LOTERÍA DEL TOLIMA

APUÉSTELE A SUS SUEÑOS

SE-CER804982

PLAN DE TRATAMIENTO DE RIESGOS LOTERIA DEL TOLIMA - 2024

1. 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.

2. TÉRMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo 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 criteriosdel 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 detiempo 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.

3. IDENTIFICAR BREVEMENTE LOS PRINCIPALES RIESGOS ASOCIADOS

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.

3.1. 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 deaplicaciones, 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 ausencia del 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.

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 asígarantizar que las normas de seguridad se cumplan. (Gupta, http://www.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).

3.2. RIESGOS TECNOLÓGICOS LOTERIA DEL TOLIMA

DESCRIPCIÓN DEL RIESGO	CAUSAS (FACTORES INTERNOS EXTERNOS)	CONSECUENCIAS (EFECTOS)	NIVEL	CONTROL
Falla en el proceso de devolución de la billetera no vendida, en el sistema de información	* Fallas en el sistema de Información * Fallas en la página web de la entidad * Ausencia de soporte del sistema de Información	* Imposibilidad para validar los archivos de devolución en el sistema de información * Imposibilidad para generar los informes	EXTREMO	*Soporte 24/7 por parte del proveedor del sistema de información * Soporte 24/7 del proveedor del

DESCRIPCIÓN DEL RIESGO	CAUSAS (FACTORES INTERNOS EXTERNOS)	CONSECUENCIAS (EFECTOS)	NIVEL	CONTROL
	* Ausencia del fluido Eléctrico * Fallas en el servicio de Internet	tipo 204-Billetería Vendida y 203-Resultados del Sorteo * Incumplimiento en los tiempos establecidos para el envío de la información a la Supersalud * Investigaciones y/o sanciones por parte del ente de control		Hosting * Planta Eléctrica del edificio * UPS ubicada en el cuarto de equipos de la lotería * utilización de líneas celulares institucionales con datos ilimitados * Copia de seguridad de la base de datos del sistema de información * Planta auxiliar ubicada en las instalaciones de la lotería

DESCRIPCIÓN DEL RIESGO	CAUSAS (FACTORES INTERNOS EXTERNOS)	CONSECUENCIAS (EFECTOS)	NIVEL	CONTROL
Inconsistencias y/o incumplimiento en el envío de los informes de la circular única	* Fallas en el sistema de información que impida generar los informes * Ausencia del servicio de Internet dedicado * No renovación de la firma digital * Problemas en la plataforma de la Supersalud que impidan el envío de la información a tiempo *Mala parametrización	* Investigaciones y/o Sanciones económicas por parte del ente de control	EXTREMO	* Soporte 24/7 por parte del ingeniero de * utilización de líneas celulares institucionales con datos ilimitados * R-060 Lista de Chequeo * Correos electrónicos definidos por la Supersalud para el envío de la

	de los informes en el sistema de información, que generen información errónea			información en caso de fallas * Compra de la firma digital con un mes de anticipación * Validador de archivos habilitado por la Supersalud

DESCRIPCIÓN DEL RIESGO	CAUSAS (FACTORES INTERNOS EXTERNOS)	CONSECUENCIAS (EFECTOS)	NIVEL	CONTROL
Perdida de información Relevante para la entidad	* No realización de BackUp en las estaciones de trabajo * No realización de BackUp del sistema de información en los discos duros externos * Daños en los archivos por causa de un virus	Perdida de información de vital importancia para le entidad	EXTREMO	* R-008 Generación de BackUp * Copia automática en los discos duros externos * Instalación de Antivirus en cada uno de las estaciones de trabajo * Copia en la Nube los días de sorteo

3.3. TRATAMIENTO DE LOS RIESGOS TECNOLOGICOS

Los riesgos tecnológicos identificados en la Lotería del Tolima presentan un riesgo de nivel extremo, sin embargo, se tienen establecidos los respectivos controles, los cuales permiten a la entidad disminuir la probabilidad de que dichos riesgos se materialicen.

La entidad tiene implementados controles para evitar la pérdida de la información de vital importancia, es por ello que se tiene establecida una infraestructura de alojamiento en la nube, lo cual permite realizar copia permanente de los datos consignados en el sistema de información; asimismo, se realizan copias de seguridad en puestos de trabajo en unidades de almacenamiento externo y cada equipo cuenta con un antivirus que bloquea cualquier tipo de amenaza.

3.4. REPORTE DE NOVEDADES

La Lotería del Tolima cuenta con un sistema de información comercial, el cual integra todas las áreas de la entidad, es por ello que, cuando se genera algún tipo de alteración en la información se debe realizar el siguiente procedimiento:

- A través de correo electrónico, se lleva a cabo la solicitud a la oficina de sistemas o directamente al ingeniero de soporte del sistema de información.
- El sistema de información tiene implementado un módulo de auditoría, el cual permite conocer el usuario que realizó ajuste o modificación a un registro.
- Una vez se conocen las causas de la modificación, se envía el respectivo reporte a la oficina solicitante.

