INTRODUCCIÓN

El presente documento permite abordar desde la temática conceptual las fases para el tratamiento de riesgos que debe tener en cuenta durante el desarrollo de un SGSI comprendiendo la planificación e implementación, determinando la solución pertinente mediante la atención de las necesidades de la Lotería del Tolima teniendo en cuenta la relación costo beneficio.

TÉRMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante eldesarrollo de la gestión de riesgos de seguridad de la información.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos,entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Identificar brevemente los principales riesgos asociados que podría tener una empresa como la indicada

Para la Lotería del Tolima, con el proyecto seleccionado, ***para la elaboración de plan tratamientos de riesgos y evidencia de las vulnerabilidades técnicas***, este corresponde a la importancia que hay en el aseguramiento de los diferentes activos a nivel tecnológicos e infraestructura, con los cuales cuenta la compañía. Para poder realizar el correcto análisis se hace necesario realizar un análisis de las vulnerabilidades tomando como referencia el ítem 12.6 de la norma ISO/IEC 27002

Riesgo	Impacto del riesgo	Mitigación	Control
Ausencia de mecanismos de cifradoo métodos de cifrado débiles	Accesos no autorizados	Implementar mecanismos de cifrado	Política de cifrado
Sistemas no hardenizados en especial los SCADApara petróleo, hidroeléctricas y nucleares	Afectación en las operaciones	Hardenizar equipos basado en los benchmarks recomendados (NIST, DOD, CIS)	Plan de hardenización
Sistemas desactualizados expuestos a vulnerabilidades conocidas	Afectación en las operaciones	Actualizar componentes de sistema operativo, herramientas instaladasy de ser necesario	Incluir proceso de actualización continuaen las políticas
		componentes de hardware	
Ausencia de controles biométricos y mecanismos de monitoreo en las instalaciones internas	Accesos no autorizados	Instalar controles biométricos y mecanismos de monitoreo como cámaras	Políticas de control de acceso
Ausencia de una política de contraseñasadecuada	Accesos no autorizados	Asignar contraseñas robustas a cada usuario	Política de gestión de contraseñas
Perfiles y accesos mal definidos o ausencia de los mismos	Accesos no autorizados	Definir roles y perfiles según el cargo y las necesidades	Política de controles de acceso, definición de roles y perfiles

1 Los riesgos identificados

Ante las labores que son realizadas en la Lotería del Tolima y de acuerdo con las vulnerabilidades quese han detectado se encuentra que la mayor prioridad en donde se debe enfocar la mitigación de los riegos detectados son lo siguiente:

- Debilidad en las contraseñas: La debilidad en las contraseñas es una fuente de vulnerabilidad debido a que los usuarios suelen usar contraseñas de números continuos o nombres para evitar olvidarlas. La solución para esto es la implementación de una política en los diferentes sistemas y aplicaciones, en donde sea requerido el uso de una contraseña alfanumérica y no inferior a 8 caracteres, adicionalmente no permitir el uso de nombres propios.
- Conexiones entre diferentes sedes no cuentan con el debido cifrado de información: Debido a que no existe un cifrado en la transmisión de datos entre lamisma empresa y diferentes sedes asociadas a la organización, los datos que sean transmitidos pueden ser interceptados y vulnerar la información como modificándolao hurtándola para venderla. Existen diferentes mecanismos para proteger la información en el cifrado, lo principal es instalar en los diferentes sistemas y en la red, los certificados de navegación para contar con protocolos SSL, otro de los mecanismos que son útiles es hacer uso de una VPN para garantizar las conexiones de los usuarios a la red, dicha VPN será accesible mediante el uso de un token que vaya acompañado de una contraseña adicional a la de red para mejorar la seguridad.
- Los usuarios de la organización realizan malas prácticas de seguridad***:*** Es muy común por parte de los usuarios dejar sesiones abiertas cuando no se encuentran presentes en sus puestos de trabajos, o que algunos presten sus usuarios de red o de aplicaciones, e incluso dejar aplicaciones abiertas cuando no requieren utilizarlas, esto claramente son malas prácticas para la seguridad lo que genera fallas en la información. La solución para esto es definir políticas claras en las sanciones al empleado o contratista frente al préstamo de usuarios de cualquier tipo, definir políticas posteriores a la política general en las que se aclare que cualquier ausenciadel puesto de trabajo se requiera dejar bloqueada la estación de trabajo, adicionalmente establecer una regla en los instructivos específicos en la cual las sesiones se cierren solas luego de una inactividad de más de 10 minutos y para las estaciones de trabajo

cerrarse luego 2 minutos de inactividad

2 **Plan detallado de acción indicando las tareas que se llevarán a cabo en el corto, medio ylargo plazo.**

