Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Plan de Gestión de Riesgos de Seguridad de la Información física y lógica para la Dirección General de Migración y Extranjería.

Hernández Navarro, Ballardo Josué

Marzo, 2018

página en blanco

Declaratoria de derechos de autor

Yo, Ballardo Josué Hernández Navarro, número de identificación 1-1084-0958, estudiante de la Universidad Cenfotec, de la carrera Maestría Profesional en Ciberseguridad, autorizo a la Universidad Cenfotec y a las Instituciones públicas del estado costarricense, que el presente documento pueda ser consultado y utilizado única y exclusivamente con fines académicos, una vez finalizados los dos años de declaratoria de privacidad y confidencialidad del mismo.

_____

Ballardo Josué Hernández Navarro

Dedicatoria

A Dios, por darme la capacidad y salud para llegar a alcanzar este objetivo, además de si infinita bondad y amor.

A mi esposa e hijos, por apoyarme en todo momento y el sacrificio que también representó para ustedes.

A mis padres, por su ejemplo y buen consejo, para seguir siempre adelante, en búsqueda de la excelencia no solo en lo académico, sino en todos los aspectos de la vida.

universidad cenfotec
tecnologías digitales

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría**, para el estudiante: **Ballardo Hernández Navarro**.

M. Sc. Miguel Pérez Montero
Tutor

MBA. Luis Carlos Naranjo Z.
Lector 1

M. Sc. Ignacio Trejos Zelaya
Lector 2

Tabla de contenido

Índice de Figuras

Índice de Tablas

1. Resumen ejecutivo

Este documento es creado con la intención de establecer y dotar a la Dirección General de Migración y Extranjería (DGME) de un plan de Gestión de Riesgos de Seguridad de la Información, específicamente en la seguridad lógica y física de sus activos de información.

Aspectos como la seguridad de la información, están en un constante cambio debido al desarrollo de las tecnologías de información, esto ha provocado que en la actualidad, los activos de información se digitalicen en su mayoría por parte de las empresas públicas y privadas; la DGME no es la excepción a esta tendencia, por lo que es de mucha importancia que la misma cuente con mecanismos, políticas, procedimientos, planes, entre otros, para resguardar esta información, además, siempre dependen de activos de información físicos que no dejan de ser importantes para gestionar los riesgos a los que estos y los activos lógicos están expuestos.

El presente plan de gestión de riesgos responde a una necesidad específica para la DGME, debido a que no se cuenta con este instrumento, por lo que resulta una excelente oportunidad de dotarla del mismo, además, si se analiza el aspecto de costos económicos para la Institución, este plan no tiene ningún costo de asesoría técnica.

Palabras clave: Continuidad, riesgos, amenazas, vulnerabilidades, impacto, probabilidad, apetito al riesgo.

1.1. Introducción

1.1.1. Antecedentes

Es trascendental en todas las empresas, públicas y privadas, que se gestionen los riesgos a los que están expuestas. En el caso de los riesgos de seguridad de la información, representan un aspecto que puede marcar la diferencia en la competitividad de las empresas, así como la posibilidad de que puedan operar en las condiciones necesarias, asegurando la disponibilidad, confidencialidad e integridad de la información, que son los principios que aseguran un correcto manejo de la información física y lógica, soportado en una efectiva gestión de riesgos de seguridad de la información, como mecanismo de administración y operación de los procesos y servicios que brinda una institución como la DGME.

Existen diversos elementos que se requieren para que una institución gestione, de manera eficiente, los riesgos de seguridad de la información, uno de estos aspectos es la importancia de contar con el apoyo de la parte gerencial de tecnologías de información y es que, debido a la necesidad de gestionar estos riesgos, es que se requiere establecer un plan de gestión de riesgos que responda a las necesidades actuales y además, que pueda ser parte integral del plan estratégico institucional.

Además, existen diversos requerimientos en cuanto a normativas, las cuales debe cumplir la DGME, por lo que este plan de gestión de riesgos de

seguridad de la información apoyaría de manera importante el esfuerzo que ha realizado la Institución como parte de la implementación de normas técnicas que ha venido realizando en los últimos años y como parte esencial de su plan de continuidad del negocio.

1.1.2. Justificación

La elaboración y puesta en marcha de un plan de gestión de riesgos de seguridad de la información nace de la necesidad de la DGME de contar con esta herramienta que coadyuve al logro de los objetivos institucionales. Por razones del desarrollo institucional de las tecnologías de información, en cuanto a su uso y dependencia en los procesos y servicios que brinda, se presenta un escenario ideal para que el presente trabajo pueda responder a las necesidades institucionales y lo que las normativas vigentes recomiendan, en cuanto a la administración pública de Costa Rica, para la gestión de riesgos de seguridad de la información.

