2023

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

Lotería del Cauca

1-1-2023

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.

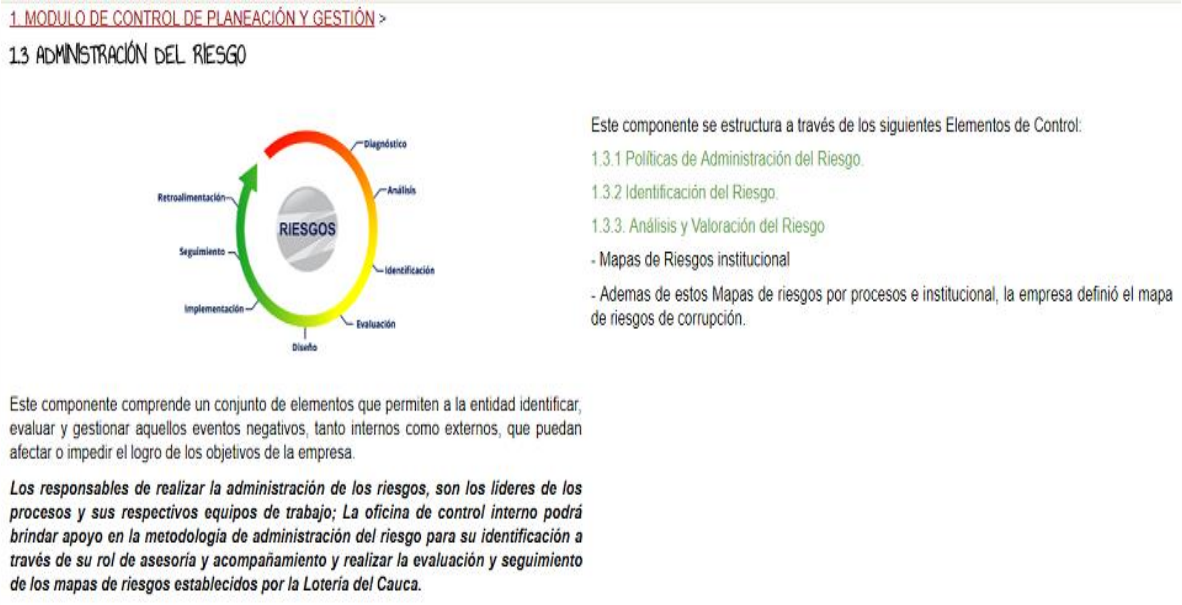
- Cuando la valoración del riesgo los ubique en zona de riesgo baja o moderada, se debe continuar con la aplicación de los controles establecidos, si se tienen, y seguir con el monitoreo trimestral al riesgo identificado.
- Cuando la valoración del riesgo se localice en zona de riesgo alta, se definirán 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



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.

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
- ✓ GuíaMIPG

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

Figura 2 – Etapas previas a la implementación

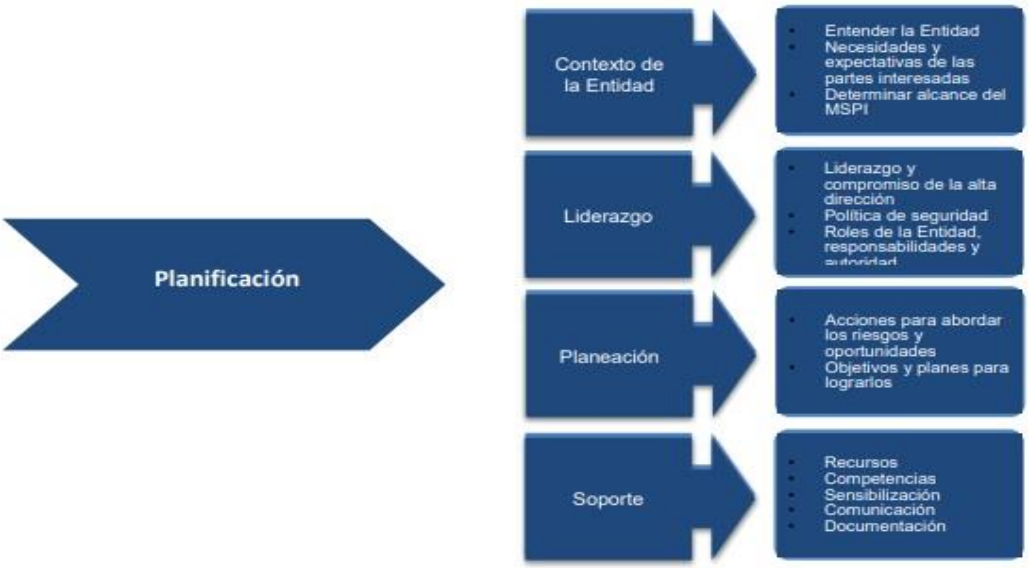


Figura 3 - Fase de planificación[1]