Actividades para los controles de riesgo

Control aplicado ISO/IEC 27002 13.1.1 Controles de red: Se requiere una administración y control en las redes que tenga la organización para así proteger la información que se tenga en los sistemas y las aplicaciones.

Control aplicado ISO/IEC 13.1.2 Mecanismos de seguridad asociados a servicios en red: Al realizar la implementación de acuerdos de los servicios (SLA) se da la garantía para que tantoel tráfico interno como el externo de la red cumpla con las políticas que defina la compañía.

Control aplicado ISO/IEC 13.1.3 Segregación de redes: Es necesario que se segmente la red de acuerdo con los diferentes servicios que tenga la organización para que al momento de ser utilizadapor los usuarios y diferentes sistemas de información exista un buen control de la red.

Control aplicado ISO/IEC 13.2.1 Políticas y procedimientos de intercambio de información***:*** Es necesario definir políticas controles y procedimientos formales de acuerdo a la infraestructura de la Lotería para que haya una transferencia segura y así proteger la información queviaja mediante el uso de los diferentes tipos de comunicación presentes dentro de la organización.

Control aplicado ISO/IEC 13.2.2 Acuerdos de intercambio: Para que exista un intercambio seguro en la información de la organización tanto interna como externamente debe de existir un esquema de llaves pre-compartidas PSK para garantizar una buena seguridad.

Control aplicado ISO/IEC 13.2.3 Mensajería electrónica***:*** Es necesario utilizar los correctos mecanismos para proteger correctamente la información que sea transmitida en los mensajes electrónicos, esto mediante una red encriptada.

Control aplicado ISO/IEC 13.2.4 Acuerdos de confidencialidad y secreto: Con el fin de tener control en los acuerdos de confidencialidad y no divulgación es necesario que los requisitos de estos se revisen y documenten de manera regular, para la protección de información.

(Gupta,http://iso27000.es, 2019)

Actividades recomendadas para los controles de riesgo

Control aplicado ISO/IEC 14.1.3 Protección de las transacciones por redes telemáticas: Toda la información en las transacciones de los servicios de aplicación deberá de serprotegida con el fin de que haya pérdida de información en la transmisión, se dé un enrutamiento incorrecto en los mensajes.

Control aplicado ISO/IEC 14.2.1 Política de desarrollo seguro de software***:*** Es necesario establecer y aplicar las correctas reglas para el desarrollo de software, así como la aplicación de sistemas dentro de la organización.

Control aplicado ISO/IEC 14.2.4 Restricciones a los cambios en los paquetes de software***:*** Con el fin de evitar fallos en software de terceros y la red, se debe de evitar realizar modificaciones al mismo en su arquitectura, los cambios deberán de estar limitados solo a lo necesario,además todo cambio que sea aplicado deberá de ser controlado estrictamente.

Control aplicado ISO/IEC 14.2.5 Uso de principios de ingeniería en protección de sistemas: Al momento de realizar cualquier implementación en los sistemas de información, es necesario que se establezcan, documenten, se mantengan y aplican los correctos principios de seguridad en cuanto a ingeniería de sistemas. (Gupta, http://iso27000.es, 2019)

Control aplicado ISO/IEC 15.1.1 Política de seguridad de la información para suministradores: Con el fin de minimizar los riesgos que están asociados al acceso a información parparte de proveedores y terceros, se deben documentar correctamente los requisitos de seguridad de la información que sean requeridos por los activos con los cuales cuenta la organización.

Control aplicado ISO/IEC 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores***:*** La prestación de servicios por parte de proveedores externos debe ser monitoreada,revisada y auditada contra los contratos y acuerdos según sus funciones ya sea por producto o por prestación de servicios. Los cambios de servicio deben ser controlados.

