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 una adecuada 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 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

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.

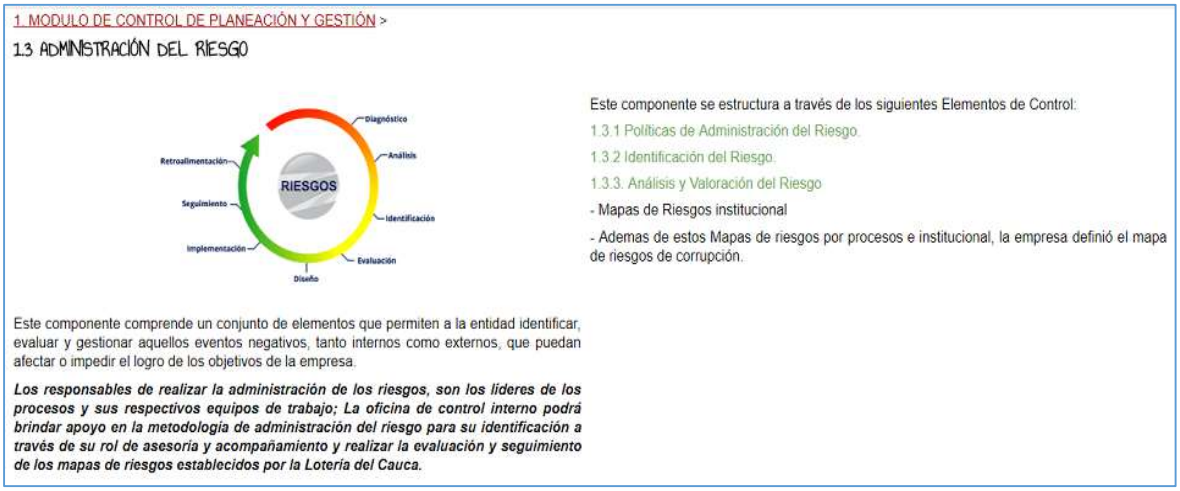
- Cuando la valoración del riesgo se localice en zona de riesgo alta, se definirán acciones para mitigar el riesgo, y se monitorean 1 vez al mes.
- Los procesos que se encuentren valorados en zona de riesgo alta y no tienen controles, deben establecerlos para evitar la materialización del riesgo.
- Los 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.
- 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



Las Guías Modelo de Seguridad y Privacidad de la Información, documentos son diseñados para un mejor entendimiento de las entidades en la implementación por parte del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC

- ✓ Modelo de Seguridad y Privacidad de la Información
- ✓ Instructivo Herramienta de Diagnostico
- ✓ Guía MIPG

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Figura 2 – Etapas previas a la implementación

Figura 3 - Fase de planificación[1]

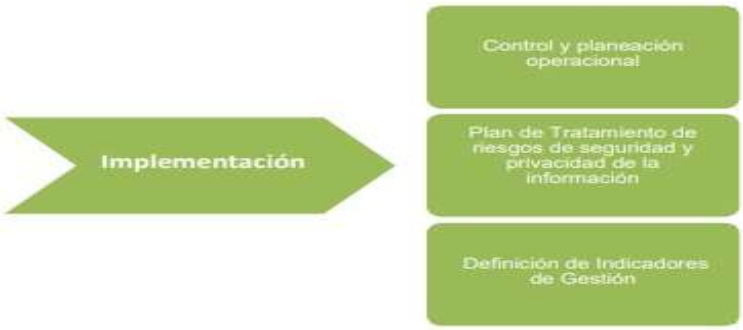


Figura 4 - Fase de implementación[2]

Figura 5 - Fase de Evaluación de desempeño[3]

Imágenes Tomadas de Guía Modelo de seguridad y privacidad de la información MinTic www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

	IDENTIFICACION Y ANALISIS DE SEGURIDAD DE LA INFORMACIÓN	CODIGO:PL – F28
		VERSIÓN: 1

PROCESO:	SISTEMAS	FECHA ACTUALIZACIÓN	31/03/2021
OBJETIVO DEL PROCESO:	Velar por el buen funcionamiento del harware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.		

