LOTERÍA DEL TOLIMA
APUÉSTELE A SUS SUEÑOS

SE-CER804982

PLAN DE SEGURIDAD DE RECUPERACION DE DESASTRES

LOTERIA DEL TOLIMA

LOTERIA DEL TOLIMA

2023

Contenido

1. INTRODUCCION 4
2. OBJETIVO GENERAL 4
3. IMPORTANCIA DEL PLAN DE RECUPERACION DE DESASTRES: 4
4. ANALISIS DE RIESGO 5
5. GESTION DE RIESGOS 7
5.1 IMPORTANCIA DE LA GESTION DE RIESGOS..... 7
5.2. DEFINICION GESTION DEL RIESGO..... 8
5.3. IDENTIFICACION DEL RIESGO 8
5.4. SITUACION NO DESEADA..... 9
6. ORIGEN DEL PLAN DE GESTION 12
7. ANALISIS DE VULNERABILIDADES 12
7.1. DESCRIPCION DE VULNERABILIDADES 12

1. INTRODUCCION

El plan de seguridad de recuperación de desastres de la Lotería del Tolima, tuvo como propósito identificar los diferentes amenazas a las que se encuentran expuestas las compañías en la actualidad en este caso se utilizaron marcos de trabajo como Cobit y estándares o normas como ISO

24762 o la NISP SP 800-34 en las cuales nos basamos para la elaboración de un plan de recuperación de desastre adecuado para la compañía.

De igual forma se identificaron los activos de la compañía que se encontraban más vulnerables a posibles fallas que podrían interrumpir el normal funcionamiento de todos sus procesos. Estos análisis se llevaron a cabo mediante entrevistas al personal de tecnología y de apoyo de las demás aéreas los cuales arrojaron muchas deficiencias en la seguridad de la información, el presente documento es un formato inicial y preliminar del plan de seguridad de recuperación de desastres de la Lotería del Tolima.

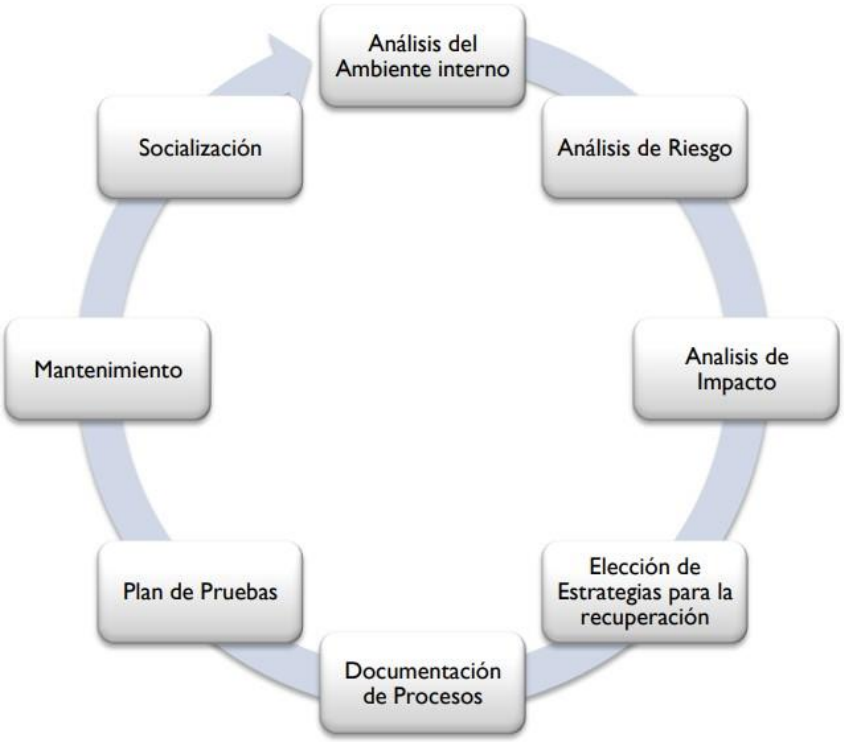
2. OBJETIVO GENERAL

Fomentar una política de seguridad para los funcionarios públicos de la Lotería del Tolima en San Luis Tolima es esencial para garantizar la integridad y el correcto funcionamiento. Esta política debe incluir protocolos claros de actuación, capacitación continua en temas de seguridad y un compromiso firme con la transparencia y la ética. La implementación de estas medidas es fundamental para proteger tanto a los funcionarios como a los ciudadanos a los que sirven.

