Risaralda Verde y emprendedora / Gobernación de Risaralda	**INFORME DE SEGUIMIENTO AL PLAN DE MEJORAMIENTO**

NUMERO DE PLAN	670
PROCESO AUDITADO	GESTION DE TECNOLOGIAS DE LA INFORMACION
NOMBRE DE LA ENTIDAD QUE SUSCRIBIO EL PLAN	GOBERNACION DE RISARALDA
NOMBRE DEL REPRESENTANTE LEGAL	Sigifredo Salazar Osorio
NOMBRE DEL JEFE DE CONTROL INTERNO	Ruby Lucia Aguirre Torres
FECHA SUSCRIPCION DEL PLAN DE MEJORAMIENTO	2016-12-28
FECHA DE SEGUIMIENTO A COMPROMISOS	2017-08-10
RESULTADOS DE SEGUIMIENTO Y CONTROL	
CUMPLIMIENTO DEL OBJETIVO GENERAL DEL PLAN	Se cumple en un 89% con el objetivo general del plan, teniendo en cuenta que de las 9 acciones propuestas, 8 de ellas cumplen en un 100%, pero la actividad No. 9 no reporta evidencias de lo realizado. Por tal razón no hay forma de validar lo dicho.
CUMPLIMIENTO DE LOS OBJETIVOS ESPECIFICOS	Cumple parcialmente.
PORCENTAJE DE CUMPLIMIENTO DEL PLAN	100%
CONCLUSIONES	Sería pertinente adjuntar la evidencia de la actividad No. 9 con el fin de cumplir con el 100% del plan de mejora.

No	DEFICIENCIA ADMINISTRATIVA	COMPROMISOS DE MEJORAMIENTO SUSCRITOS	RESPONSABLE	TERMINO	INDICADORES DE CUMPLIMIENTO	LOGROS ALCANZADOS	PORCENTAJE DE CUMPLIMIENTO	OBSERVACIONES
1	Se evidenció la utilización del toma corriente regulado (Naranja), para conectar aparatos eléctricos diferentes a los equipos de cómputo, la utilización de este circuito regulado para la conexión de equipos diferentes a los informáticos pueden llegar a causar daños irreparables a los demás equipos informáticos que a su vez se encuentre conectados a dicha red.	Realizar revisión para identificar este tipo de conexiones y subsanar la anomalía. - Difundir, a través de mensaje, el cuidado que se debe tener con el uso de los tomas regulados	Alejandro Usma Vasquez	2016-12-14	-Mensaje de socialización con la recomendación requerida. - Recomendaciones en las fichas de los equipos cuando se realizan recorridos.	• -Se trasmite mensaje instantaneo y correo con recomendaciones en el manejo de tomas regulados -Se realiza visitas a puestos de trabajo para validar recomencaciones	100%	Se adjuntan evidencias
2	Se comprobó el consumir líquidos cerca a los equipos de cómputo por parte de los usuarios, lo cual ocasionaría daños irreparables a los equipos en caso de derrame.	Difundir infromación sobre las politicas, en particular las que tienen que ver con el consumo de alimentos en los puestos de trabajo	Alejandro Usma Vasquez	2016-12-30	Mensajes enviados para recordar politicas de operación mediante los diferentes medios.	• Se realiza divulgación de las politicas de operación mediante diferentes medios incluyendo SIGyC y capacitacion a funcionarios. Se realizan además barridos periodicamente por personal de la Dirección de informática para la eliminación de software.	100%	Se anexa divulgación de las políticas de operación mediante capacitaciones
3	Se observó la caducidad en la licencia del Antivirus de algunos equipos de cómputo.	Adquirir licencias para dar cubrimiento en la totalidad de equiposDar cubrimiento de licencias antivirus a todos los equipos de la Gobernación.	Alejandro Usma Vasquez	2016-12-30	Licencias adquiridas para cubrir la necesidad de la administración.	• En el año 2016 se amplió la cobertura de antivirus adquiriendo 100 licencias adicionales. En el presente año se amplio cobertura con 50 licencias adicionales	100%	Se anexa contratos de compra y soporte
4	Se evidenció música e imágenes de carácter personal, almacenados en los equipos de cómputo.	Realizar difusión sobre las políticas de la Dirección de Informática	Alejandro Usma Vasquez	2016-12-30	Mensajes publicados sobre las politicas de operación	• Se realiza divulgación de las politicas de operación mediante diferentes medios incluyendo SIGyC y capacitacion a funcionarios. Se realizan además barridos periodicamente por personal de la Dirección de informática para la eliminación de software.	100%	Se anexa evidencia de capacitación
5	Se detectó el paquete de juegos habilitado en algunos equipos, lo cual se encuentra prohibida dentro de las Políticas de Operación de Seguridad Informática.	Eliminación de juegos en puestos de trabajo	Alejandro Usma Vasquez	2016-12-30	Socialización de politicas de la Dirección de informática	• Se realiza divulgación de las politicas de operación mediante diferentes medios incluyendo SIGyC y capacitacion a funcionarios. Se realizan además barridos periodicamente por personal de la Dirección de informática para la eliminación de software. Se eliminan privilegios de administrador en equipos de cómputo.	100%	Se anexa evidencia de capacitación
6	El subproceso de GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN, suscribió el día 13 de enero de 2016 el Plan de Mejoramiento No. 517 por hallazgos negativos en auditoria de Seguimiento y Evaluación a la Seguridad Informática en el año 2015, el cual	Adicionar la evidencia respectiva a cada hallazgo	Alejandro Usma Vasquez	2016-12-15	Hallazgos con su respectivo documento adjutno en el que se evidencie el tratamiento correspondiente	• En el mes de agosto se adjuntan las evidencias respectivas	100%	