Otro aspecto importante es el económico, ya que en la actualidad existen diversas herramientas y metodologías para la gestión de riesgos que tienen un costo económico importante en cuanto a su implementación, lo cual genera una limitante debido al presupuesto que posee la Institución. Así, mediante este proyecto, la elaboración e implementación de este plan de gestión de riesgos no devenga ningún costo económico para ella.

La importancia de gestionar los riesgos para cualquier empresa pública o privada, reside en poder contar con mecanismos que les permita operar de

manera más eficiente y con una mayor capacidad competitiva y un mejor y más continuo servicio al cliente, en el caso de la DGME, que tenga una garantía razonable de alcanzar sus objetivos y pueda lograr ejecutar sus procesos con seguridad y brindar servicios de calidad para los habitantes de Costa Rica y para las personas inmigrantes que utilizan sus servicios, basándose en sus objetivos estratégicos institucionales.

El Instituto de Normas Técnicas de Costa Rica, hace referencia a la importancia de la gestión de riesgos, al indicar que:

> *"Todas las actividades de una organización implican riesgos. Las organizaciones gestionan el riesgo identificándolo, analizándolo y evaluando si el riesgo se debería modificar mediante un tratamiento que satisfaga sus criterios de riesgo. A lo largo de todo este proceso, las organizaciones comunican y consultan a las partes interesadas y realizan seguimiento y revisan el riesgo y los controles que lo modifican para asegurar que no se requiere un tratamiento adicional del riesgo."* (INTECO. Instituto de Normas Técnicas de Costa Rica, 2011)

Como lo muestra el texto anterior, es de suma importancia que las instituciones gestionen riesgos como un proceso integral, que identifique, analice y evalúe amenazas y que sus resultados sean comunicados a todas las partes interesadas y revisados continuamente, para que se puedan implementar los controles necesarios y respondan a las necesidades de seguridad de la DGME.

1.2. Marco institucional.

1.2.1. Historia

Se establece en el sitio web de la DGME (DGME, 2017) que el 7 de junio de 1940, se promulgó la Ley 37, "Creación de la Oficina de Migración y Extranjeros" y su Reglamento. Esta Ley buscaba unificar las funciones referentes a migración y orientarlas de acuerdo con las necesidades del período, ya que hasta entonces eran realizadas por varias instituciones, como la cartera de Relaciones Exteriores, la de Gobernación y Policía y la del Ministerio de Seguridad Pública.

También se indica en esta página web que, en 1952, se crea el Consejo Nacional de Migración, como un órgano dependiente del Ministerio de Relaciones Exteriores, para fomentar la inmigración, regularla y establecer medidas de control, bajo la observación de los convenios internacionales, para el conocimiento y estudio de todo lo relativo a la migración.

Según esta página web, el Consejo Nacional de Migración estaba representado por delegados de las siguientes dependencias:

- Ministerio de Trabajo y Prevención Social
- Ministerio de Seguridad Pública
- Ministerio de Agricultura y Ganadería
- Ministerio de Relaciones Exteriores

- Ministerio de Gobernación
- Procuraduría de la República

Según esta página web, el 10 de setiembre de 1957, se emite el Decreto Ejecutivo No. 2, con el cual se traslada el Consejo Nacional de Migración al Ministerio de Seguridad Pública, debido a que no había cumplido con las expectativas, además, el 15 de enero de 1974, con la Ley 5874, la Oficina de Migración y Extranjeros pasa a ser la Dirección General de Migración y Extranjería, órgano especializado en materia migratoria, siempre adscrito al Ministerio de Seguridad Pública. Ya contaba con seis departamentos, incluyendo delegaciones representadas en los puestos fronterizos terrestres, marítimos y aéreos ubicados dentro del territorio nacional.

Asimismo, de acuerdo con lo que indica este sitio web, en 1982, el Gobierno efectuó ajustes en la estructura administrativa del Poder Ejecutivo, aprobó la Ley 6812 el 21 de setiembre de ese año, en la cual se establece que la Dirección General de Migración y Extranjería quedaría adscrita al Ministerio de Gobernación, siendo esta Dirección, el órgano ejecutor de la política migratoria.

A pesar de que existían decretos, circulares y resoluciones que regulaban las funciones migratorias, se carecía de un cuerpo normativo con carácter de ley unívoco para regir la materia, de acuerdo con las necesidades del creciente flujo migratorio, razón por la cual el Consejo Nacional de Migración se abocó a la elaboración de un proyecto de ley acorde con las exigencias del fenómeno migratorio.