4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

Elaborar el plan de tratamiento de riesgos de Seguridad y privacidad de la Información de la lotería del Tolima E.I.C.E., que permita definir y aplicar los controles necesarios que mitiguen la materialización del riesgo dentro de la entidad.

4.1. OBJETIVOS ESPECIFICOS

- Identificar los riesgos asociados al tratamiento de la información en la Lotería del Tolima.
- Calcular el nivel de riesgo al que está expuesta la información dentro de la entidad.
- Definir el plan de tratamiento de riesgos que se va a llevar a cabo en la entidad.
- Realizar seguimiento y control al plan diseñado para el tratamiento de los riesgos.
- Promover el uso de mejores prácticas de seguridad de la información, que impidan el acceso a la información por terceros no autorizados.

4.2. ETAPAS PARA LA GESTIÓN DE RIESGOS

Para la gestión del riesgo en la lotería del Tolima se establecen las siguientes etapas:

4.2.1. ETAPA DE IDENTIFICACIÓN

La lotería del Tolima realiza la identificación de sus riesgos con un enfoque basado en procesos, donde toma como fundamento el objetivo del mismo para la definición de los riesgos. La identificación del riesgo es responsabilidad de la primera línea de defensa, es decir del dueño del proceso, así mismo, en esta etapa se define el riesgo, sus causas, fuentes, procesos y activos de información asociados, así como el responsable de su gestión.

4.2.2. ETAPA DE MEDICIÓN

La entidad establece las métricas para la medición de la probabilidad e impacto de los riesgos identificados por el Líder de Proceso. En esta etapa se establecen el impacto legal, reputacional y operativo el cual incluye los aspectos asociados a la seguridad y privacidad de la información (disponibilidad, integridad y confidencialidad), los cuales se consideran relevantes para la continuidad y credibilidad de la entidad.

	IMPACTO				
PROBABILIDAD	INSIGNIFICANTE 1	MENOR 2	MODERADO 3	MAYOR 4	CATASTROFICO 5
E - RARO - 1	B	B	M	A	A
D - IMPROBABLE - 2	B	B	M	A	E
C - POSIBLE - 3	B	M	A	E	E
B - PROBABLE -4	M	A	A	E	E
A - CASI CERTEZA - 5	A	A	E	E	E

B	ZONA DE RIESGO BAJA
M	ZONA DE RIESGO MODERADA
A	ZONA DE RIESGO ALTA
E	ZONA DE RIESGO EXTREMO

4.2.3. ETAPA DE CONTROL

Esta etapa para la gestión de los riesgos operativos es responsabilidad del Líder del Proceso, ya que debe definir las acciones concretas a través de las cuales gestionará el riesgo y/o custodiará los activos a su cargo.

Los controles deben estar documentados preferiblemente dentro de los procedimientos con el objeto de contar con la trazabilidad necesaria de su aplicación, así como la exigibilidad de su uso por parte de los encargados de su ejecución.

4.2.4. ETAPA DE MONITOREO

La lotería del Tolima E.I.C.E cuenta con diversas herramientas de monitoreo de los riesgos, como primer filtro, se encuentra el Líder de Proceso, debe supervisar que los controles de su proceso se estén ejecutando a través de la definición de indicadores, revisiones aleatorias u otros mecanismos que considere pertinentes.

Así mismo, La auditoría interna se debe realizar periódicamente y cuyos resultados son insumo para que el Líder del Proceso fortalezca la gestión de los riesgos.

5. CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	MES											
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1. Etapa de Identificación		01-01 / 31-05										
2. Etapa de Medición						01-06 / 31-10						
3. Etapa de control						01-06 / 31-10						
4. Etapa de monitoreo											01-11	15-12

5. TÉRMINOS Y DEFINICIONES

- **RIESGO:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

- **RIESGO POSITIVO:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

- **SEGURIDAD DE LA INFORMACIÓN:** Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

- **INFORMACIÓN PUBLICA RESERVADA:** Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

- **INFORMACIÓN PÚBLICA CLASIFICADA:** Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

- **NO CLASIFICADA:** Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de

INFORMACIÓN PUBLICA RESERVADA.

- **CONFIDENCIALIDAD:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

- **INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **DISPONIBILIDAD:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

CONCLUSIONES

- Se determinaron buenas prácticas de servicios TI y gestión de seguridad con el fin de generar 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.

ALEXANDER CASTRO SALCEDO
Gerente

Elaboró: Ing. Leonardo Gutierrez Fajardo _____ Contratista
Revisó: Ing. Ever Fabian Rojas Rubio _____ Técnico de Sistemas
Revisó: Dra. Blanca Ena Barragán Toro _____ Secretaria General y Jurídica – Unidad Administrativa