PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVO GENERAL

Establecer conceptos, procedimientos y metodología para una adecuada administración de riesgos teniendo en cuenta su identificación, control, manejo y seguimiento.

OBJETIVOS ESPECIFICOS

- Identificar las situaciones de riesgo o riesgos que afecten el cumplimiento de la misión de la empresa.
- Establecer acciones de respuesta o controles según los riesgos identificados.
- Realizar un adecuado evaluación y seguimiento de la efectividad de las acciones o controles definidos.

ALCANCE

Proporciona la metodología establecida por la empresa Lotería del Cauca para la administración y gestión de los riesgos a nivel de procesos, siguiendo los lineamientos de la política de administración del riesgo existente en el SGC.

DEFINICIONES

- INCERTIDUMBRE: Se desconoce si va a suceder.
- IMPACTO O CONSECUENCIAS: Resultados si se llega materializar el riesgo.
- RIESGO: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

- RIESGO DE CORRUPCIÓN: Posibilidad que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información se lesionen los intereses de la empresa y en consecuencia del Estado, para la obtención de un beneficio particular.
- RIESGO INHERENTE: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- CONTEXTO EXTERNO: Entorno en el cual opera la empresa, se considera como: Políticos, Sociales y culturales, legales y reglamentarios, tecnológicos, financieros y económicos.
- CONTEXTO INTERNO: características o aspectos internos del ambiente interno en el que la organización busca alcanzar sus objetivos.
- POLÍTICA PARA LA GESTIÓN DEL RIESGO: Declaración la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- PLAN PARA LA GESTIÓN DEL RIESGO: esquema dentro del marco de referencia para la gestión del riego que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo.
- PARTE INVOLUCRADA: Persona u organización que puede afectar o verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.
- IDENTIFICACIÓN DEL RIESGO: proceso para encontrar, reconocer y describir el riesgo. La identificación implica la identificación de las fuentes de riesgo, causa y consecuencias.
- PROBABILIDAD: posibilidad de ocurrencia del riesgo.
- CONTROL: medida que modifica el riesgo. Los controles incluyen proceso políticas dispositivos, prácticas u otras acciones que modifiquen el riesgo.
- EVITAR EL RIESGO: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.

- FRECUENCIA: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- IDENTIFICACIÓN DEL RIESGO: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- MAPA DE RIESGOS**:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- MATERIALIZACION DEL RIESGO**:** ocurrencia del riesgo identificado
- OPCIONES DE MANEJO**:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- PLAN DE CONTINGENCIA**:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- PROBABILIDAD**:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- PROCEDIMIENTO**:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- PROCESO: conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.
- VALORACION DEL RIESGO**:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.
- DECLARACION DE APLICABILIDAD: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la

Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- DERECHO A LA INTIMIDAD: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- ENCARGADO DEL TRATAMIENTO DE DATOS: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- INFORMACION PUBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado 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 Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- INFORMACION PUBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- PLAN DE CONTINUIDAD DEL NEGOCIO: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

POLITICAS DE ADMINISTRACION DEL RIESGO

LINEAMIENTOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Para el tratamiento de los riesgos en la Lotería del Cauca, se deben tener en cuenta los siguientes lineamientos:

- El nivel Directivo de la empresa identificara las amenazas según el análisis DOFA realizado por la organización. Los riesgos valorados en zona de riesgos alta y extrema, deben permanecer en un plan de manejo del riesgo para ser controlados.
- Los funcionarios de la empresa identifican los posibles riesgos que puedan afectar el cumplimiento del objetivo del proceso al cual pertenecen.
- Cuando la valoración del riesgo los ubique en zona de riesgo baja o moderada, se debe continuar con la aplicación de los controles establecidos, si se tienen, y seguir con el monitoreo trimestral al riesgo identificado.
- Cuando la valoración del riesgo se localice en zona de riesgo alta, se definirán acciones para mitigar el riesgo, y se monitorean 1 vez al mes.
- Los procesos que se encuentren valorados en zona de riesgo alta y no tienen controles, deben establecerlos para evitar la materialización del riesgo.
- Los mapas de riesgo por proceso son un insumo para el mapa de riesgo institucional, teniendo en cuenta que solo se trasladan al institucional los riesgos que permanecieron en la zona de riesgo extrema.
- Dado que todos los procesos son susceptibles de ser afectados por la ocurrencia de eventos de riesgo, los responsables de los procesos deben adelantar la gestión de sus riesgos y reportarlos al Proceso de Planificación, para efectos de los controles, registros y monitoreo correspondientes.
- Cuando un riesgo se materialice se deberá seguir con el protocolo respectivo correspondiente y se evaluara nuevamente.
- Cuando se diseñen nuevos controles, los responsables de los procesos deberán enviar un email al Proceso de planificación, para efectos de actualizar el mapa correspondiente.
- Opciones de tratamiento, después de valorarlo:

➢ **Evitar el riesgo**: Tomar las acciones encaminadas a prevenir su materialización, a través de la formulación de planes de acción o acciones.

➢ **Reducir el riesgo**: Implica tomar medidas encaminadas a disminuir tanto la probabilidad como el impacto, a través de controles preventivos o correctivos o la formulación de acciones.

- **Compartir o transferir el riesgo**: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o la distribución de una porción del riesgo con otra entidad.

ADMINISTRACION DEL RIESGO

1. MODULO DE CONTROL DE PLANEACIÓN Y GESTIÓN >

1.3 ADMINISTRACIÓN DEL RIESGO

Este componente se estructura a través de los siguientes Elementos de Control:

1.3.1 Políticas de Administración del Riesgo.

1.3.2 Identificación del Riesgo.

1.3.3. Análisis y Valoración del Riesgo

- Mapas de Riesgos institucional

- Ademas de estos Mapas de riesgos por procesos e institucional, la empresa definió el mapa de riesgos de corrupción.

Este componente comprende un conjunto de elementos que permiten a la entidad identificar, evaluar y gestionar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos de la empresa.

Los responsables de realizar la administración de los riesgos, son los líderes de los procesos y sus respectivos equipos de trabajo; La oficina de control interno podrá brindar apoyo en la metodología de administración del riesgo para su identificación a través de su rol de asesoría y acompañamiento y realizar la evaluación y seguimiento de los mapas de riesgos establecidos por la Lotería del Cauca.

MATRIZ DE IDENTIFICACIÓN DEL RIESGO

	IDENTIFICACIÓN DEL RIESGO		CODIGO:GC-F7 VERSIÓN: 1
PROCESO:	SISTEMAS	**FECHA ACTUALIZACIÓN**	Junio 30 de 2018
OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.		