RIESGO - QUÉ	TIPOLOGIA DEL RIESGO	CLASIFICACION DEL RIESGO	ACTIVO DE INFORMACIÓN	CAUSAS / VULNERABILIDADES	CONSECUENCIAS	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Perdida de confidencialidad,Integridad y disponibilidad de la información	Factor Humano	Operativo	1.Datos/Información	Desconocimiento de buenas prácticas	Perdida de información relevante	3 - Media	4 - Mayor	4 - EXTREMA
		Tecnológicos	1.Datos/Información	Divulgación no autorizada de claves	Apropiación ilicita de información sensible	1- Muy Baja	4 - Mayor	3 - ALTA
		Operativo	1.Datos/Información	Desactualización de la información	Producción de información inexacta	3 - Media	3 - Moderado	3 - ALTA
	Fisico	Tecnológicos	4.Equipos Informaticos	Fallas tecnológicas	Reprocesos	4 - Alta	3 - Moderado	3 - ALTA
	Factor Humano	Operativo	1.Datos/Información	Falta de claridad en el nivel de responsabilidad y autoridad	Problemas de articulación en resultados entre servidores,niveles jerárquicos y dependencia	4 - Alta	2 - Menor	3 - ALTA
		Estratégicos	2.Servicio	Flujos de comunicación deficientes y desarticularizados	Perdida de imagen y credibilidad institucional	4 - Alta	2 - Menor	1- BAJA
		Operativo	1.Datos/Información	Inadecuado manejo de roles y privilegios del personal en acceso a la información	Acceso a la información por parte de personal no autorizado	1- Muy Baja	4 - Mayor	3 - ALTA
		Operativo	1.Datos/Información	Incumplimiento de politicas	Procesos disciplinarios	3 - Media	2 - Menor	2 - MODERADA
		Estratégicos	1.Datos/Información	Desconocimiento del nivel de clasificación o reserva de la información	incumplimiento a la ley de protección de datos personales y otras.	3 - Media	2 - Menor	2 - MODERADA
		Operativo	1.Datos/Información	Inadecuada aplicación de los procedimientos	Ineficiencia operativa y administrativa	4 - Alta	3 - Moderado	3 - ALTA
	Lógico	Operativo	3.Software/Aplicaciones informaticas	Alta dependencia en proveedor externo para la operación del sistema de información	Demoras en las respuestas a eventos o entrega de productos o servicios.	4 - Alta	4 - Mayor	4 - EXTREMA
	Lógico	Tecnológicos	3.Software/Aplicaci	Falta de fortalecimiento en herramientas para bloquear ataques	Perdida de información			

	CONTEXTO ESTRATÉGICO	CODIGO:PL - F16
		VERSIÓN: 3

PROCESO:	SISTEMAS	FECHA ACTUALIZACIÓN	31/03/2021
OBJETIVO DEL PROCE	Velar por el buen funcionamiento del harware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.		

CONTEXTO EXTERNO		CAUSAS
TECNOLÓGICOS Y/O DE SERVICIOS	Nuevas tecnológias de la información y comunicaciones	Falta de fortalecimiento en herramientas para bloquear ataques informáticos,suplantación de identidad, robo de datos.
	Falta de suministro de energía	Falla en el servicio contratado, se carece de plan de contingencia (energia)
	Proveedores de servicios de tecnológias externos(hosting)	Falla en el servicio contratado, se carece de plan de contingencia(hosting)
	Falla en el servicio de acceso a internet	Falla en la conectividad y suministro del servicio (internet)
AMBIENTALES	Condiciones inadecuadas de temperatura o humedad	Falta de adecuación del sitio alterno definido
	Catastrofes Naturales: destrucción total o parcial de la infraestructura.	
SOCIO POLITICOS	Asonada,Terrorismo.	Ausencia de un plan de contingencia para afrontar situaciones de asonada o terrorismo
		En caso necesario abandonar el lugar de trabajo por riesgo grave o inminente para la vida o la salud

CONTEXTO INTERNO		CAUSAS
FINANACIEROS	Incumplimiento a actividades del plan de acción	Cambios en la prioridad presupuestal
	Incumplimiento a actividades del plan de adquisición de herramientas tecnológicas	Falta de recursos
PERSONAL	Obsolescencia de los conocimientos del personal	Falta de capacitación y actualización de conocimientos
		Concentración de conocimiento en las personas, NO en los procesos