Figura 4 - Fase de implementación[2]

Figura 5 - Fase de Evaluación de desempeño[3]

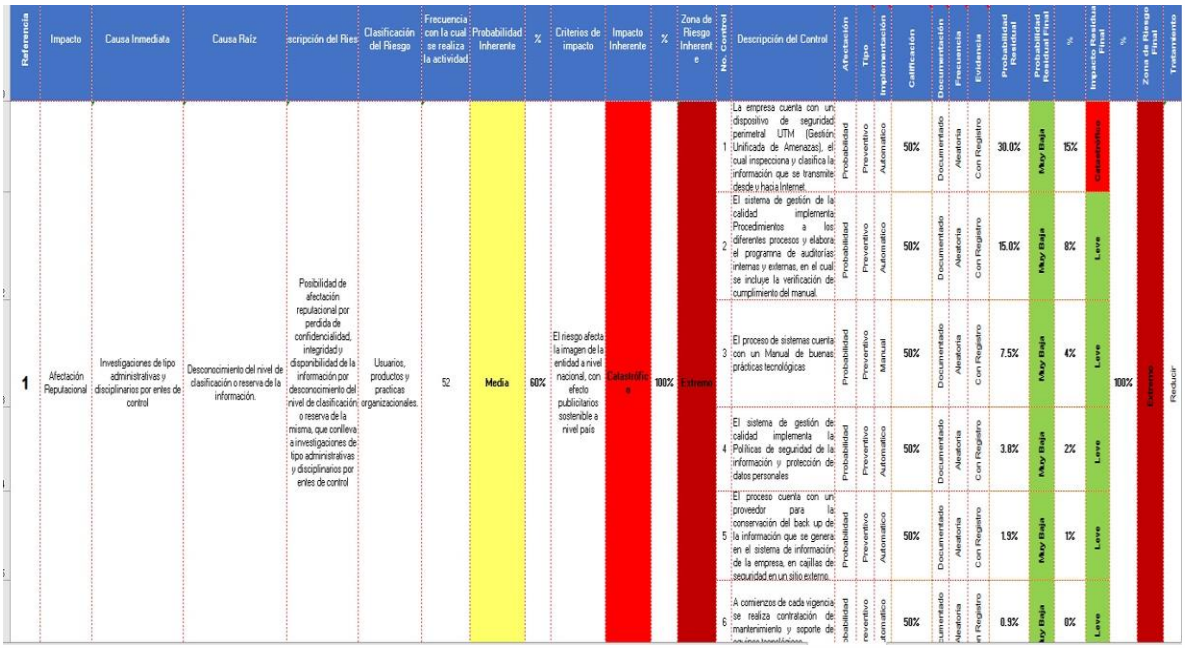
Imágenes Tomadas de Guía Modelo de seguridad y privacidad de la información MinTic www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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)

MATRIZ DE IDENTIFICACIÓN DEL RIESGO

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.



Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad	Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente	No. Control	Descripción del Control	Afectación	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia	Probabilidad Residual	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
1	Afectación Reputacional	Investigaciones de tipo administrativas y disciplinarios por entes de control	Desconocimiento del nivel de clasificación o reserva de la información.	Posibilidad de afectación reputacional por pérdida de confidencialidad, integridad y disponibilidad de la información por desconocimiento del nivel de clasificación o reserva de la misma, que conlleva a investigaciones de tipo administrativas y disciplinarios por entes de control	Usuarios, productos y practicas organizacionales.	52	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	La empresa cuenta con un dispositivo de seguridad perimetral UTM (Gestión Unificada de Amenazas), el cual inspecciona y clasifica la información que se transmite desde y hacia Internet.	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	30.0%	Muy Baja	15%	Catastrófico	100%	Extremo	Reducir
													2	El sistema de gestión de la calidad implementa Procedimientos a los diferentes procesos y elabora el programa de auditorías internas y externas, en el cual se incluye la verificación de cumplimiento del manual.	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	15.0%	Muy Baja	8%	Leve			
													3	El proceso de sistemas cuenta con un Manual de buenas prácticas tecnológicas	Probabilidad	Preventivo	Manual	50%	Documentado	Aleatoria	Con Registro	7.5%	Muy Baja	4%	Leve			
													4	El sistema de gestión de calidad implementa la Políticas de seguridad de la información y protección de datos personales	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	3.8%	Muy Baja	2%	Leve			
													5	El proceso cuenta con un proveedor para la conservación del back up de la información que se genera en el sistema de información de la empresa, en cajillas de seguridad en un sitio externo.	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	1.9%	Muy Baja	1%	Leve			
													6	A comienzos de cada vigencia se realiza contratación de mantenimiento y soporte de	Probabilidad	Preventivo	Automático	50%	Documentado	Aleatoria	Con Registro	0.9%	Muy Baja	0%	Leve			
2	Afectación económica	Reproceso y demoras en la ejecución de actividades	Pérdida de capacidad operativa por diferentes causas: asonada, terrorismo, pandemia, abandono del lugar de trabajo por inminente riesgo grave a la vida o la salud, y/o desastres naturales.	Posibilidad de afectación económica por impedimento al normal funcionamiento de actividades, imposibilidad de acceder a datos e información; conlleva a reproceso y demoras en la ejecución de actividades y pérdida de capacidad operativa por diferentes causas asonada, terrorismo, pandemia	Usuarios, productos y practicas organizacionales.	52	Media	60%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	1	La empresa cuenta con un plan de continuidad de negocio	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	30.0%	Muy Baja	15%	Moderado	60%	Moderado	Aceptar
													2	Se cuenta con la posibilidad de conexiones remotas para trabajo en casa	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro	15.0%	Muy Baja	8%	Leve			
													3	El proceso cuenta con un proveedor para la conservación del back up de la información que se genera en el sistema de información de la empresa, en cajillas de seguridad en un sitio externo.	Probabilidad	Preventivo	Manual	50%	Documentado	Aleatoria	Con Registro	7.5%	Muy Baja	4%				
3	Afectación Reputacional	Dependencia total del proveedor	El sistema informático de la empresa es propiedad de un tercero unipersonal.	Posibilidad de afectación reputacional por la gestión indebida de la información por parte del proveedor unipersona del sistema informático ya que este es de su	Fraude Interno,	52	Media	60%	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	Catastrófico	100%	Extremo	1	Seguimiento mensual realizado por el supervisor, con formatos unificados según el SGC	Probabilidad	Detectivo	Automático	50%	Documentado	Continua	Con Registro	30.0%	Muy Baja	15%	Catastrófico	100%	Extremo	Reducir
4	Afectación Económica	Posibles requerimientos de entes de control y de los procesos internos de la entidad	Gestión del control documental del sistema de gestión de calidad fuera de los requisitos procedimentales	Posibilidad de afectación económica debido a la pérdida de información del sorteo por daño en las bases de datos, software o hardware o ataques informáticos.	Fallas Tecnológicas	52	Media	60%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	La empresa adquiere un segundo servidor espejo y se programan copias de respaldo de la información.	Probabilidad	Correctivo	Automático	FALSO	Documentado	Continua	Con Registro	60.0%	Media	60%	Menor	40%	Moderado	Reducir
													2	Cronograma y ejecución de mantenimiento preventivo de equipos	Probabilidad	Correctivo	Automático	FALSO	Documentado	Continua	Con Registro	60.0%	Media	60%	Leve			

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)

5	Afectación Reputacional	Incumplimiento de las disposiciones legales	Desconocimiento y/o desactualización de las normas o leyes respecto a las políticas de gobierno digital	Posibilidad de afectación reputacional por incumplimiento a normatividad sobre transparencia y acceso a la	Usuarios, productos y practicas organizacionales.	12	Baja	40%	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector	Catastrófico	100%	Extremo	1	Se cuenta con Normagrama del proceso actualizado	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	20.0%	Muy Baja	10%	Catastrófico	100%	Extremo	Reducir
6	Afectación Reputacional	Generación de papel en la documentación, poco espacio para almacenamiento en archivo físico	Se sigue utilizando el papel en la documentación diaria laboral generando falta de espacio en el almacenamiento de archivos, propenso al daño, con limitaciones en edición, redundancia de copias y daño ambiental	Posibilidad de afectación reputacional por el manejo desarticulado de documentación e información entre procesos	Ejecución y Administración de procesos	12	Baja	40%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Se realiza en recepción radicación manual de documentación de oficios internos y externos.	Probabilidad	Preventivo	Automático	FALSO	Documentado	Continua	Con Registro	40.0%	Baja	40%	Moderado	60%	Moderado	Reducir
													2	Se realiza la custodia de los documentos en papel Archivo físico	Probabilidad	Preventivo	Automático	FALSO	Documentado	Continua	Con Registro	40.0%	Baja	40%	Leve			
7	Afectación Económica	ación de leyes y normas en	Aplicación, seguimiento y ejecución de planes y programas para potenciar de manera favorable para la empresa el clima laboral y la motivación. Identificación de los peligros físicos y de salud mental a los cuales puede encontrarse un funcionario.	Posibilidad de afectación económica por la inadecuada gestión del conocimiento en optimización de condiciones de seguridad laboral física y salud mental, y no aplicación de leyes y normas en sst, se materializa el riesgo	Relaciones Laborales	12	Baja	40%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	El proceso de planeación implementa el Plan de SST.	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	20.0%	Muy Baja	10%	Menor	40%	Bajo	Aceptar
													2	Programación de Capacitaciones	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	10.0%	Muy Baja	5%	Leve		Bajo	Aceptar