CAUSAS	RIESGO	DESCRIPCIÓN	CONSECUENCIAS POTENCIALES
Ataques informáticos	Infección de equipos por virus,acceso a información confidencial, perdida de la información, daño del equipo.	Virus informático es un progrma de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo.	Perdida de información importante, daño en los equipos, fuga de información confidencial.
Falla en suministro de energía	Perdida de información, daño en equipos.	Se cuenta con el suministro de fluido eléctrico de una única empresa prestadora del servicio.	Perdida de información daño en equipos, alteración en el normal funcionamiento de las actividades de la empresa.
Falla en servicio de acceso a internet	Incomunicación en el momento de devoluciones en página web.	La empresa posee un sitio web, en el cual se realiza mediante el módulo de devoluciones el proceso de cargue de la información de devoluciones en el proceso misional de sorteo.	Incomunicación en el momento de devoluciones, inconvenientes en el normal funcionamiento del proceso.
Falla en servicio de servidor y base de datos	Perdida de información, presentandose impedimentos al normal funcionamiento de actividades	Existe un servidor en la empresa en el cual se aloja toda la información en una base de datos.	Perdida de información, impedimento al normal funcionamiento de actividades de la empresa.
Inseguridad en el acceso a las instalaciones	Perdida de información confidencial.	El descuido en el puesto de trabajo y dejar los computadores encendidos sin ningún tipo de seguridad.	Perdida o daño en la información, salida o conocimiento de información confidencial, perdida de elementos.
Ausencia de contrato de mantenimiento de equipos	Falla en el mantenimiento de la infraestructura necesaria para lograr la conformidad con los requisitos del servicio	la entidad es propietaria de la totalidad de equipos,varios de los cuales fueron adquiridos desde el año 2.010 o antes; configuraciones de HW y sistemas operativos no actualizados ni acordes al tiempo.	Daño en el único servidor de la empresa el cual contiene toda la información de ella, puesto que la ubicación de los servidores se encuentra compartida con el sitio de trabajo de otras personas , temperatura ambiente no recomendable para los servidores, se observa el cableado de red en algunos sitios bordeando las paredes, no existen sistema de detección y extinción de incendios.
Software hecho a la medido por el proveedor unipersonal	Dependencia del proveedor	Teniendo en cuenta la importancia del SW Velero para los objetivos misionales de la entidad, se evaluaron las condiciones pactadas en los contratos relacionados con la adquisición de la licencia de uso del SW para el manejo y control de los procesos de la empresa.	Aumento de Nivel de dependencia hacia un solo proveedor.
Ausencia de plan de contingencia	Falla en la comunicación interna y externa.	La información escrita es manejada por los correos personales de los funcionarios, el PBX es obsoleto y al presentar un daño es muy difícil el soporte para su funcionamiento.	Falta de comunicación acertiva y de responsabilidad en lo referente a la información escrita y enviada por los correos personales , incomunicación por obsolencia de equipos.
Los funcionarios no realicen eficazmente la información que debe ser copiada en la nube.	Distorsión en la imagen empresarial por falta de un adecuado diseño de página web.	La interfaz gráfica del portal evidencia aspectos a mejorar, dadas las nuevas tendencias que existen.	Imagen deficiente hacia sus clientes.

Uso y desgaste normal	Fallas en el servidor	En cualquier momento la empresa se puede ver afectada por fallas de Componentes de Hardware del Servidor.	Perdida de información, Suspensión de operaciones
	Fallas en el cuarto eléctrico	El cuarto electico es el sitio donde se encuentra la conectividad de la red de la empresa puede presentar fallas por diferentes causas una de ellas y la más común es la falta de fluido electrico la cual se suple con UPS.	Perdida de conectividad
	Fallas en equipos de computo e impresoras	Los equipos de computo como las impresoras, están compuestos por una serie de dispositivos, los cuales están expuestos a fallos simples o complejos.	Daño en dispositivos dificultad para realizar las tareas diarias.
Se tiene un solo servidor el cual contiene toda la información de la empresa	Perdida de la información	Existe un servidor en la empresa en el cual se aloja toda la información en una base de datos.	Perdida de información, impedimento al normal funcionamiento de actividades de la empresa.
Ausencia de controlador de temperatura y carencia de sirenas y alarmas que detecten la presencia de humo	Incendio	El cuarto eléctrico es el sitio donde se encuentra la conectividad de la red de la empresa por su objetivo es altamente vulnerable a los incendios.	Perdida total de los equipos que conforman el cuarto como tambien de la conectividad y la comunicación de la empresa.
Se carece de un sistema de control de ingreso al cuarto eléctrico	Ingresos no permitidos	El cuarto eléctrico es el sitio donde se encuentra la conectividad de la red y la información de la empresa, la cual debe estar salvaguardada, y solo deben tener acceso personal autorizado.	Fuga de información, daño en los equipos.
Se carece de seguridad perimetral	Ataques a la información	Las tecnologías de protección perimetral y de red sirven para proteger la red de la empresa de amenazas y vulnerabilidades externas	Los ataques por red y pérdidas de información ocasionan un gran trastorno al funcionamiento de la organización como tambien el progreso de la empresa se ven afectados.
Datos guardados por programas independientes	Discordancia de datos al momento de la restauración	Los datos son guardados por progrmas independientes y van asociados a la clase de datos (sql, Mdb o carpetas del sistema) este modelo no permite garantizar la consistencia o concordancia de los datos despues de una restauración.	Inconsistencia en la información
Ausencia de capacitacion de administración de BD	Imposibilidad de restauración de la información como contingencia	Se debe contar con un plan claro de contingencia al momento de realizar una restauración de copias de seguridad.	Tardanza en el tiempo de restauración de la información
Alta dependencia del proveedor	Ausencia de soporte técnico del proveedor unipersonal.	Implica que toda modificación técnica la efectúa directamente el proveedor	Al presentarse un evento urgente a resolver se presenta trastorno en el normal desarrollo de las acciones, debido a la dependencia hacia el proveedor
Los módulos básicos generan información al módulo contable	Redundancia en datos	El diagrama refleja que el flujo de información va en un solo sentido (unidireccional) lo que deja la posibilidad de mantener información asincrónica cuando se realizan cambios	Generacion de información inconsistente
Dispersión y redundancia de da	Duplicidad en la información	fallas técnicas generan información	Informes con datos inconsistentes
Falta de registro cronólogico en	Cambios sin registro de auditoria	No existe en el aplicativo un proceso que lleve registro cronológico sobre los cambios que se efectuan y al cual puedan acceder.	Cambios sin registros cronologicos
Manuales de usuario desactual	Errores operativos	Son una guia los cuales son de gran utilidad para dar explicación sobre dudas relacionadas con el aplicativo	Ausencia de una guia para la resolución de dudas de usuario
Ausencia de plan de contingenc	Imposibilidad de reanudación de actividades	Un plan de contingencia es el proceso de determinar qué hacer si una catástrofe se abate sobre la empresa y es necesario recuperar el sistema informativo.	Ausencia de una solución completa y totalmente probada para recuperar las operaciones.
Falta de mecanismos de contro	Posibles errores no detectados	Debido a que el proceso de las devoluciones se efectúa actualmente en términos de venta se hace necesario activar sobre los archivos virtuales mecanismos de control	Errores en informes por deficiencia en filtro de inconsistencias
Ausencia de módulo administra	Retraso en solución de incidentes	Con el fin de dar atención oportuna a los incedentes delegables se hace necesario incluir dentro del aplicativo un conjunto de parámetros y cracteristicas que granticen la flexibilidad en los cambios.	Imposibilidad de llevar a cabo los cambios delegables, y se hagan de una manera segura y justificada bajo un informe o log de cambios.
ausencia de plan de contingenci	Perdida de información e imposibilidad de reanudación de operaciones	Se cuenta con copias de seguridad pero su custodia se realiza dentro de las instalaciones de la empresa.	Al presentarse un evento grave que comprometa las instalaciones del edificio Lotería del Cauca, se encuentra en riesgo la restauración de la información puesto que no se cuenta con copias de seguridad guardadas externamente.
Los funcionarios no realicen eficazmente la información que debe ser copiada en la nube.	Perdida de información	Se cuenta con un aplicativo a la nube para la salvaguarda de la información de cada equipo de computo, en la actualidad se guarda información con una frecuencia a criterio del funcionario.	Al no limitar el horario y dias al cual se debe salvaguardar la información, se dificulta la verificación de la tarea, se debe unificar una fecha y hora igual para todos.