VALORACION DE CONTROLES

		VALORACIÓN DE CONTROLES																		CODIGO:PL - F19		
																				VERSIÓN: 1		
		SISTEMAS											FECHA DE ACTUALIZACIÓN:							31/03/2021		
	PROCESO	Velar por el buen funcionamiento del harware y software de la empresa atendiendo oportunamente los requerimientos de los procesos y garantizando la seguridad informática de la empresa.																				
RIESGO	ACTIVIDADES DE CONTROL	CONTROL PREVENTIVO, DETECTIVO O CORRECTIVO	DISEÑO DEL CONTROL																			
			RESPONSABLE		PERIODICIDAD	PROPOSITO	COMO SE REALIZA LA ACTIVIDAD DE CONTROL	QUE PASA CON LAS OBSERVACIONES O DESVIACIONES	EVIDENCIAS DE LA EJECUCION DEL CONTROL	CALIFICACION	PESO DISEÑO DEL CONTROL	PROMEDIO DEL DISEÑO DE LOS CONTROLES	PESO EJECUCION DEL CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL	PROMEDIO SOLIDEZ	SOLIDEZ DEL CONJUNTO DE CONTROLES			
			Existe un responsable asignado a la ejecución del control?	El responsable tiene autoridad y adecuada segregación de funciones en la ejecución del control?	La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	La actividad que desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej. Verificar, validar, cotejar, comparar, revisar, etc.?	La fuente de información que utiliza en el desarrollo del control, es información confiable que permita mitigar el riesgo?	Las observaciones, desviaciones o diferencias identificadas como resultado de la ejecución del control son investigadas y resueltas de manera oportuna?	Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?											
Perdida de confidencialidad,Integridad y disponibilidad de la información	Manual de buenas practicas	PREVENTIVO	15	15	15	15	15	15	10	100	FUERT	93	MODE	50	SI	82	MODERADO					
	Políticas de seguridad de la información	PREVENTIVO	15	15	15	15	15	15	10	100	FUERT		MODE	50	SI							
	Auditorias internas o externas	DETECTIVO	15	15	15	10	15	15	10	95	DÉB		FUER	100	NO							
	Contratos de soporte y mantenimiento	PREVENTIVO	15	15	15	15	15	15	10	100	FUER		FUER	100	NO							
	Manual de funciones	DETECTIVO	15	15	15	15	15	15	10	100	DÉB		FUE	100	SI							
	Procedimientos	PREVENTIVO	15	15	15	0	15	0	5	65	DÉB		MO	50	SI							
	UTM	PREVENTIVO	15	15	15	15	15	15	10	100	FUER		FUER	100	NO							

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	
5	1	2	Política de Seguridad de la Información								
		2	Orientación de la dirección para la gestión de la seguridad de la información								
		1	Debe	Políticas para la seguridad de la información	SI				X		
		2	Debe	Revisión de las políticas de seguridad de la información	SI				X		
6	2	7	Organización de la seguridad de la información								
	1	5	Organización Interna								
		1	Debe	Roles y responsabilidades para la seguridad de la información	SI				X		
		2	Debe	Separación de deberes	SI					X	
		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							
7	3	6	Seguridad de los recursos humanos								
	1	2	Antes de asumir el empleo								
		1	Debe	Selección	T. H.		X				
		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				

Lotería del Cauca
NIT 891500650-6
PBX: (2) 823 38 56 FAX: (2) 823 12 34
Cra 7 # 1N - 66, Edificio Lotería del Cauca
Popayán (Cauca)

Motivos para avanzar

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**								
	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					
		3	**Clasificación de la información**								
8	2	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	**Manejo de medios**								
		1	Debe	Gestión de medios removibles	SI						Politica de uso de dispositivos de almacenamiento extraibles
	3	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**								
		2	**Áreas Seguras**								
	1	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	
		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					
	2	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					
9		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.
		5	**Control de acceso a sistemas y aplicaciones**								
		1	Debe	Restricción de acceso a la información	SI				X		Politica de administracion de contraseña
	4	2	Debe	Procedimiento de ingreso seguro	SI					X	Politica de administracion de contraseña
		3	Debe	Sistema de gestión de contraseña	SI					X	Politica de administracion 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**								
		2	**Controloes criptográficos**								
10	1	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 TECNOLÓGICOS LOTERIA DEL CAUCA-SISTEMAS