3. IMPORTANCIA DEL PLAN DE RECUPERACION DE DESASTRES:

Los últimos acontecimientos mundiales, nos han hecho evaluar fuertemente que aquí en nuestro país son mínimas las previsiones que tomamos para salvaguardar las compañías. Sabemos que las empresas hoy en día son un ente vivo y en continuo cambio es por eso que debemos adoptar una postura de dinámica ante estos cambios. Para eso es importante que no solo cuenten con los documentos si no que se conviertan en una constante a lo largo de la vida de la compañía.

A continuación, representamos gráficamente cada uno de los pasos y/o actividades que se deben seguir para implementar de manera efectiva un plan de recuperación de desastres para la compañía.



4. ANALISIS DE RIESGO

Para este proyecto se realizará un análisis de cada una de las amenazas con sus respectivas vulnerabilidades que puedan materializarse en el ente territorial. —En la siguiente figura se muestra las diferentes amenazas que puede afrontar una compañía de acuerdo al factor que lo inicia ya sean humanas o por factores naturales y ambientales.

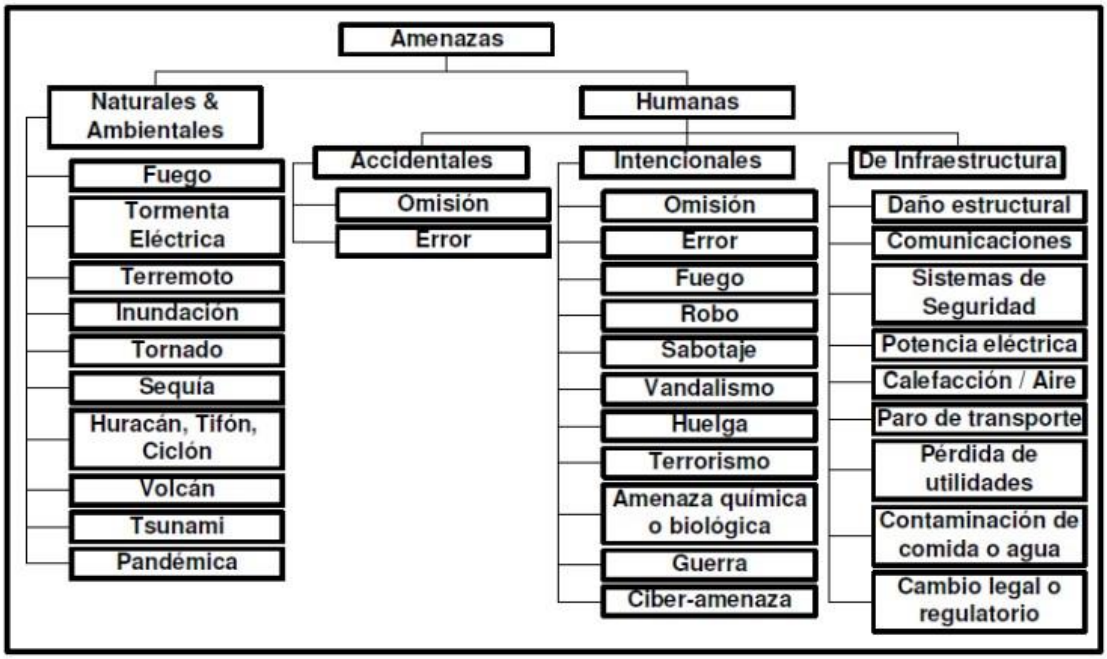
4.1 Riesgos de infraestructura on premise;

La infraestructura on-premise, aunque proporciona un alto grado de control y personalización en la Lotería del Tolima, ciertamente presenta desafíos únicos que la organización deben navegar con cuidado. La seguridad física es primordial, ya que el servidor está expuestos a riesgos tangibles como el robo o desastres naturales. Los costos de mantenimiento son también una consideración importante, con inversiones significativas en hardware, software y contratar a personal especializado. Además, la escalabilidad limitada puede restringir el crecimiento y la adaptabilidad, especialmente en comparación con las soluciones en la nube que ofrecen flexibilidad y escalabilidad casi instantáneas. Los problemas de rendimiento y disponibilidad pueden afectar la continuidad del negocio, mientras que el cumplimiento de las regulaciones y la seguridad de los datos requieren un enfoque riguroso y actualizado.