Control aplicado ISO/IEC 15.2.1 Supervisión y revisión de los servicios prestados por terceros***:*** Cada requerimiento contratado por terceros debe estar plenamente documentado para así garantizar que las normas de seguridad se cumplan. (Gupta, http://www.iso27000.es, 2019)

Actividades para los controles de riesgo

Control aplicado ISO/IEC 16.1.1 Responsabilidades y procedimientos***:*** Con el fin de garantizar que haya una respuesta rápida ante cualquier incidente de seguridad de la información, se deben definir y establecer tanto responsabilidades como los procedimientos para la gestión de los incidentes.

Control aplicado ISO/IEC 16.1.2 Notificación de los eventos de seguridad de la información***:*** Todo evento respecto a la seguridad de la información debe de ser notificado cuantoantes haciendo uso de los canales de administración definidos para tal fin.

Control aplicado ISO/IEC 16.1.3 Notificación de puntos débiles de la seguridad: Toda falla o debilidad sospechosa respecto a la seguridad de la información que sea detectada en los sistemaso los servicios, deberá de notificada a aquellos que hacen uso de los sistemas o los servicios de la organización.

Control aplicado ISO/IEC 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones***:*** Realizar la evaluación de los eventos que involucren laseguridad de la información y posteriormente realizar la clasificación como incidentes.

Control aplicado ISO/IEC 16.1.5 Respuesta a los incidentes de seguridad***:*** De acuerdo con los procedimientos que están debidamente documentados, se requiere que haya una respuesta adecuada ante los incidentes de seguridad de la información que se presenten.

Control aplicado ISO/IEC 16.1.6 Aprendizaje de los incidentes de seguridad de la información: Con el conocimiento que se ha adquirido respecto a eventos e incidentes pasados y como fueron solucionados se deberán tomar medidas para reducir la probabilidad de que se presentennuevas fallas a futuro. (Gupta, http://iso27000.es, 2019)

Control aplicado ISO/IEC 17.1.1 Planificación de la continuidad de la seguridad de la información: La organización debe de establecer los requisitos necesarios en cuanto a la seguridad deinformación, con el fin de que haya una continuidad en la gestión de seguridad de la información, en caso de presentarse crisis o desastre.

Control aplicado ISO/IEC 17.1.2 Implementación de la continuidad de la seguridad de la información***:*** La organización debe de establecer, documentar e implementar procedimientos y controles con el fin de que se garantice y se asegure un nivel de continuidad para la seguridad de la información en caso de que se presente una situación adversa.

Control aplicado ISO/IEC 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información: Con el fin de garantizar que la continuidad de la seguridadde la información en caso de que se presenten situaciones adversas, la organización debe de realizar verificaciones periódicamente en los controles establecidos de la seguridad de la información. (Gupta,http://iso27000.es, 2019)

Con el fin de cumplir con el triángulo de la seguridad, el objetivo es buscar que no se lleven a cabo ataques de hombre en medio (man-in-the-middle).

Objetivo (ISO 27002, Control 13.1 Gestión de la seguridad en las redes): Establecer mecanismos parael aseguramiento y protección de la información que la organización envía a través de las diferentes redes que tiene, para así proteger tanto aplicativos como repositorios.

Para poder llevar a cabo lo antes mencionado con el "control de red" el cual nos indica que todas las redes deben de ser gestionadas y controladas esto con el fin de que se protejan todos los sistemas, aplicaciones y la información que se tenga.

Este control cuenta con una guía para poder implementarlo la cual consta de los siguientes puntos.

(ISO/IEC 27002 punto 13.1.1):

- Definir las responsabilidades sobre los correctos procedimientos al momento de realizar la gestión de los equipos que están asociados a la red, para esto se asignarán las

responsabilidadesa personal informáticos del departamento técnico.