CONTEXTO

	CONTEXTO ESTRATÉGICO		CODIGO:GC-F6
			VERSIÓN: 1
PROCESO:	SISTEMAS	FECHA ACTUALIZACIÓN	Junio 30 de 2018
OBJETIVO DEL PROCE	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.		
FACTORES EXTERNOS	CAUSAS	FACTORES INTERNOS	CAUSAS
Nuevas tecnologías de la información y las comunicaciones	Ataques informáticos	Sistemas de información	Incumplimiento de las copias de respaldo
			No se actualiza el hardware y el software.
Proveedores	Ausencia de soporte al sistema informatico	Ausencia del proveedor	No se determina un plan de contingencia
	Falla en suministro de energía	Procesos y Procedimientos	Mal uso de controles o contraseñas de suguridad y definición de accesos.
	Falla en servicio de acceso a internet		Ausencia de contrato de mantenimiento de equipos
	Falla en servicio de servidor y base de datos		Falta de mantenimiento preventivo y correctivo a los equipos.
	Inseguridad en el acceso a las instalaciones	Infraestructura y tecnología	Falta de controles de seguridad dispositivos de monitoreo.
	Errores (usuarios y administrador)	Capacitación	Deficiencia en programas de capacitación
	Errores de configuración		
	Errores de enrutamiento		
	Alteración, destrucción y escapes de la información		
	Fugas de información.		
	Caída del sistema por agotamiento de recursos		
	Perdida de equipo		
	Errores de mantenimiento y actualización de sw		
	suplantación de identidad		
	Manipulación de registros configuraciones y logs		
	Abuso de privilegios de acceso		
	Difución de sw dañino		
Amenazas del Entorno (Ambientales)	Contaminación	Procedimientos de control	Falta de contingencias
	Falla de equipos o sw		
	Condiciones inadecuadas de temperatura o humedad		
	Deterioro de equipos	Condiciones ambientales	Uso y desgaste normal
		Falta de priorizar compra de equipos	
	No se incluyeron en el momento de la realización del cuarto eléctrico.	Falta de inclusión en el plan de compras	Se tiene un solo servidor el cual contiene toda la información de la empresa
			Ausencia de controlador de temperatura y carencia de sirenas y alarmas que detecten la presencia de humo.
			Se carece de un sistema de control de ingreso al cuarto eléctrico
	Datos guardados por programas independientes	No permite garantizar la consistencia de la restauración	Se carece de seguridad perimetral
	Ausencia de capacitacion de administración de BD	Falta de capacitación en el modelo para ubicación de datos.	Procesos realizados de manera independiente
Software	Ausencia de capacitacion de administración de BD	Falta de capacitación en el modelo para ubicación de datos.	Procesos realizados de manera independiente
	Alta dependencia del proveedor	Modificaciones técnicas las realiza unicamente el proveedor	Desconocimiento en el proceso de copia y restauración
	Los módulos básicos generan información al módulo contable	El flujo de información va en un solo sentido (unidireccional)	No existe aplicativo de opción de modificación de datos delegables a administrador de base de datos.
	Dispersión y redundancia de datos	Información inconsistente	Falta de herramienta que permita determinar inconsistencias e integridad de los datos
	Falta de registro cronólogico en el aplicativo	Control de cambio que se efectúan	No existe esquema de parametrización a nivel de usuario
	Manuales de usuario desactualizados	No se maneja un inventario del aplicativo	No se tiene incorporado a manera de consulta por el administrador de la base de datos a manera de consulta los cambios
	Ausencia de plan de contingencia	Proveedor unipersonal	Manuales de administración no han sido entragados
	Falta de mecanismos de control	Controles ineficientes o ausentes	No se ha contemplado un plan alternativo
	Ausencia de módulo administrativo	Control de Incidentes delegables	Ausencia de activación de mecanismos de control al procedimiento de archivos en devoluciones
	Software hecho a la medido por el proveedor unipersonal		No existe en el software un conjunto de parametros que garanticen la flexibilidad de los cambios de una manera segura y justificada.
Desastre Grave que interrumpa operaciones	Ausencia de plan de contingencia	Las copias de seguridad estan guardadas en la empresa en el mismo sitio.	
	Los funcionarios no realicen eficazmente la información que debe ser copiada en la nube.	No se han definido políticas para definir criticidad de información guardada en la nube.	No existe contratación de custodia de copias de seguridad