Por último, la flexibilidad limitada para modificar o actualizar la infraestructura puede resultar en una desventaja competitiva. Por lo tanto, es esencial que la Lotería del Tolima evalúe estos riesgos al considerar la infraestructura on-premise y busquen estrategias para mitigarlos, como la implementación de soluciones híbridas o la transición gradual a la nube.

4.2 Riesgos de servicio en la nube;

La adopción de la computación en la nube por parte de la Lotería del Tolima trae consigo una serie de riesgos de seguridad que deben ser cuidadosamente evaluados y gestionados. Es esencial que el personal de TI esté bien capacitado para manejar vulnerabilidades del sistema y configuraciones inadecuadas para proteger contra ataques. Además, la dependencia de proveedores de servicios en la nube requiere una consideración detallada sobre la privacidad, la confidencialidad y el cumplimiento normativo, asegurando que los datos y procesos estén seguros y en conformidad con las leyes pertinentes. Por último, es crucial tener planes de contingencia para la dependencia del proveedor y los riesgos de ataques cibernéticos, como los DDoS, para mantener la integridad y disponibilidad de los servicios.



5. GESTION DE RIESGOS

5.1 IMPORTANCIA DE LA GESTION DE RIESGOS

La importancia de la gestión de riesgos en el ámbito empresarial es crucial, especialmente en lo que respecta a la protección y custodia de la información. La Lotería del Tolima es un ejemplo de entidad que se alinea con las directrices nacionales para garantizar la transparencia y la seguridad digital, siguiendo la Ley 1712 de 2014 y el Decreto 1078 de 2015. Sin embargo, los desafíos persisten debido a factores externos como desastres naturales y riesgos inherentes a procesos inadecuados. El desconocimiento o incumplimiento de las normativas de seguridad puede resultar en pérdidas significativas. Por ello, es fundamental que todas las organizaciones implementen planes de gestión de riesgos robustos que aborden los riesgos a los sistemas de información y tecnologías de la información. El Directorio Activo es una herramienta que puede ofrecer soluciones en este aspecto, ayudando a mitigar los riesgos asociados con ataques al software empresarial y fortaleciendo la infraestructura de seguridad de la información.

5.2. DEFINICION GESTION DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización International de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización".

5.3. IDENTIFICACION DEL RIESGO

• Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

• Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

• Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

• Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

• Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

• Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la

Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

5.4. SITUACION NO DESEADA

• Hurto de información o de equipos informáticos.

• Hurto de información durante el cumplimiento de las funciones laborales, por intromisión

• Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.

• Alteración de claves y de información.

• Perdida de información.

• Baja Cobertura de internet.

• Daño de equipos y de información.

• Atrasos en la entrega de información.

6. ORIGEN DEL PLAN DE GESTION

debido a que la Lotería del Tolima no tenía un área de Informática y tecnología conformada y se evidencio que no existen procesos asignados a dicha área entre otras vulnerabilidades que se encontraron en el sistema actual, es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información. La situación actual del sistema de seguridad de la información. El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las entidades públicas en el país. Es por ello necesario que se cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma Lotería.

7. ANALISIS DE VULNERABILIDADES

7.1. DESCRIPCION DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Lotería del Tolima se encontraron otras amenazas e impactos como los siguientes:

• Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos puntos cableados evidentes en la lotería del Tolima según se va presentando la necesidad.

• Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardado.

- No cuenta con un firmware físico y administrable.
- No tiene un directorio activo para implementar reglar a los usuarios.
- No tiene un servidor Nas para el respaldo de los Backups.