ACTIVO	CANT	UBICACIÓN	PROPIETARIO	CUSTODIO	$	C	I	D	TOTAL	CLASIFICACION
DATOS/INFORMACION										
BASES DE DATOS										
1.De velero	1	Servidor # 05 físico DELLR630	Lotería del Cauca	Responsable Sistema	5	5	5	5	20	ALTO
2.De hosting devoluciones	1	Servidor web	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
BACKUPS										
1.BD de velero	1	Servidor físico	Lotería del Cauca	Responsable Sistema	5	5	5	5	20	ALTO
2.BD hosting devoluciones	1	Servidor web	servidor web	Contratista	5	5	5	5	20	ALTO
INFORMACION										
1.correo instiutcional	30	Servidor web	Lotería del Cauca	Sistemas	3	5	3	3	14	MEDIO
CONTRASEÑAS										
1.computadores	38	Estaciones de trabajo	Lotería del Cauca	Recursos Físicos	3	5	5	5	18	ALTO
2.portatiles	4	Estaciones de trabajo	Lotería del Cauca	Recursos Físicos	3	5	5	5	18	ALTO
3.sw velero	1	Licencia de uso	Lotería del Cauca	Responsable Sistema	5	5	5	5	20	ALTO
4.correo institucional	30	Servidor web GOOGLE	GMAIL	Sistemas	3	5	5	5	18	ALTO
SERVICIOS										
AL PUBLICO EN GENRAL										
1. Página web	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12	MEDIO
2.facebook	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12	MEDIO
3.twitter	1	Servidor web	Lotería del Cauca	Sistemas	3	3	3	3	12	MEDIO
AL USUARIO INTERNO										
1.ftp	2	Computadores sistemas	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
AL USUARIO EXTERNO										
1.Nuevodevoluciones	1	Servidor web	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
SW/APLICACIONES INFORMATICAS										
1.Office	42	Computadores	Lotería del Cauca	Sistemas	3	3	3	3	12	MEDIO
2.Nicoftp	2	Computadores sistemas	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
3.Nicoftp server	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
4.MySQL	1	Servidor físico	Lotería del Cauca	Sistemas	5	5	5	5	20	ALTO
5.Antivirus (KARSPESKY)	35	Computadores	Lotería del Cauca	Sistemas	3	3	3	3	12	MEDIO