- El personal encargado de analizar los sistemas estará enfocado en gestionar y garantizar queoperen con normalidad y que estos se encuentren con sus respectivas actualizaciones.
- Debe de haber garantías para que la información con la cual cuenta la organización cuente con su respectiva confidencialidad, integridad y disponibilidad en los diferentes sistemas y la red dela organización.
- Seguimiento de la bitácora que se tiene los incidentes y eventos con el fin de que se detecten lasfallas de seguridad para luego solucionarlas.
- Cronograma de actividades definido para las actividades correctivas y de implementación, asegurando que todas las indicaciones y controles sean aplicados correctamente en la red corporativa.
- Definir controles en los cuales se verifiquen que los equipos realicen la autenticación de formaefectiva hacia el dominio.
- Los diferentes equipos de red deben de contar con restricciones de navegación en la red, segúnsu perfil y sus funciones.

Como equipo consultor de la empresa se llevarían a cabo la validación de los puntos más urgentescomo los son:

- Controlar la seguridad de la red.

- Validar políticas.

- Validar los procedimientos para el intercambio de información.

Estos puntos son relativamente fáciles de llevar a cabo y cumplir.

Otro de las revisiones que se llevarían a cabo seria la revisión independiente respecto a la seguridad dela información, para lo cual se cumpliría con los respectivos requisitos legales y contractuales.

Como validaciones finales y adicionales se llevarían a cabo revisiones en cuanto a la parte técnica y validaciones de la seguridad de la información.

DESARROLLO DE LOS EXCENARIOS SEGÚN EL PLAN

Definición Del Alcance

Con el desarrollo del presente análisis, se buscar realizar mejoras al proceso de Seguridad Digitalde la Lotería del Tolima, las cuales estarán enfocadas al área de infraestructura o sistemas de información, tomando en cuenta las amenazas de los servicios que son prestados en esta área.

Identificación De Los Activos, Amenazas Y Vulnerabilidades

En las actividades anteriores se identificaron de los Activos de Información, y las posibles Amenazas y Vulnerabilidades que pueden presentarse de la Lotería de Tolima, las cuales se detallan a continuación en la tabla No. 1

Tabla No.1. Activos de Información, Amenazas y Vulnerabilidades de la Lotería del Tolima

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
Servidor de sistemaLotería	[E15] Alteración accidentalde la información	Alteración de la información de impresión
	[A11] Acceso no autorizado	No se han cambiado las credenciales de acceso
	[A6] Abuso de privilegiosde acceso	Modificación parámetros de impresión.

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
	[E2] Errores deladministrador	Configuración usuarios por defecto
	[E23] Errores de mantenimiento / actualización de equipos(hardware)	Falla por falta de mantenimiento preventivo
	[A11] Acceso no autorizado	Acceso a la configuracióndel equipo
Impresoras	[E2] Errores deladministrador	Falla por falta de mantenimiento preventivo
	[E23] Errores de mantenimiento / actualización de equipos(hardware)	Falla por falta de mantenimiento preventivo
	[A11] Acceso no autorizado	Acceso a la configuración del equipo
Servidor de archivos FTP	[A15] Modificacióndeliberada de la información	Acceso a la configuracióndel equipo
	[A11] Acceso no autorizado	credenciales de acceso generales
	[A6] Abuso de privilegiosde acceso	Modificación parámetros de configuración.
Página web	[A5] Suplantación de la identidad del usuario	No se cambia frecuentemente las clavesde acceso
	[A6] Abuso de privilegiosde acceso	Modificación deinformación
	[A15] Modificacióndeliberada de la información	Alteración de los datos
	[A11] Acceso no autorizado	No se cambia frecuentemente las clavesde acceso

Servidor de registro ycontrol académico	[A15] Modificacióndeliberada de la información	Alteración de lainformación.
	[A11] Acceso no autorizado	credenciales de acceso generales
	[A6] Abuso de privilegiosde acceso	Modificación parámetros de configuración.

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
	[A18] Destrucción de información	Borrado de información almacenada
Plataforma registro y seguimiento de juegos	[A5] Suplantación de la identidad del usuario	No se cambia frecuentemente las clavesde acceso
	[A6] Abuso de privilegios de acceso	Modificación de información
	[A15] Modificacióndeliberada de la información	Alteración de los datos
	[A11] Acceso no autorizado	No se cambia frecuentemente las clavesde acceso
Servidor DHCP Ubiquiti-Servidore Firewall	[A15] Modificacióndeliberada de la información	Alteración de la información en el FTP
	[A11] Acceso no autorizado	Credenciales de acceso generales
	[A18] Destrucción de información	Borrado de información almacenada
Equipos de cómputo para gestión de Sistema de contable	[A6] Abuso de privilegiosde acceso	Creación de usuarios con privilegios para obtener información
	[A11] Acceso no autorizado	No se cambia frecuentemente las clavesde acceso
	[A25] Robo	poco control de acceso

