna

Riesgos causados por el Factor humano

Las medidas a este nivel deberían ser más procedimentales, ligadas a la regulación y concientización. Dentro de éstas se pueden incluir:

- Hacer seguimiento a las políticas de seguridad con el fin de dar cumplimiento.
- Generar Controles relacionados a acuerdos con terceros, prestación de servicios que se puedan dar con éstos y segregación de funciones.
- Hacer gestión antes, durante y después de la terminación de los contratos.
- Crear programas de formación permanente al personal en aspectos de seguridad de la información.
- Crear procedimientos e instructivos para manejo de información.
- Como estamos trabajando en plataformas web se debe tener un sistema de doble autenticación, como opción se podría pensar en tener una intranet a la cual accederíamos con la contraseña y dentro de esta intranet encontraríamos los aplicativos a los cuales podemos acceder desde cualquier lugar.
- Se debe crear el cargo de oficial de seguridad estipulado en la ley de protección de datos.

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 presenten 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 norma ISO 27001 y por una encuesta interna en la Administración donde se determinó el conocimiento de los usuarios acerca de la seguridad de la información, así como el cumplimiento de las políticas existentes en el manejo de dicha seguridad.

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

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

GLOSARIO DE TÉRMINOS

Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas:

- Impresa
- Almacenada electrónicamente
- Transmitida por medios electrónicos
- Mostrada en videos
- Suministrada en una conversación
- Conocimiento de las personas
- Alcance de la auditoría: Extensión y límites de una auditoría.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

Análisis de Riesgos: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Audiovisuales: Colección conformada por videos, disquetes, casetes, usb, microfichas, CD-ROM, discos duros y cintas.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

Auditado: Organización o Dependencia a la cual se le vá a realizar una auditoría.
Auditor: Persona con la competencia para llevar a cabo una auditoría.

Auditor en seguridad de la información: Persona con la competencia para efectuar auditorías internas de seguridad de la información

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Conclusiones de auditoría: Resultado de una auditoría, proporcionada por el equipo auditor después de la consideración de los objetivos de la auditoría y de todos los hallazgos de auditoría.

Conformidad: cumplimiento de un requisito.
Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Criterios de auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como una referencia frente a la cual se compara la evidencia de la auditoría.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.

Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.
Equipo auditor: Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.

Estimación del riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad de la información.

Evidencia de auditoría: Registros, declaraciones de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoría puede ser cuantitativa o cualitativa.

Evitar el riesgo: Decisión de la organización de no involucrarse en una situación de riesgo o tomar acciones para retirarse de dicha situación.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

Hallazgo de auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Información: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
Integridad: La información de ISAGXXX debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

La Dirección: Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa.

No conformidad: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

No conformidad mayor: El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades.

No conformidad menor: El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento.

No conformidad potencial: Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia.

Observación: Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar.

Observador: Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo.

Perfil de uso:

Plan de auditoría: Descripción de las actividades en el sitio y arreglos para una auditoría.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Proceso: conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

Programa de auditoría: Conjunto de una o más auditorías planificadas para un período de tiempo específico y dirigido hacia un propósito específico.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.

Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

Riesgo Inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

Riesgo Residual: Nivel restante de riesgo después de su tratamiento.

Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa información y tiene valor para la organización, como bases de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la empresa. La información, como activo corporativo, puede existir de muchas formas: Impresa, Almacenada electrónicamente, Transmitida por medios electrónicos, Mostrada en videos, Suministrada en una conversación, Conocimiento de las personas

Alcance de la auditoría: Extensión y límites de una auditoría.

Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.

Análisis de Riesgos: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
Audiovisuales: Colección conformada por videos, disquetes, casetes, usb, microfichas, CD-ROM, discos duros y cintas.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permiten determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.

Auditado: Organización o Dependencia a la cual se le vá a realizar una auditoría.
Auditor: Persona con la competencia para llevar a cabo una auditoría.

Auditor en seguridad de la información: Persona con la competencia para efectuar auditorías internas de seguridad de la información

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la organización. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Conclusiones de auditoría: Resultado de una auditoría, proporcionada por el equipo auditor después de la consideración de los objetivos de la auditoría y de todos los hallazgos de auditoría.

Conformidad: cumplimiento de un requisito.

Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una compañía. Un control incluye entre otras: la definición de políticas, la puesta en marcha de procedimientos, la definición de guías, la definición de cambios en una estructura organizacional, o la ejecución de buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Criterios de auditoría: Conjunto de políticas, procedimientos o requisitos utilizados como una referencia frente a la cual se compara la evidencia de la auditoría.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Declaración de aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la compañía.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante nuestros clientes.

Efectividad: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.
Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

Eficiencia: Relación entre el resultado alcanzado y los recursos utilizados.