EVALUACION DEL RIESGO

ANALISIS DEL RIESGO							CODIGO:GC-F8 VERSION: 1
PROCESO:	SISTEMAS				FECHA ACTUALIZACIÓN: junio 30 de 2018		
OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.						
RIESGO	CALIFICACIÓN				TIPO IMPACTO	EVALUACIÓN ZONA DE RIESGO	MEDIDAS DE RESPUESTA
	probabilidad		impacto				
Infección de equipos por virus,acceso a información confidencial, perdida de la información, daño del equipo.	1	RARO	3	MODERADO	Operativo	ZONA DE RIESGO MODERADA	Reducir el riesgo
Perdida de información, daño en equipos.	1	RARO	4	MAYOR	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Incomunicación en el momento de devoluciones en página web.	1	RARO	3	MODERADO	Tecnología	ZONA DE RIESGO MODERADA	Reducir el riesgo
Perdida de información, presentandose impedimentos al normal funcionamiento de actividades	1	RARO	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO ALTA	Reducir el riesgo
Perdida de información confidencial.	1	RARO	2	MENOR	Operativo	ZONA DE RIESGO BAJA	Asumir el riesgo
Falla en el mantenimiento de la infraestructura necesaria para lograr la conformidad con los requisitos del servicio	1	RARO	2	MENOR	Tecnología	ZONA DE RIESGO BAJA	Asumir el riesgo
Dependencia del proveedor	4	PROBABLE	5	CATASTRÓFICO	Operativo	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Falla en la comunicación interna y externa.	1	RARO	2	MENOR	Operativo	ZONA DE RIESGO BAJA	Asumir el riesgo
Distorsión en la imagen empresarial por falta de un adecuado diseño de página web.	1	RARO	3	MODERADO	Imagen	ZONA DE RIESGO MODERADA	Asumir el riesgo
Fallas en el servidor	1	RARO	5	CATASTRÓFICO	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Fallas en el cuarto eléctrico	1	RARO	3	MODERADO	Operativo	ZONA DE RIESGO MODERADA	Asumir el riesgo
Fallas en equipos de computo e impresoras	3	POSIBLE	3	MODERADO	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Perdida de la información	1	RARO	4	MAYOR	Tecnología	ZONA DE RIESGO ALTA	Reducir el riesgo
Incendio	1	RARO	3	MODERADO	Operativo	ZONA DE RIESGO MODERADA	Asumir el riesgo
Ingresos no permitidos	2	IMPROBABLE	4	MAYOR	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Ataques a la información	3	POSIBLE	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Discordancia de datos al momento de la restauración	3	POSIBLE	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Imposibilidad de restauración de la información como contingencia	3	POSIBLE	4	MAYOR	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Ausencia de soporte técnico del proveedor unipersonal.	3	POSIBLE	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Redundancia en datos	3	POSIBLE	3	MODERADO	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Duplicidad en la información	3	POSIBLE	3	MODERADO	Operativo	ZONA DE RIESGO ALTA	Reducir el riesgo
Cambios sin registro de auditoria	3	POSIBLE	4	MAYOR	Operativo	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Errores operativos	3	POSIBLE	4	MAYOR	Operativo	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Imposibilidad de reanudación de actividades	3	POSIBLE	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Posibles errores no detectados	3	POSIBLE	3	MODERADO	Tecnología	ZONA DE RIESGO ALTA	Reducir el riesgo
Retraso en solución de incidentes	3	POSIBLE	4	MAYOR	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Perdida de información e imposibilidad de reanudación de operaciones	3	POSIBLE	5	CATASTRÓFICO	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo
Perdida de información	4	PROBABLE	4	MAYOR	Tecnología	ZONA DE RIESGO EXTREMA	Reducir el riesgo

VALORACION DE LOS RIESGOS

	VALORACIÓN DEL RIESGO	CODIGO:GC-F9
		VERSIÓN: 1

PROCESO:	SISTEMAS	FECHA ACTUALIZACIÓN	Junio 30 de 2018
OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.		

RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN						
					PUNTAJE Herramientas para ejercer el control			PUNTAJE Seguimiento al Control		
	Probabilidad	Impacto		Tipo de Control aminora la probabilidad o el impacto	Posee una Herramienta para ejercer el control?	Existen manuales, Instructivos o procedimientos para el manejo de la herramienta?	En el tiempo que lleva la herramienta ha demostrado ser efectiva?	Está definidos los responsables de la ejecución del control y del seguimiento?	La frecuencia de ejecución del control y seguimiento es adecuada?	Puntaje Final
Infección de equipos por virus,acceso a información confidencial, perdida de la información, daño del equipo.	1	3	Antivirus actualizados	Preventivo	15	15	30	15	25	100
			Programa de mantenimiento preventivo de equipos, programa de copias de seguridad	Preventivo	15	15	30	15	25	100
Perdida de información, daño en equipos.	1	4	Se dispone de una instalación básica de contingencia	Preventivo	15	15	30	15	25	100
			NINGUNO		0	0	0	0	0	0
Incomunicación en el momento de devoluciones en página web.	1	3	Seguridad en el hosting	Preventivo	15	15	30	15	25	100
			Recibo de devoluciones via e-mail.	Correctivo	15	15	30	15	25	100
Perdida de información, presentandose impedimentos al normal funcionamiento de actividades	1	5	Mantenimiento preventivo de la Base de Datos	Preventivo	0	0	0	15	0	15
			Servidor de respaldo	Correctivo	0	0	0	15	0	15
Perdida de información confidencial.	1	2	Acceso restringido a visitantes.	Preventivo	15	15	30	15	25	100
			copias de seguridad	Preventivo	15	15	30	15	25	100
Falla en el mantenimiento de la infraestructura necesaria para lograr la conformidad con los requisitos del servicio	1	2	No se ha realizado mantenimiento físico y a sistema operativo al servidor de la empresa.	Preventivo	15	15	30	15	25	100
			Con el cambio a la nueva sede se realiza reemplazo de equipos. Se adquieren equipos de impresión de alta capacidad,se adquieren dos scanner de alta capacidad, se provee de un	Preventivo	15	15	30	15	25	100
Dependencia del proveedor	4	5	Se evita la solicitud directa entre usuario y proveedor y se implementa el registro de control de cambios, exigiendo para ello el formato de requerimiento F3.	Preventivo	15	15	30	15	25	100
			En el contrato de prestación de servicios se define que dará respuesta a los requerimientos teniendo en cuenta la complejidad o gravedad de la incidencia como tambien cursos de capacittación y reinducción, y entrega de registros logs a control interno.	Preventivo	0	0	0	15	0	15
Falla en la comunicación interna y externa.	1	2	Se implementan los correos institucionales en la empresa.	Correctivo	15	15	30	15	25	100
			Se realiza la adquisición de un PBX hibrido IP/ANALOGO.	Correctivo	15	15	30	15	25	100
Distorsión en la imagen empresarial por falta de un adecuado diseño de página web.	1	3	Se realiza el rediseño de la página web, se realiza cambio de proveedor.	Correctivo	15	15	30	15	25	100
			Se realiza la adquisicion de un componente Rsfirewall que corrige vulnerabilidades y mantiene la seguridad en la web.	Correctivo	15	15	30	15	25	100
Fallas en el servidor	1	5	Se programan dos (2)mantenimientos preventivos a servidor para el año 2016,se realizan copias de seguridad.	Preventivo	15	15	30	15	25	100
			NINGUNO		0	0	0	0	0	0
Fallas en el cuarto eléctrico	1	3	El cuarto tiene un tiempo de servicio menor a un año, por el cual no se ha realizado su mantenimiento preventivo.	Preventivo	15	0	0	15	0	30
			NINGUNO		0	0	0	0	0	0
Fallas en equipos de computo e impresoras	3	3	Se realiza mantenimiento preventivo a impresoras y se programan dos (2) mantenimientos preventivos para los equipos para el año 2016.	Preventivo	15	15	30	15	25	100
			NINGUNO		15	0	0	0	0	15
Perdida de la información	1	4	Se programan dos (2)mantenimientos preventivos a servidor para el año 2016,se realizan copias de seguridad.	Preventivo	15	15	30	15	25	100
			NINGUNO		15	0	0	0	0	15