MAPA Y PLAN DE TRATAMIENTO DE RIESGOS

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

MAPA Y PLAN DE TRATAMIENTO DE RIESGOS

PROCESO	SISTEMAS														FECHA DE ACTUALIZACIÓN:
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 INHERENTE					RIESGO RESIDUAL							
	RIESGO	CAUSAS	CONSECUENCIAS	PROBABILIDAD		IMPACTO		NIVEL	CONTROL EXISTENTE	PROBABILIDAD		IMPACTO		NIVEL	OPCIÓN DE MANEJO	ACCIONES PREVENTIVAS	RESPONSABLE
1	Perdida de confidencialidad,integridad y disponibilidad de la información	Desconocimiento de buenas prácticas	Perdida de información relevante	3	Media	4	Mayor	EXTREMO	Manual de buenas practicas	1	Muy Baja	4	Mayor	ALTO	REDUCIR	Continuar con la verificación,revisión y validación	Profesional Universitario/Técnico administrativo grado 04
		Divulgación no autorizada de claves	Apropiación ilícita de información sensible	1	Muy bajo	4	Mayor	ALTO	Políticas de seguridad de la información	1	Muy Bajo	3	Moderado	MODERADO	EVITAR	Socializar y dar a conocer los diferentes riesgos de seguridad digital	Profesional Universitario/Técnico administrativo grado 04
		Desactualización de la información	Producción de información incorrecta	3	Media	3	Moderado	ALTO	Auditorias internas o externas	3	Media	2	Menor	MODERADO	EVITAR	Autocontrol y verificación de la información	Profesional Universitario/Técnico administrativo grado 04
		Fallas tecnológicas	Reprocesos	4	Alta	3	Moderado	ALTO	Contratos de soporte y mantenimiento	3	Media	2	Menor	MODERADO	EVITAR	Registrar las novedades para seguimiento	Profesional Universitario/Técnico administrativo grado 04
		Falta de claridad en el nivel de responsabilidad y autoridad	Problemas de articulación en resultados entre servidores,niveles jerárquicos y dependencia	4	Alta	2	Menor	ALTO	Manual de funciones	2	Baja	2	Menor	BAJO	ACEPTAR	Socializar al interior del área la novedad y el responsable de dar solución	Profesional Universitario/Técnico administrativo grado 04
		Flujos de comunicación deficientes y desarticularizados	Perdida de imagen y credibilidad institucional	1	Muy bajo	2	Menor	BAJO	Procedimientos	1	Muy Bajo	2	Menor	BAJO	ACEPTAR	Reinducción para cada aplicación a las personas que participan en los procesos	Profesional Universitario/Técnico administrativo grado 04
		Inadecuado manejo de roles y privilegios del personal en acceso a la información	Acceso a la información por parte de personal no autorizado	1	Muy bajo	4	Mayor	ALTO	UTM	1	Muy Bajo	3	Moderado	MODERADO	EVITAR	Continuar con la verificación y monitoreo de eventos	Profesional Universitario/Técnico administrativo grado 04
		Incumplimiento de políticas	Procesos disciplinarios	3	Media	2	Menor	MODERADO	Seguridad física (cámaras) y de acceso (biométrico) a las instalaciones	2	Baja	2	Menor	BAJO	ACEPTAR	Campañas de socialización de cumplimiento de políticas	Profesional Universitario/Técnico administrativo grado 04
		Desconocimiento del nivel de clasificación o reserva de la información	incumplimiento a la ley de protección de datos personales y otras.	3	Media	2	Menor	MODERADO	Políticas de seguridad de la información	2	Baja	2	Menor	BAJO	ACEPTAR	Socializar y dar a conocer los diferentes riesgos de seguridad digital	Profesional Universitario/Técnico administrativo grado 04
		Inadecuada aplicación de los procedimientos	Ineficiencia operativa y administrativa	4	Alta	3	Moderado	ALTO	Auditoria interna o externa	3	Media	2	Menor	MODERADO	EVITAR	Reinducción para cada aplicación a las personas que participan en los procesos	Profesional Universitario/Técnico administrativo grado 04
		Alta dependencia en proveedor externo para la operación del sistema de información	Demoras en las respuestas a eventos o entrega de productos o servicios.	4	Alta	4	Mayor	EXTREMO	Auditoria interna o externa	3	Media	3	Moderado	ALTO	REDUCIR	Vinculación de personal especializado en programación y desarrollo de software	Profesional Universitario/Técnico administrativo grado 04
	Impedimento al normal funcionamiento de actividades,imposibilidad de acceder a datos e información	Falla en el servicio contratado, se carece de plan de contingencia (energía)	Reprocesos y demora en la ejecución de actividades	4	Alta	4	Mayor	EXTREMO	Concesión no Convencional	3	Media	3	Moderado	ALTO	REDUCIR	Incluir anualmente en el plan de compras la adquisición de una planta electrica para toda la empresa Lotería del Cauca	Profesional Universitario/Técnico administrativo grado 04
		Falla en el servicio contratado, se carece de plan de contingencia(hosting)	Perdida de la imagen institucional	3	Media	3	Moderado	ALTO	Supervisoría	3	Media	2	Menor	MODERADO	EVITAR	Seguimiento mensual de la información registrada por el supervisor	Profesional Universitario/Técnico administrativo grado 04