Equipo auditor: Uno o más auditores que llevan a cabo una auditoría con el apoyo, si es necesario, de expertos técnicos.

Estimación del riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.

Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc.), asociada a una posible violación de la política de seguridad de la información, falla en controles y contramedidas, o que implica una situación desconocida que puede ser pertinente a la seguridad de la información.

Evidencia de auditoría: Registros, declaraciones de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoría puede ser cuantitativa o cualitativa.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al Riesgo dentro de una organización.

Hallazgo de auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de la auditoría.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo asociados a la seguridad de la información.

Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos del negocio.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.

Integridad: La información de ISAGXXX debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la Empresa a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen o pérdidas financieras.

La Dirección: Es la encargada de combinar los recursos humanos y técnicos lo mejor posible para conseguir los objetivos de la empresa; está conformada por la presidencia y directivos, quienes se encargarán de desarrollar los planes a largo plazo de la empresa.

No conformidad: El no cumplimiento de un requisito especificado. También puede denominarse no conformidad real.

No conformidad mayor: El no cumplimiento de un requisito debido a la falta frecuente o deliberada de cumplimiento de un requisito documentado en el sistema, incumplimiento de requisitos legales o reglamentarios, múltiples no conformidades menores dentro del mismo requisito de la Norma o la falta deliberada en corregir No Conformidades.

No conformidad menor: El no cumplimiento de un requisito sin que exista una amenaza relevante o significativa para el Sistema de Gestión de Calidad o cuando sea una instancia aislada de incumplimiento.

No conformidad potencial: Evento en el cual no hubo No Conformidad, pero en caso de repetirse pudiera serlo, por la existencia de un riesgo. Una acción preventiva pudiera ser tomada para evitar su ocurrencia.

Observación: Apartado del informe de auditoría en el que el auditor deja constancia de las oportunidades de mejora, de los riesgos para la calidad o de cualquier otro detalle que haya observado y le parece relevante registrar.

Observador: Integrante del equipo auditor que se encuentra en proceso de entrenamiento y su objetivo es adquirir competencia mediante la observación. Algunas veces apoya al equipo auditor tomando notas de los hallazgos de la auditoría en las listas de chequeo.

Plan de auditoría: Descripción de las actividades en el sitio y arreglos para una auditoría.

Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Proceso: conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.

Programa de auditoría: Conjunto de una o más auditorías planificadas para un período de tiempo específico y dirigido hacia un propósito específico.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.

Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.

Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la información en los activos de una empresa.

Riesgo Inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde se presenta. Es propio de las actividades que conlleva el proceso relacionado.

Riesgo Residual: Nivel restante de riesgo después de su tratamiento.
Riesgo en la seguridad de la información: Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño a la organización.

Seguridad de la información: preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTC-ISO/IEC 27001:2005).

SGSI: Sistema de Gestión de Seguridad de la Información.

Transferencia del riesgo: Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

Tratamiento de la Información: Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Vulnerabilidades: Debilidad de un activo de información frente a una amenaza, preservación de la integridad, la confidencialidad, y la disponibilidad de la información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTC-ISO/IEC 27001:2005).

S.G.S.I: Sistema de Gestión de Seguridad de la Información.

Transferencia del riesgo: Compartir con otra de las partes la pérdida (consecuencias negativas) de un riesgo.

Tratamiento de la Información: Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Valoración del riesgo: Proceso global de análisis y evaluación del riesgo.

Vulnerabilidades: Debilidad de un activo de información frente a una amenaza.

REFERENCIAS BIBLIOGRÁFICAS

Decreto 103, 2015
http://www.archivogeneral.gov.co/sites/default/files/NoticiasAdjuntos/DECRETO%20103%20DEL%2020%20DE%20ENERO%20DE%202015.pdf

Decreto 2573, 2014
http://wp.presidencia.gov.co/sitios/normativa/decretos/2014/Decretos2014/DECRETO%202573%20DEL%2012%20DE%20DICIEMBRE%20DE%202014.pdf
Internet, Agosto 2016

Manual Gobierno en línea, 2015
http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8011.html
Internet, agosto de 2016

Seguridad de la información en Colombia, 2010
http://seguridadinformacioncolombia.blogspot.com.co/2010/02/seguridad-de-la-informacion-y-seguridad.html.
Internet, (agosto, 2016)

Ley 1712, 2014
http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf
Internet, (Septiembre, 2016)

Anexo 1 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, 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;

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 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	

Anexo 2 Tablas de retención documental

Se encuentran en la página web en la sección Normatividad políticas y lineamientos – otras http://www.risaralda.gov.co/site/main/intradocuments/webExplorer/otras_publicaciones_483#otras