Incendio	1	3	Se tiene instalado un aire acondicionado tipo minisplit. Se instala detector de humo y camara de vigilancia 7/24.	Preventivo	15	15	30	15	25	100
			NINGUNO		15	0	0	0	0	15
Ingresos no permitidos	2	4	El ingreso a este cuarto solo esta autorizado a los dos funcionarios del área de sistemas.Se instala cámara de vigilancia y acceso biometrico.	Preventivo	15	15	30	15	25	100
			NINGUNO		15	0	0	0	0	15
Ataques a la información	3	5	Se posee la protección básica de firewall de windows y el antivirus actualizado. Se adquiere un equipo de seguridad perimetral.	Preventivo	15	15	30	15	25	100
			NINGUNO		0	0	0	0	0	0
Discordancia de datos al momento de la restauración	3	5	Se realiza un simulacro de restauración	Preventivo	0	0	30	15	0	45
			NINGUNO		0	0	0	0	0	0
Imposibilidad de restauración de la información como contingencia	3	4	Se realiza simulacro de restauración de copia de seguridad	Preventivo	0	0	30	15	0	45
			NINGUNO		0	0	0	0	0	0
Ausencia de soporte técnico del proveedor unipersonal.	3	5	NINGUNO		0	0	0	0	0	0
			NINGUNO		0	0	0	0	0	0
Redundancia en datos	3	3	Formato de requerimientos	Correctivo	15	15	0	15	0	45
			NINGUNO		0	0	0	0	0	0
Duplicidad en la información	3	3	Formato de requerimientos	Correctivo	15	15	30	15	0	75
			NINGUNO		0	0	0	0	0	0
Cambios sin registro de auditoria	3	4	Formato de requerimientos	Correctivo	15	15	30	15	0	75
			NINGUNO		0	0	0	0	0	0
Errores operativos	3	4	Formato de requerimientos	Correctivo	15	15	30	15	25	100
			NINGUNO		0	0	0	0	0	0
Imposibilidad de reanudación de actividades	3	5	Simulacro de Recuperación de operciones	Correctivo	15	0	0	15	0	30
			NINGUNO		0	0	0	0	0	0
Posibles errores no detectados	3	3	Planilla de pruebas	Correctivo	15	0	30	15	0	60
			NINGUNO		0	0	0	0	0	0
Retraso en solución de incidentes	3	4	Formato de requerimientos	Correctivo	15	0	30	15	0	60
			NINGUNO		0	0	0	0	0	0
Perdida de información e imposibilidad de reanudación de operaciones	3	5	Simulacro de recuperacion de operaciones	Preventivo	0	0	0	15	0	15
			NINGUNO		0	0	0	0	0	0
Perdida de información	4	4	Verificación de la frecuencia de salvaguarda de la información	Preventivo	0	0	0	15	0	15

IDENTIFICACION DE CONTROLES (SOA statement of applicability)

Enumera los controles aplicados por la empresa, tras el resultado de los procesos de evaluación y tratamiento de riesgos, así como la justificación de las exclusiones de controles del anexo A de ISO 27001 (ISO/IEC 27000).

DECLARACION DE APLICABILIDAD SoA

Dominios	Objetivos de Control	Controles	Orientación	Descripción	CONTROLES ACTUALES	OBSERVACIONES (justificación de la exclusión)	LOS CONTROLES SELECCIONADOS Y LOS MOTIVOS DE LA SELECCIÓN				OBSERVACIONES
							Legal	Obligación contractual	Req.negocios/buena práctica	o de la evaluación de riesgos	
	1	2	Política de Seguridad de la Información								
5		2	Orientación de la dirección para la gestión de la seguridad de la información								
	1	1	Debe	Políticas para la seguridad de la información	SI				X		
		2	Debe	Revisión de las políticas de seguridad de la información	SI				X		
	2	7	Organización de la seguridad de la información								
		5	Organización Interna								
		1	Debe	Roles y responsabilidades para la seguridad de la información	SI				X		
		2	Debe	Separación de deberes	SI					X	
6	1	3	Puede	Contacto con las autoridades	NO	No aplica					
		4	Puede	Contacto con grupos de interés especial	NO	No aplica					
		5	Debe	Seguridad de la información en la gestión de proyectos	NO	No aplica					No definido Gestión de Proyectos
	2	2	Dispositivos móviles y teletrabajo								
		1	Debe	Politica para dispositivos moviles	NO	No aplica					
		2	Debe	Teletrabajo	NO	No aplica					
Dominios	Objetivos de Control	Controles	Orientación	Descripción							
	3	6	Seguridad de los recursos humanos								
	1	2	Antes de asumir el empleo								
		1	Debe	Selección	T. H.		X				
7		2	Debe	Terminos y condiciones del empleo	T.H.		X				
	2	3	Durante el empleo								
		1	Debe	Responsabilidades de la gerencia	SI				X		Politicas y procedimientos
		2	Debe	Educación y formación en seguridad de la información	SI				X		Politicas y procedimientos
		3	Debe	Procesos disciplinarios	T.H.		X				

DECLARACION DE APLICABILIDAD SoA

Dominios	Objetivos de Control	Controles	Orientación	Descripción	CONTROLES ACTUALES	OBSERVACIONES (justificación de la exclusión)	LOS CONTROLES SELECCIONADOS Y LOS MOTIVOS DE LA SELECCIÓN				OBSERVACIONES
							Legal	Obligación contractual	Req.negocios/buena práctica	o de la evaluación de riesgos	
	3	1	**Terminación o cambio del empleo**								
		1	Debe	Terminación o cambio de responsabilidades de empleo	T.H.		X				Politicas y procedimientos
	3	**8**	**Gestión de activos**								
		4	**Responsabilidad sobre los activos**								
8	1	1	Debe	Inventario de activos	SI				X		
		2	Debe	Propietario de activos	SI				X		
		3	Debe	Uso aceptable de los activos	SI				X		
		4	Debe	Devolución de activos	NO	Procedimiento por definir					
	2	**3**	**Clasificación de la información**								
		1	Debe	Clasificación de la información	NO	Procedimiento por definir					
		2	Debe	Etiquetado de la información	NO	Procedimiento por definir					
		3	Debe	Manejo de activos	NO	Procedimiento por definir					
	3	**3**	**Manejo de medios**								
		1	Debe	Gestión de medios removibles	SI						Politica de uso de dispositivos de almacenamiento extraibles
		2	Debe	Disposición de los medios	NO	Procedimiento por definir					
		3	Debe	Transferencia de medios físicos	SI						Custodia de backup
Dominios	**Objetivos de Control**	**Controles**	**Orientación**	**Descripción**							
	4	**14**	**Control de acceso**								
	1	**2**	**Áreas Seguras**								
		1	Debe	Requisitos del negocio para control de acceso	SI					X	Acceso biométrico
		2	Debe	Acceso a redes y a servicios de red	SI					X	Politicas de uso de redes y acceso a internet
		6	**Gestión de acceso de usuarios**								