8	Afectación Económica	Empalme y entrega de puesto de trabajo con toda la documentación necesaria del funcionario Profesional Universitario Grado 01 Responsable del área de sistemas saliente al funcionario entrante.	De acuerdo a la planta de personal en el área de sistemas se encuentra creado un (1) cargo de Profesional Universitario para TIC con el apoyo de un técnico administrativo grado 04, los cuales son los únicos que tienen el conocimiento y la experiencia del procesos misionales se presenta la renuncia por jubilación del Profesional Universitario, y queda únicamente el Técnico administrativo al frente de los eventos que se presenten tanto en el Proceso de Sistemas como los procesos	Posibilidad de afectación económica por inadecuada gestión del conocimiento fallas tecnológicas, inadecuada realización de procedimiento en sorteo, errores en publicaciones de resultados, generación y envío de archivos a entidades de control extemporáneas, empalme y entrega de puesto de trabajo	Fallas Tecnológicas	52	Media	60%	Entre 100 y 500 SMLMV	Mayor	80%	Alto	1	Contratación de prestación de servicios a ingenieros externos para labores especificas de soporte.	Probabilidad	Detectivo	Manual	35%	Documentado	Continua	Con Registro	80.0%	Alta	80.0%	Mayor	80%	Alto
9	Afectación Reputacional	Resolución de trabajo en caso duración de la pandemia	No contextualizar a todo el personal del trabajo en casa, porque es de aplicabilidad en toda la empresa	Posibilidad de afectación reputacional por seguridad de la información	Fallas Tecnológicas	360	Alta	80%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Alto	1	Copia de seguridad de la información crítica del proceso en el drive compartido.	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	40.0%	Muy Baja	20%	Moderado	60%	Moderado
		No realizar copias frecuentes de copias de seguridad	Vulnerabilidad de los equipos de trabajo en casa por debilidad del antivirus										2	Traslado de equipo de oficina para el trabajo en casa	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	20.0%	Muy Baja	10%	Leve		
		El funcionario cuente con un equipo de computo personal desactualizado	No le permita cumplir con las actividades en la modalidad de trabajo en casa de manera eficaz										3	El funcionario realiza el reporte del daño al operador de internet, del cual queda un numero radicado	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	10.0%	Muy Baja	5%	Leve		
10	Afectación Reputacional	Incumplimiento a los protocolos de bioseguridad implementados en la empresa	Contagio del virus covid-19	Posibilidad de afectación reputacional por condiciones de salud al equipo de trabajo	Ejecución y Administración de procesos	360	Alta	80%	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Alto	1	Verificación y seguimiento del cumplimiento a los protocolos de bioseguridad establecidos por el SG-SST, con acompañamiento de los comités y copasst.	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	40.0%	Muy Baja	20%	Moderado	60%	Moderado
													2	El aprendiz SENA de seguridad y salud en el trabajo hace entrega de elementos de protección personal a los funcionarios y lo regitra en el formato del mismo nombre, el primer día hábil de casa semana	Probabilidad	Preventivo	Manual	50%	Documentado	Continua	Con Registro	20.0%	Muy Baja	10%	Leve		

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).

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: Legal	Obligación contractual	Req.negocios/buena práctica	o de la evaluación de riesgos	OBSERVACIONES
	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	Política para dispositivos moviles	NO	No aplica					
		2	Debe	Teletrabajo	NO	No aplica					
	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				
7	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: Legal	Obligación contractual	Req.negocios/buena práctica	o de la evaluación de riesgos	OBSERVACIONES
	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					
8	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		Manejo de medios							
	3	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
	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							

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	
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						Política 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		Política de administración de contraseña
		2	Debe	Procedimiento de ingreso seguro	SI					X	Política de administración de contraseña
		3	Debe	Sistema de gestión de contraseña	SI					X	Política de administración de contraseña
		4	Debe	Uso de programas utilitarios privilegiados	NO	Falta política 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**							
10	1	2	Criptografía								
		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 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