		Falla en la conectividad y suministro del servicio (Internet)	Perdida de capacidad operativa	4	Alta	4	Mayor	EXTREMO	Supervisoría	4	Alta	2	Menor	MODERADO	EVITAR	Seguimiento mensual de la información registrada por el supervisor	Profesional Universitario/Técnico administrativo grado 04
		Falta de adecuación del sitio alterno definido	Improvisaciones	1	Muy baja	2	Menor	BAJO	Plan de acción	2	Baja	2	Menor	BAJO	ACEPTAR	Continuar con la verificación	Profesional Universitario/Técnico administrativo grado 04
		Ausencia de un plan de contingencia para afrontar situaciones de asonada o terrorismo	Ambiente de incertidumbre	3	Media	3	Moderado	ALTO	Protocolos Institucionales	3	Media	3	Moderado	ALTO	REDUCIR	Cumplir con procedimientos y protocolos establecidos por la empresa	Profesional Universitario/Técnico administrativo grado 04
		En caso necesario abandonar el lugar de trabajo por riesgo grave o inminente para la vida o la salud	Ambiente de incertidumbre	5	Muy alta	4	Mayor	EXTREMO	Protocolos Institucionales	4	Alta	3	Moderado	ALTO	REDUCIR	Cumplir con procedimientos y protocolos establecidos por la empresa	Profesional Universitario/Técnico administrativo grado 04
		El sistema informatico de la empresa es propiedad de un tercero uniprocesal	Apropiación de datos e información empresarial	3	Media	4	Mayor	EXTREMO	Supervisoría	3	Media	3	Moderado	ALTO	REDUCIR	Seguimiento mensual de la información registrada por el supervisor	Profesional Universitario/Técnico administrativo grado 04
3	Direccionamiento indebido de información,abuso de confianza	Ausencia de modulo de administración, dependencia total de soporte en general del proveedor	Ineficiencia operativa y administrativa	3	Media	3	Moderado	ALTO	Auditoria interna o externa	3	Media	3	Moderado	ALTO	REDUCIR	Vinculación de personal especializado en programación y desarrollo de software	Profesional Universitario/Técnico administrativo grado 04
		Dispersión y redundancia de datos que conllevn a información inconsistente	Producccion de información incorrecta	3	Media	3	Moderado	ALTO	Auditoria interna o externa	3	Media	2	Menor	MODERADO	EVITAR	Fortalecer la revisión, verificación y validación de la información	Profesional Universitario/Técnico administrativo grado 04
		Falta de mecanismos de control para soportar la integridad de los datos	Inseguridad en la autenticidad de los datos	3	Media	3	Moderado	ALTO	Auditoria interna o externa	3	Media	2	Menor	MODERADO	EVITAR	Fortalecer la revisión, verificación y validación de la información	Profesional Universitario/Técnico administrativo grado 04
		Ausencia del personal a las capacitaciones	Ineficiencia operativa y administrativa	4	Alta	2	Menor	ALTO	Cronograma de capacitaciones	3	Media	3	Moderado	ALTO	REDUCIR	Programar en conjunto con la oficina de talento humano y Gerencia la asistencia obligatoria a las capacitaciones programadas	Profesional Universitario/Técnico administrativo grado 04
4	Manejo desarticulado de documentación e información entre procesos	Debilidad en la articulación de procesos	Inadecuada toma de decisiones	3	Media	3	Moderado	ALTO	Procedimientos	3	Media	2	Menor	MODERADO	EVITAR	Validar con los lideres la información reportada para realizar los ajustes en caso de requerirse	Profesional Universitario/Técnico administrativo grado 04
		Alta resistencia al cambio	Atraso en innovación y avance de resultados	5	Muy alta	3	Moderado	EXTREMO	Procedimientos	4	Alta	2	Menor	ALTO	REDUCIR	Proyecto de trabajo en equipo, y concientización de autoaprendizaje	Profesional Universitario/Técnico administrativo grado 04
		No ejecución de acciones definidas para el tratamiento de eventos entre los procesos	Inadecuada toma de decisiones	3	Media	3	Moderado	ALTO	Procedimientos	3	Media	2	Menor	MODERADO	EVITAR	Planes de mejoramiento y procedimientos claros de cargue de información entre los procesos	Profesional Universitario/Técnico administrativo grado 04
5	Manejo inadecuado de la información	Inadecuado manejo del canal de información oficial,registrada,autorizada y firmada	Errores en el almacenamiento de la información	2	Baja	2	Menor	BAJO	Procedimientos	2	Baja	2	Menor	BAJO	ACEPTAR	Realizar una planificación coordinada para el manejo de la información y sus responsables	Profesional Universitario/Técnico administrativo grado 04
6	Daño y/o Obsolescencia de equipos	Deficiente gestión para la adquisición de equipos y herramientas tecnológicas, contemplado en el plan de acción anual.		2	Baja	2	Menor	BAJO	Plan de acción	2	Baja	2	Menor	BAJO	ACEPTAR		
7	Deficiencia en la entrega oportuna de resultados	Falta de gestión y liderazgo		3	Media	2	Menor	MODERADO	Matriz de Planificación de Cambios	3	Media	2	Menor	MODERADO	EVITAR	Desarrollar los ejes de gestión del conocimiento	Profesional Universitario/Técnico administrativo grado 04