Plan Cloud Plus	[A5] Suplantación de la identidad del usuario	No se cambia frecuentemente las clavesde acceso
	[A6] Abuso de privilegiosde acceso	Modificación deinformación
	[A15] Modificacióndeliberada de la información	Alteración de los datos
	[A11] Acceso no autorizado	No se cambia frecuentemente las clavesde acceso
Cortafuegos Pfsense	[E2] Errores deladministrador	No se encuentran configuradas las reglas

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
	[A11] Acceso no autorizado	Acceso total a la red
Equipos de climatización	[I7] Condiciones inadecuadas de temperaturao humedad	Daño por excesivo calor en los servidores
Equipos de cómputo trabajadores	[A11] Acceso no autorizado	No se cambia frecuentemente las claves de acceso
Sistema OperativoWindows 10 PRO	[E2] Errores deladministrador	Configuración de las actualizaciones
	[E18] Destrucción de información	Perdida de información
	[A8] Difusión de software dañino	No cuenta con actualización de los parches de seguridad de Windows
Puntos de acceso alámbricos (hub) Ubiquiti	[E2] Errores deladministrador	No hay segmentación de la red LAN
Switches Aruba 24puertos	[E2] Errores deladministrador	Los usuarios y contraseñas son las que vienen pordefecto
Teléfonos IP	[A12] Análisis de tráfico	Análisis de las llamadas

	[A9] [Re-]encaminamientode mensajes	Interceptación de llamadas
Puntos de acceso Campus	[E2] Errores deladministrador	No hay segmentación de la red WLAN
	[A12] Análisis de tráfico	Análisis en el tráfico
	[A9] [Re-]encaminamientode mensajes	Direccionamiento de conexión a base de datos
	[A6] Abuso de privilegios de acceso	Usuarios y contraseñas de acceso por defecto
Credenciales	[A11] Acceso no autorizado	Cambio no frecuente de claves
	[A6] Abuso de privilegiosde acceso	No hay segmentación de privilegios
	[A5] Suplantación de la identidad del usuario	Cambio no frecuente de claves
Correo Electrónico	[E19] Fugas de información	No hay procesos de capacitación
	[E1] Errores de los usuarios	No se cambia las contraseñas frecuentemente

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
Campus Virtual	[A5] Suplantación de la identidad del usuario	No se cambia frecuentemente las clavesde acceso
	[A6] Abuso de privilegiosde acceso	Modificación deinformación
	[A15] Modificación deliberada de lainformación	Alteración de los datos
	[A11] Acceso no autorizado	No se cambia frecuentemente las clavesde acceso
Bases de datos	[A5] Suplantación de la identidad del usuario	No se cambia frecuentemente las clavesde acceso

	[A6] Abuso de privilegiosde acceso	Modificación deinformación
	[A15] Modificacióndeliberada de la información	Alteración de los datos
	[A11] Acceso no autorizado	No se cambia frecuentemente las claves de acceso
Edificio de la institución	[N*] Desastres naturales	No hay plan de continuiddade negocio
	[I*] Desastres industriales	No hay plan de mitigaciónde riesgos industriales
	[A11] Acceso no autorizado	No hay sistema de acceso biométrico ni monitoreo
Usuarios internos	[A28] Indisponibilidad del personal	No se cuenta con un sistema de teletrabajo
	[A30] Ingeniería social (picaresca)	No hay un plan de capacitación
	[E19] Fugas de información	No se han creado criterios de confidencialidad
Administradores desistemas	[A28] Indisponibilidad del personal	No se cuenta con un sistema de teletrabajo
	[A30] Ingeniería social (picaresca)	No hay un plan de capacitación
	[E19] Fugas de información	No se han creado criteriosde confidencialidad