DECLARACION DE APLICABILIDAD SoA

Dominios	Objetivos de Control	Controles	Orientación	Descripción	CONTROLES ACTUALES	OBSERVACIONES (justificación de la exclusión)	LOS CONTROLES SELECCIONADOS Y LOS MOTIVOS DE LA SELECCIÓN				OBSERVACIONES
							Legal	Obligación contractual	Req.negocios/buena práctica	o de la evaluación de riesgos	
9	2	1	Debe	Registro y cancelación del registro de usuarios	NO	No se tiene registro formal					
		2	Debe	Suministro de acceso de usuarios	NO	No se tiene registro formal					
		3	Debe	Gestión de derechos de acceso privilegiado	NO	No se tiene registro formal					Acceso privilegiado solo para personal de sistemas
		4	Debe	Gestión de información de autenticación secreta de usuarios	NO	No se define información secreta					
		5	Debe	Revisión de los derechos de acceso de usuarios	NO	No se tiene registro formal					
		6	Debe	Retiro o ajuste de los derechos de acceso	NO	No se tiene registro formal					
	3	**1**	**Responsabilidades de los usuarios**								
		1	Debe	Uso de información de autenticación secreta	SI						Politica de administración de contraseña y salvaguarda de información en la nube.
	4	**5**	**Control de acceso a sistemas y aplicaciones**								
		1	Debe	Restricción de acceso a la información	SI				X		Politica de administración de contraseña
		2	Debe	Procedimiento de ingreso seguro	SI					X	Politica de administración de contraseña
		3	Debe	Sistema de gestión de contraseña	SI					X	Politica de administración de contraseña
		4	Debe	Uso de programas utilitarios privilegiados	NO	Falta politica de limitación de					
		5	Debe	Control de acceso a código fuente de programas	SI		X				software es uso exclusivo del contratista y dueño del aplicativo.
Dominios	**Objetivos de Control**	**Controles**	**Orientación**	**Descripción**							
	1	**2**	**Criptografía**								
10	1	**2**	**Controloes criptográficos**								
		1	Debe	Politica sobre el uso de controles criptograficos	NO	Falta de politica					Se realiza cifrado para DDE con información de
		2	Debe	Gestión de llaves	NO	Falta de politica					Se realiza cifrado para DDE con información de salvaguarda.

INVENTARIO DE ACTIVOS

INVENTARIO DE ACTIVOS LOTERIA DEL CAUCA-SISTEMAS

ACTIVO	CANT	UBICACIÓN	PROPIETARIO	CUSTODIO	$	C	I	D	TOTAL
DATOS/INFORMACION									
BASES DE DATOS									
1.De velero	1	Computadores	Lotería del Cauca	Responsable Sistem	5	5	5	5	20
2.De hosting devoluciones	1	Servidor web	Contratista	Sistemas	5	5	5	5	20
BACKUPS									
1.BD de velero	1	Servidor físico	Lotería del Cauca	Responsable Sistem	5	5	5	5	20
2.BD hosting devoluciones	1	Servidor web	Lotería del Cauca	Sistemas	5	5	5	5	20
INFORMACION									
1.correo instiutcional	30	Servidor web	Contratista	Sistemas	3	5	3	3	14
CONTRASEÑAS									
1.computadores	27	Estaciones de trabajo	Lotería del Cauca	Recursos Físicos	3	5	5	5	18
2.portatiles	3	Estaciones de trabajo	Lotería del Cauca	Recursos Físicos	3	5	5	5	18
3.sw velero	1	Licencia de uso	Contratista	Contratista	5	5	5	5	20
4.correo institucional	30	Servidor web	Lotería del Cauca	Sistemas	3	5	5	5	18
SERVICIOS									
AL PUBLICO EN GENRAL									
1. Página web	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12
2.facebook	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12
3.twitter	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12
AL USUARIO INTERNO									
1.ftp	2	Computadores sistemas	Lotería del Cauca	Sistemas	5	5	5	5	20
AL USUARIO EXTERNO									
1.Página devoluciones	1	Servidor web	Contratista	Sistemas	5	5	5	5	20
SW/APLICACIONES INFORMATICAS									
1.Office	30	Computadores	Lotería del Cauca	Sistemas	3	3	3	3	12
2.Nicoftp	2	Computadores sistemas	Lotería del Cauca	Sistemas	5	5	5	5	20
3.Nicoftp server	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20
4.MySQL	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20
5.Antivirus (KARSPESKY)	30	Computadores	Lotería del Cauca	Sistemas	3	3	3	3	12
6.Windows	30	Computadores	Lotería del Cauca	Sistemas	3	3	3	3	12
7.server2011	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20
DATOS/INFORMACION									
BASES DE DATOS									
EQUIPOS INFORMATICOS									
1.Servidor HP proliant	1	Cuarto TELCO	Lotería del Cauca	Sistemas	5	5	5	5	20
2.Enrutadores	1	Cuarto TELCO	Lotería del Cauca	Sistemas	3	3	3	3	12
3.Transceiver	1	Cuarto TELCO	Lotería del Cauca	Sistemas	3	3	3	3	12
4.Planta telefónica	1	Cuarto TELCO	Lotería del Cauca	Sistemas	1	1	1	1	4
5.Equipo de seguridad perimetr	1	Cuarto TELCO	Lotería del Cauca	Sistemas	3	3	3	3	12
ISP INTERNET									
1.Emtel	1	Cuarto TELCO	Contratista	Sistemas	1	1	1	5	8
2.Dobleclik	1	Cuarto TELCO	Contratista	Sistemas	1	1	1	5	8
3.Radioenlace contingencia	1	Antena ultimo piso edificio	Contratista	Sistemas	1	1	1	1	4
SOPORTES DE INFORMACION									
1.DD externos	6	Caja de seguridad-activo	Lotería del Cauca	Sistemas	5	5	5	5	20
2.DD interno del servidor	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20
2.DD interno de cada estación d	30	PC individual	Lotería del Cauca	Recursos Físicos	3	3	3	3	12
EQUIPO AUXILIAR									
1. UPS	2	Cuarto TELCO	Lotería del Cauca	Sistemas	3	3	3	3	12
2.Red electrica	1	Cuarto TELCO	Lotería del Cauca	Recursos Físicos	3	3	3	3	12
3.Red LAN	1	Cuarto TELCO	Lotería del Cauca	Recursos Físicos	3	3	3	3	12
4.Aire acondicionado minisplit	5	Cuarto TELCO	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
INSTALACIONES									
1.Cuarto TELCO	1	Edificio Lotería del Cauca	Lotería del Cauca	Recursos Físicos	5	5	5	5	20
2.Gabinete (Rack)	1	Cuarto TELCO	Lotería del Cauca	Recursos Físicos	5	5	5	5	20
3.Estaciones de trabajo	32	Edificio Lotería del Cauca	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
LICENCIAS									
1.Antivirus para 30 equipos	30	PC individual	Lotería del Cauca	Sistemas	3	3	3	3	12
2.Windows server	1	Servidor	Lotería del Cauca	Sistemas	5	5	5	5	20
3.Licencia de uso sw velero	1	Modulos software veler	Lotería del Cauca	Sistemas	5	5	5	5	20