	registra un seguimiento el 22 de julio del presente año, donde se reporta un porcentaje de cumplimiento del 100%, lo cual no es coherente con lo detectado en la presente auditoria, además que al verificar los avance de este plan de mejoramiento no se registran ninguna evidencias teniendo en cuenta los hallazgos relacionados.							
7	Sería pertinente realizar periódicamente la socialización de las políticas de operación de la seguridad informática a los funcionarios y contratistas de la Administración Departamental por todos los medios (SAIA, SPARK, Correo Electrónico).	Divulgar las diferentes politicas de seguridad de la información a traves de los diferentes medios de difusión	Alejandro Usma Vasquez	2017-02-28	Mensajes de difusión sobre políticas de seguridad de la información	• Se realiza proceso de divulgación a través de diferentes medios, incluyendo plataforma SAIA y capaciotacion a personal	100%	Se anexa evidencia de capacitación
8	Los equipos informáticos de los funcionarios o contratistas auditados posee gran vulnerabilidad ya que el 68% de las cuentas de los usuario auditadas poseen privilegios administrativos, habilitando al usuario el acceso al sistema con poder de alterarlo en su funcionamiento o la instalación de paquetes informáticos no licenciados, la Norma NTC-ISO-27001 propone procedimientos para mitigar el riesgo como es: - NTC-ISO-27001/A.11.2.2 nos sugiere: Se debe restringir y controlar la asignación y uso de privilegios. - NTC-ISO-27001/A.11.2.4 nos sugiere: La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.	Solicitar al proveedor del software una solución en cuanto a los niveles de privilegios necesarios para la ejecucion del aplicativo a través de windows.	Ligelly Hernandez Mayorga	2017-01-31	Solicitud enviada al proveedor para el ajuste pertinente al aplicativo	• Se hace la verificación con el personal técnico sobre la configuración de los usuarios administradores quedando de la siguiente forma: En ninguna máquina de la Gobernación debe quedar el usuario administrador para uso del usuario final por medio memorando a las áreas relacionadas con la administración de recursos informáticos No.2089 del 14/02/2017 Para el caso de máquinas que ejecuten el aplicativo PCT, se determinó un cambio en la instalación del mismo, se deja manual actualizado. A pesar de las comunicaciones con el proveedor de PCT, no se obtuvo respuesta positiva para determinar cómo evitar que este aplicativo funcionara con usuarios administradores, por lo tanto, la solución se dio al interior de la Dirección, se hicieron pruebas y se estandarizó. Queda la tarea de aplicar la solución en las 319 máquinas que tienen PCT, durante la presente vigencia. • Se implementa el nuevo procedimiento de instalación de PCTG en las nuevas máquinas. • Se adjuntar procedimiento para la instalación de PCTG, disponible en la plataforma de calidad.	100%	Se seguiran depurando las instalaciones viejas de acuerdo al avance de mantenimiento preventivo de los computadores ya instalados en el Departamento.
9	Es pertinente realizar un barrido por los diferentes puestos de trabajo, con el fin de deshabilitar el paquete de juegos de los equipos de cómputo y con ello dar cumplimiento a las políticas del proceso. - NTC-ISO-27001/A.11.6.1 nos sugiere:	Realizar recorrido para configurar los equipos de manera que no se disponga de juegos con los que vienen provistos los equipos de computo para acceso al usuario.	Argemiro Gomez Calderon	2016-12-31	Numero de maquinas con juegos preinstalados igual a cero	• Con el contrato de mantenimiento de los equipos, y barrido adicional por parte de los aprendices SENA, se configuraron los equipos para no cargar el paquete de juegos que vienen con Windows.	100%	En los equipos nuevos adquiridos en dic/2016, y que se entregan a partir de enero de 2017 se tienen como tarea de configuración desactivar los juegos que vienen

	Se debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso. - NTC-ISO-27001/A.12.4.1 nos sugiere: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.							activados.

LUIS ALEXANDER VASQUEZ HERNANDEZ
Contratista
DIRECCION DE CONTROL INTERNO