ACTIVOS DE INFORMACIÓN	AMENAZAS	VULNERABILIDADES
Proveedores	[A28] Indisponibilidad del personal	No se cuenta con un sistema de teletrabajo
	[A30] Ingeniería social (picaresca)	No hay un plan de capacitación
	[E19] Fugas de información	No se han creado criteriosde confidencialidad

Agente de Antivirus	[E2] Errores deladministrador	No se lleva registro de actualizaciones
	[A8] Difusión de software dañino	No se tiene registro delestado del antivirus
Servidor de correos Electrónico en nube	[A11] Acceso no autorizado	No se han cambiado las credenciales de acceso
	[A6] Abuso de privilegios de acceso	Modificación de configuraciones
	[A18] Destrucción de información	Borrado de información almacenada
	[A15] Modificacióndeliberada de la información	Alteración de lainformación
Servidor PBX -Telefonia	[A15] Modificacióndeliberada de la información	Alteración de lainformación
	[A11] Acceso no autorizado	Credenciales de acceso generales
	[A6] Abuso de privilegios de acceso	Modificación de parámetros de configuración
	[A18] Destrucción de información	Borrado de información almacenada

Mapa De Calor De La Matriz De Riesgos Informáticos Lotería Del Tolima

El mapa de calor representa gráficamente como están ubicados los riesgos en un cuadrante, dependiendo de la probabilidad de que determinado riesgo pueda ocurrir y el impacto cuantitativo o cualitativo que se produce en caso de que se materialice el riesgo; Los riesgos identificados deben ser evaluados estimando con qué frecuencia podrían aparecer y cuál es el impacto estimado a nivel financiero, de buen nombre y estratégico. Para la empresa de análisis una vez revisados la probabilidady el impacto de los riesgos dio como resultado el siguiente grafico de mapa de calor:

Mapa de Calor de riesgos Informáticos

R: Riesgo

APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA			,R48	,R49, R43, R42, R33, R32, R31, R29, R26, R24, R21, R18, R16, R13, R10, R6, R4, R1	,R52, R51, R50, R47, R46, R45, R44, R40, R39, R38, R37, R36, R35, R34, R28, R27, R25, R23, R22, R20, R19, R17, R15, R14, R12, R11, R9, R7, R3, R2
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Plan de Tratamiento de Riesgos

En la siguiente tabla se presenta el Plan de Tratamiento dado a los riesgos, de acuerdo Controlesdel Anexo A del estándar ISO/IEC 27001:2022, el cual fue elaborado conjuntamente por los ingenierosde la Lotería del Tolima.

Plan de Tratamiento dado a los riesgos, de acuerdo Controles del Anexo A del estándar ISO/IEC27001:2022

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
Servidor de Impresión	[E15] Alteración accidental de la información	A8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Transferencia de medios físicos	Se debe documentaren las políticas de seguridad los controles ya implementados paraasegurar correctamente las copias de seguridad de los distintos dispositivos de almacenamiento, además de las configuraciones de los dispositivos y cifrado de la información
	[A11] Acceso no autorizado	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sistema de gestión de contraseñas	Se debe cambiar lascontraseñas y usuarios que están por defectos en los sistemas de almacenamiento y configuración, además de documentar en las políticas de seguridad la complejidad de dichas contraseñas y el cambio periódico.

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
	[A6] Abuso de privilegiosde acceso	A9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado	Gestión de derechos de acceso privilegiado	Restringir permisos de los distintos usuarios, teniendo en cuenta su perfil y con previa autorización al acceso a la información o sistemas de almacenamiento de documentos o información de suma importancia.
Impresora HP LaserJet Enterprise serie 600	[E2] Errores del administrador	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sistema de gestión de contraseñas	Se debe realizar el cambio de todos los usuarios y contraseñas de los sistemas que sean predeterminados, para evitar un ataque de elevación de privilegios.
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado.	Gestión de derechos de acceso privilegiado	Se debe realizar seguimiento periódico al mantenimiento que se realiza a los equipos, además de llevar una hoja de vida de cada dispositivo.