IMPRESIÓN Y ESCANNEO									
1. Puntos de impresión	2	Instalaciones Lotería del	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
2. escanner de alto rendimient	2	Tesorería- Juridica	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
3.Un escanner plano	1	Comercial	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
4. Impresoras auxiliares	8	Instalaciones Lotería del	Lotería del Cauca	Recursos Físicos	1	1	1	1	4
GRABACION Y MONITOREO									
1.Camaras de vigilancia	7	Instalaciones Lotería del	Lotería del Cauca	Recursos Físicos	3	3	3	3	12
2.Sistema biométrico	2	Instalaciones Lotería del	Lotería del Cauca	Recursos Físicos	3	3	3	3	12
PERSONAL									
1.ing. Encargado del proceso	1	Oficina de sistemas	Contrato de trab	Recursos Humanos	1	3	3	3	10
2.ing.de Apoyo	1	Oficina de sistemas	Contrato de trab	Recursos Humanos	1	3	3	3	10

EVALUACION DE LOS CONTROLES

Permite determinar en que medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo.

OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.

RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN						
	Probabilidad	Impacto		Tipo de Control aminora la probabilidad o el impacto	PUNTAJE Herramientas para ejercer el control: Posee una Herramienta para ejercer el control?	Existen manuales, Instructivos o procedimientos para el manejo de la herramienta?	En el tiempo que lleva la herramienta ha demostrado ser efectiva?	PUNTAJE Seguimiento al Control: Está definidos los responsables de la ejecución del control y del seguimiento?	La frecuencia de ejecución del control y seguimiento es adecuada?	Puntaje Final

Se evalúa verificando los registros y documentación.

RIESGO RESIDUAL Y OPCIONES DE MANEJO

		IMPACTO				
		1	2	3	4	5
PROBABILIDAD		INSIGNIFICANTE	MENOR	MODERADO	MAYOR	CATASTRÓFICO
1	RARO	ZONA DE RIESGO BAJA Asumir el riesgo	ZONA DE RIESGO BAJA Asumir el riesgo	ZONA DE RIESGO MODERADA Asumir el riesgo, Reducir el riesgo	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir
2	IMPROBABLE	ZONA DE RIESGO BAJA Asumir el riesgo	ZONA DE RIESGO BAJA Asumir el riesgo	ZONA DE RIESGO MODERADA Asumir el riesgo, Reducir el riesgo	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir
3	POSIBLE	ZONA DE RIESGO BAJA Asumir el riesgo	ZONA DE RIESGO MODERADA Asumir el riesgo, Reducir el riesgo	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir
4	PROBABLE	ZONA DE RIESGO MODERADA Asumir el riesgo, Reducir el riesgo	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir
5	CASI SEGURO	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE RIESGO ALTA Reducir el Riesgo, Evitar el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir	ZONA DE REISGO EXTREMA Reducir el riesgo, Compartir o transferir

OPCIONES DE MANEJO DE RIESGO:	
Asumir el riesgo	Luego que el riesgo ha sido reducido o trasnfereido puede quedar un riesgo residual que s emantiene, en este cado el jefe del proceso acepta la perdida residual probable.
Reducir el riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección)
Compartir o transferir el riesgo	Reduce su efecto a través del traspaso de las perdidas a otras organizaciones o la distribución de una proción del riesgo con otra entidad. Por ejemplo , la inforacion de gran importancia se puede duplicar y alamcenar en un lugar distante y de ubicción segura y nod ejarla concentrada en un solo lugar.
Evitar el riesgo	Tomar las medidas encaminadas a prevenir su materialización u ocurrencia.

MAPA DE RIESGOS

Lotería del Cauca	MAPA DE RIESGOS										CODIGO:GC-F10		
											VERSIÓN: 1		
PROCESO:	SISTEMAS				FECHA ACTUALIZACIÓN						junio 30 de 2018		
OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del hardware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.												
RIESGO	CALIFICACIÓN		EVALUACIÓN DEL RIESGO	CONTROLES	NUEVA CALIFICACIÓN			NUEVA EVALUACIÓN	OPCIONES DE MANEJO	TRATAMIENTO SEGÚN LA POLITICA ADMON RIESGO	PLAN DE ACCION (SOLO CUANDO EL RIESGO SE ENCUENTRE EN ZONA ALTA)	RESPONSABLE	
	Probabilidad	Impacto			Probabilidad	Impacto							
Infección de equipos por virus,acceso a información confidencial, perdida de la información, daño del equipo.	1	3	ZONA DE RIESGO MODERADA	Antivirus actualizados Programa de mantenimiento preventivo de equipos, progrma de copias de seguridad	1	3	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Cronograma con las fechas de vencimiento de los antivirus. Cronograma de mantenimiento de	Profesional Universitario Grado 01	
Perdida de información, daño en equipos.	1	4	ZONA DE RIESGO ALTA	Se dispone de una instalación básica de contingencia NINGUNO	1	4	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Se disponiendo de la instalación básica de contingencia		
Incomunicación en el momento de devoluciones en página web.	1	3	ZONA DE RIESGO MODERADA	Seguridad en el hosting Recibo de devoluciones via e-mail.	1	1	1	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Realizar registro y seguimiento de fallos de servicio, con el fin	Técnico Administrativo Grado 01	
Perdida de información, presentandose impedimentos al normal funcionamiento de actividades	1	5	ZONA DE RIESGO ALTA	Mantenimiento preventivo de la Base de Datos Servidor de respaldo	1	5	5	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Implantación de controles de seguridad que protejan la información de ataques externos e internos	Técnico Administrativo Grado 01	
Perdida de información confidencial.	1	2	ZONA DE RIESGO BAJA	Acceso restringido a visitantes. copias de seguridad	1	1	1	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES			
Falla en el mantenimiento de la infraestructura necesaria para lograr la conformidad con los requisitos del servicio	1	2	ZONA DE RIESGO BAJA	No se ha realizado mantenimiento físico y a sistema operativo al servidor de la empresa. Con el cambio a la nueva sede se realiza reemplazo de equipos. Se adquieren equipos de impresión de alta capacidad,se adquieren dos scanner de alta capacidad, se provee de un cuarto telco con especificaciones según la norma.	1	1	1	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Dar continuidad al plan de mantenimiento preventivo de los equipos de cómputo y servidores que se ejecute con forme se programe.	Profesional Universitario Grado 01	
Dependencia del proveedor	4	5	ZONA DE RIESGO EXTREMA	Se evita la solicitud directa entre usuario y proveedor y se implementa el registro de control de cambios, exigiendo para ello el formato de requerimiento F3. En el contrato de prestación de servicios se define que dará respuesta a los requerimientos teniendo en cuenta la complejidad o gravedad de la incidencia como tambien cursos de capacittación y reinducción, y entrega de registros logs a control interno.	2	5	10	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Definir administrador de sistemas con sus perfiles, accesos y responsabilidades. Creación de contingencia al no tener soporte del proveedor.	Profesional Universitario Grado 01	
Falla en la comunicación interna y externa.	1	2	ZONA DE RIESGO BAJA	Se implementan los correos institucionales en la empresa. Se realiza la adquisición de un PBX hibrido.IP/ANALOGO.	1	1	1	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES			
Distorsión en la imagen empresarial por falta de un adecuado diseño de página web.	1	3	ZONA DE RIESGO MODERADA	Se realiza el rediseño de la página web, se realiza cambio de proveedor. Se realiza la adquisicion de un componente Rsfirewall que corrige vulnerabilidades y mantiene la seguridad en la web.	1	1	1	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES			
Fallas en el servidor	1	5	ZONA DE RIESGO ALTA	Se programan dos (2)mantenimientos preventivos a servidor para el año 2016,se realizan copias de seguridad. NINGUNO	1	5	5	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	CRONOGRAMA, REGISTRO, DOCUMENTACION DEL SERVIDOR	Profesional Universitario Grado 01	
Fallas en el cuarto eléctrico	1	3	ZONA DE RIESGO MODERADA	El cuarto tiene un tiempo de servicio menor a un año, por el cual no se ha realizado su mantenimiento preventivo. NINGUNO	1	3	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES			
Fallas en equipos de computo e impresoras	3	3	ZONA DE RIESGO ALTA	Se realiza mantenimiento preventivo a impresoras y se programan dos (2) mantenimientos preventivos para los equipos para el año 2016. NINGUNO	1	3	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES			
Perdida de la información	1	4	ZONA DE RIESGO ALTA	Se programan dos (2)mantenimientos preventivos a servidor para el año 2016,se realizan copias de seguridad. NINGUNO	1	4	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Adquisición de un servidor .	Profesional Universitario Grado 01	