	[A11] Acceso no autorizado	A9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado	Gestión de derechos de acceso privilegiado	Restringir los diferentes permisos de los usuarios, desactivar usuarios que no se van a utilizar y que no son necesarios para la configuración de las impresoras.
Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
Impresora SMART MultiXpress M4370LX	[E2] Errores del administrador	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sistema de gestión de contraseñas	Se debe realizar el cambio de todos los usuarios y contraseñas de los sistemas que sean predeterminados, para evitar un ataque de elevación de privilegios.
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Transferencia de medios físicos	Se debe documentaren las políticas de seguridad los controles ya implementados paraasegurar correctamente las copias de seguridad de los distintos dispositivos de almacenamiento, además de las configuraciones de los dispositivos y cifrado de la información

	[A11] Acceso no autorizado	A9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado	Gestión de derechos de acceso privilegiado	Restringir los diferentes permisos de los usuarios, desactivar usuarios que no se van a utilizar y que no son necesarios parala configuración de las impresoras.
Servidor de archivos FTP	[A15] Modificación deliberada de la información	A8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Transferencia de medios físicos	Se debe documentaren las políticas de seguridad los controles ya implementados paraasegurar correctamente las copias de seguridad de los distintos

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
					dispositivos de almacenamiento, además de las configuraciones de los dispositivos y cifrado de la información
	[A11] Acceso no autorizado	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Sistema de gestión de contraseñas	Se debe realizar el cambio de todos los usuarios y contraseñas de los sistemas que sean predeterminados, para evitar un ataque de elevación de privilegios.

	[A6] Abuso de privilegiosde acceso	A9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado	Gestión de derechos de acceso privilegiado	Restringir los diferentes permisos de los usuarios, desactivar usuarios que no se van a utilizar y que no son necesarios parala configuración y manipulación del servidor.
	[A18] Destrucciónde información	A9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	Política de control de acceso	Se debe documentaren las políticas de seguridad los controles ya implementados paraasegurar correctamente las copias de seguridad de los distintos dispositivos de almacenamiento, además de las configuraciones de los dispositivos y cifrado de la información

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
Página web	[A5] Suplantación de la identidad del usuario	A9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Política de control de acceso	Se debe documentaren las políticas de seguridad los controles ya implementados parael acceso de la información, con el fin de que los usuarios no sean suplantados
	[A6] Abuso de privilegiosde acceso	A9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Política de control de acceso	Se debe documentaren las políticas de seguridad los controles ya implementados parael acceso de la información, con el fin de asegurar que la información de la página web no sea alterada
	[A15] Modificación deliberada de la información	A9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de accesoa todo tipo de usuarios para todos los sistemas y servicios.	Suministro de acceso de usuarios	Se debe establecer una política sobre el uso de la información de la página web del Centro

	[A11] Acceso no autorizado	A9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de	Política de control de acceso	Se debe documentaren las políticas de seguridad los controles ya implementados la periodicidad en el cambio de contraseñas y

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamiento MITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
			seguridad de la información		claves para evitar riesgos
Servidor de registro y control académico	[A15] Modificación deliberada de la información	A.10.1.1	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Política sobre el uso de controles criptográficos	Se debe establecer una política sobre el uso de controles criptográficos para el acceso a la información sensible del centro, además una política de copias de respaldo

	[A11] Acceso no autorizado	A6.1.1	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	Roles y responsabilidades para la seguridad de información	Se deben establecerroles y responsabilidades frente al manejo de la información del Centro
	[A6] Abuso de privilegiosde acceso	A6.1.2	Los deberes y áreasde responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Separación de deberes	Reglamentación de sanciones ante casos de abuso de confianza y negligencia.
	[A18] Destrucciónde información	A18.1.3	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los	Protección de registros	Se implantará controles que protegen de la destrucción de la información, por mecanismos legalesy contractuales que aseguren el compromiso de los empleados.

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
			requisitos legislativos, de reglamentación, contractuales y de negocio.		
Plataforma registro y control académico	[A5] Suplantación de la identidad del usuario	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar lacalidad de las contraseñas	Sistema de gestión de contraseñas	Establecimiento de protocolos de cierre de las sesiones en inactividad y con seguridad de mínimo 2 pasos para cambio de contraseñas, así como de la encriptación de las mismas
	[A6] Abuso de privilegiosde acceso	A6.1.2	Los deberes y áreasde responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	Separación de deberes	Reglamentación de sanciones ante casos de abuso de confianza y negligencia.

	[A15] Modificación deliberada de la información	A9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso	Restricción de acceso a la información.	La documentación de los procesos parael establecimiento de privilegios en los accesos al sistema debe estar reglamentados y con controles que permitan la revisión para auditar.
	[A11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de	Gestión de derechos de	Se debe restringir y controlar la asignación y uso de

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
			derechos de accesoprivilegiado.	acceso privilegiado	derechos de acceso privilegiado
ServidorDHCP	[A15] Modificación deliberada de la información	A12.3.1	Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copiasde respaldo aceptada.	Respaldo de la información	Implementar reglamentos de información de eventualidades para restauración de las copias de respaldo existentes, y correcciones con el respectivo registro de cambio.

	[A11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
	[A18] Destrucciónde información	A18.1.3	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Protección de registros	Se implantará controles que protegen de la destrucción de la información, por mecanismos legalesy contractuales que aseguren el compromiso de los empleados.

Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
Equipos de cómputo para gestiónde Sistema de contable	[A6] Abuso de privilegiosde acceso	A9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado.	Gestión de derechos de acceso privilegiado	Se debe reglamentar el uso y derechos para la utilización de equipos que evite el ingreso de usuarios no autorizados o preparados. Se debe establecer políticas de ingreso de información que proteger la información evitando que se pueda alterar o ingresar de informaciónerrónea.

	[A11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de accesoprivilegiado.	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
	[A25] Robo	A11.1.1	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	Perímetro de seguridad física	Ampliar la cobertura del sistema existente ocontratar a una empresa que cumpla con esta función.
Plan Cloud Plus	[A5] Suplantación de la identidad del usuario	A9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso	Restricción de acceso a la Información	Establecer políticas de acceso a la información y restringir acceso a usuarios no autorizados.
Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
	[A6] Abuso de privilegiosde acceso	A9.1.1	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Política de control de acceso	La documentación de los procesos parael establecimiento de privilegios en los accesos al sistema debe estar reglamentados y con controles que permitan la revisión para auditar.

	[A15] Modificación deliberada de la información	A12.4.2	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Protección de la información de registro	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallasy eventos de seguridad de la información.
	[A11] Acceso no autorizado	A9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar lacalidad de las contraseñas	Sistema de gestión de contraseñas	Establecimiento de protocolos de cierre de las sesiones en inactividad y con seguridad de mínimo 2 pasos para cambio de contraseñas, así como de la encriptación de las mismas.
Cortafuegos Cisco ASA 5505	[E2] Errores del administrador	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad	Gestión de Cambios	Se deben controlar los cambios en la organización, en los procesos de negocio , en las estaciones yen los sistemas de procesamiento de información que afectan la seguridad de la organización
Nombre del activo de información	Amenazas	Plan de tratamiento			
		Control a aplicar para el tratamientoMITIGAR, norma ISO 27001			Descripción de la aplicación del control
		No.	Control	Objetivos de Control	
			de la información		

	[A11] Acceso no autorizado	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
equipos de climatización	[I7] Condiciones inadecuadas de temperatura o humedad	A11.1.4	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Protección contra amenazas externas y ambientales.	implementación de mejoras que permitan satisfacer las necesidades ambientales requeridas.

CONCLUSIONES

- Se determinaron buenas prácticas de servicios TI y gestión de seguridad con el fin degenerar una mejor gestión y determinar un buen desempeño dentro de los SGSI.
- Se dio a conocer los objetivos y recursos necesarios para la implantación de un SGSI,así como la definición de roles y de planes de acción y definir controles para la empresa.
- El trabajo nos ha permitido comprender con énfasis el estándar ISO 27001 mediante la aplicaciónde procedimientos y controles que permita asegurar la información; para ello es indispensable realizar el análisis de la empresa y determinar el costo beneficio de la solución.
- La importancia no solo de crear el SGSI, sino también de su mantenimiento y mejor.

NIDIA VICTORIA CASTILLO GONZALES
Gerente

Elaboro : Ever Fabian Rojas Rubio_____Técnico de Sistemas

ev.	Fecha	Elaboro	Reviso / Aprobó	Observaciones y/o Ajustes
0	7/9/2023	Técnico en sistemas	Comité de calidad	1. Creación Del documento