Perdida de la información	1	4	ZONA DE RIESGO ALTA	Se programan dos (2)mantenimientos preventivos a servidor para el año 2016,se realizan copias de seguridad. NINGUNO	1	4	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Adquisición de un servidor .	Profesional Universitario Grado 01
Incendio	1	3	ZONA DE RIESGO MODERADA	Se tiene instalado un aire acondicionado tipo minisplit. Se instala detector de humo y camara de vigilancia 7/24. NINGUNO	1	3	3	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Mantenimiento del cuarto TELCO	Profesional Universitario Grado 01
Ingresos no permitidos	2	4	ZONA DE RIESGO ALTA	El ingreso a este cuarto solo esta autorizado a los dos funcionarios del área de sistemas.Se instala cámara de vigilancia y acceso biometrico. NINGUNO	1	4	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES		
Ataques a la información	3	5	ZONA DE RIESGO EXTREMA	Se posee la protección básica de firewall de windows y el antivirus actualizado. Se adquiere un equipo de seguridad perimetral. NINGUNO	1	5	5	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Continuar con capacitciones a funcionarios alertando de los peligros informáticos	Técnico Admimistrativo Grado 01
Discordancia de datos al momento de la restauración	3	5	ZONA DE RIESGO EXTREMA	Se realiza un simulacro de restauración NINGUNO	3	5	15	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Continuar con simulacros de restauración y en base a ellas realizar un plan de restauración	Profesional Universitario Grado 01
Imposibilidad de restauración de la información como contingencia	3	4	ZONA DE RIESGO EXTREMA	Se realiza simulacro de restauración de copia de seguridad NINGUNO	3	4	12	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Continuar con simulacros de restauración de copias de seguridad y elaborar guia correspondiente	Profesional Universitario Grado 01
Ausencia de soporte técnico del proveedor unipersonal.	3	5	ZONA DE RIESGO EXTREMA	NINGUNO NINGUNO	3	5	15	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Solicitar al proveedor del aplicativo un modulo de administración	Profesional Universitario Grado 01
Redundancia en datos	3	3	ZONA DE RIESGO ALTA	Formato de requerimientos NINGUNO	3	3	9	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Seguimiento especifico a esta clase de eventos	Profesional Universitario Grado 01
Duplicidad en la información	3	3	ZONA DE RIESGO ALTA	Formato de requerimientos NINGUNO	3	2	6	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Seguimiento especifico a esta clase de eventos	Profesional Universitario Grado 01
Cambios sin registro de auditoria	3	4	ZONA DE RIESGO EXTREMA	Formato de requerimientos NINGUNO	3	3	9	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Seguimiento especifico a esta clase de eventos	Profesional Universitario Grado 01
Errores operativos	3	4	ZONA DE RIESGO EXTREMA	Formato de requerimientos NINGUNO	1	4	4	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Solicitar a proveedor la actualizacion de manuales de usurio	Profesional Universitario Grado 01
Imposibilidad de reanudación de actividades	3	5	ZONA DE RIESGO EXTREMA	Simulacro de Recuperación de operciones NINGUNO	3	5	15	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Plan de recuperacion de operciones	Técnico Admimistrativo Grado 02
Posibles errores no detectados	3	3	ZONA DE RIESGO ALTA	Planilla de pruebas NINGUNO	3	2	6	ZONA DE RIESGO BAJA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Seguimiento al plan de pruebas	Técnico Admimistrativo Grado 02
Retraso en solución de incidentes	3	4	ZONA DE RIESGO EXTREMA	Formato de requerimientos NINGUNO	3	3	9	ZONA DE RIESGO MODERADA	Asumir el riesgo	NO SE DEFINEN ACCIONES	Solicitar al proveedor del aplicativo un modulo de administración	Profesional Universitario Grado 01
Perdida de información e imposibilidad de reanudación de operaciones	3	5	ZONA DE RIESGO EXTREMA	Simulacro de recuperacion de operaciones NINGUNO	3	5	15	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Realizar diseño de continuidad de operaciones	Profesional Universitario Grado 01
Perdida de información	4	4	ZONA DE RIESGO EXTREMA	Verificación de la frecuencia de salvaguarda de la información NINGUNO	4	4	16	ZONA DE RIESGO ALTA	Asumir el riesgo	PLAN ACCIÓN	Realizacion y capacitación del procedimiento de salvaguarda de la información.	Profesional Universitario Grado 01