Se indica, en este mismo sitio, que el 4 de agosto de 1986, se emite la Ley General de Migración y Extranjería Número 7033, con la cual se conformó legalmente la Dirección General de Migración y Extranjería, como una institución adscrita al Ministerio de Gobernación y Policía para que cumpliera las funciones de órgano ejecutor de la política migratoria que dicta el Poder Ejecutivo. Esta ley fue derogada por la Ley de Migración y Extranjería, Ley 8487, del 22 de noviembre de 2005, publicada en La Gaceta No. 239 del 12 de diciembre de 2005, que entró en vigencia el 12 de agosto de 2006.

Posteriormente, el 1° de setiembre de 2009 se publica la Ley General de Migración y Extranjería, Ley 8764, en el Diario Oficial La Gaceta No. 170, la cual entró en vigencia el 1° de marzo de 2010.

Los reglamentos de la Ley 8764 se publicaron en el año 2011.

1.2.2. Misión

"La Dirección General de Migración y Extranjería es el ente público ejecutor de la política migratoria, que controla el ingreso y egreso de personas al territorio nacional, promueve la integración de las personas extranjeras a la sociedad costarricense, regula permanencia y actividades de las personas extranjeras en el país y coadyuva en el combate contra los delitos de trata de personas y tráfico ilícito de migrantes, mediante la administración efectiva de los flujos migratorios que contribuyan al desarrollo y a la seguridad de Costa Rica" (DGME, 2017).

1.2.3. Visión

“Ser la institución conformada por un equipo de personas comprometido con un modelo de gestión efectivo, evolutivo y transparente, que, mediante la administración de los flujos migratorios y la integración de la población migrante, refugiada y nacional, coadyuva en el desarrollo del país, el respeto de los derechos humanos y el fortalecimiento de la seguridad pública” (DGME, 2017).

1.3. Objetivos del proyecto

Los objetivos del presente informe se desarrollan utilizando la taxonomía de Bloom, la cual permite su establecimiento de forma clara y concisa.

Utilizando este modelo, se logra el establecimiento del objetivo general y los objetivos específicos, basándose en sus seis niveles jerárquicos.

1.3.1. Objetivo general

- Diseñar un plan de gestión de riesgos de seguridad de la información física y lógica para la Dirección General de Migración y Extranjería.

1.3.2. Objetivos específicos

- Identificar los riesgos a los que está expuesta la seguridad de la información de la DGME.
- Revisar las políticas y procedimientos para el manejo de riesgos de la seguridad de la información existentes en la DGME.
- Analizar los riesgos existentes, para su debido tratamiento.
- Construir un plan de gestión de riesgos de seguridad de la información física y lógica, acorde con las necesidades y en función a los objetivos estratégicos de la DGME.

1.4. Alcance

Se toman en cuenta para la elaboración del presente plan, los riesgos de seguridad de la información físicos y lógicos de la sede central y las oficinas regionales de la DGME en el territorio costarricense. Otros aspectos por tomar en cuenta, como parte del alcance el presente plan, son los siguientes:

- No se incluirán los consulados donde presta servicios la DGME fuera del territorio costarricense, pero sí el trasiego de su información.
- No se incluirá el análisis de los riesgos de seguridad de la información de proveedores o terceros.
- Las observaciones o controles que deriven del presente plan serán aquellos que estén relacionados solo con los riesgos críticos para la DGME.

1.5. Limitaciones

Algunas de las limitaciones identificadas para el desarrollo del presente plan de gestión de riesgos son:

- Falta de conocimiento por parte del personal de la DGME en cuanto a la gestión de riesgos.
- Inexistencia de una gestión de riesgos en la DGME formalmente establecida.
- Falta de conocimiento por parte del personal de la DGME, para determinar la criticidad de la información física y lógica.

- Falta de compromiso y cultura de gestión de riesgos en la mayoría del personal de la DGME, principalmente en los altos mandos de la administración.
- Información institucional desactualizada referente a procesos y funciones críticas.

1.6. Estado de la cuestión

Se limitan las fuentes bibliográficas por el tipo de plan por realizar, debido a que es de gestión de riesgos de seguridad de información, dado que existe una gran cantidad de información disponible, referente a normativas y estándares internacionales, por lo que se limita a consultar fuentes relacionadas con la gestión de riesgos recomendadas en la legislación costarricense, para lo que se utilizan las fuentes referentes a las técnicas de valoración de riesgos, así como los principios y directrices para dicha gestión.

1.6.1. Planificación

Se consulta como fuente recomendada para establecer el enfoque del desarrollo del plan, el documento de normas técnicas establecidas por la Contraloría General de la República de Costa Rica, del capítulo I, específicamente el apartado 1.3 sobre gestión de riesgos, que establece:

> *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."* (Contraloría General de la República, 2007)

Estas directrices establecen aspectos relevantes para la *administración* pública, en lo referente a las normativas establecidas para los criterios básicos de control de las tecnologías de información.

1.6.2. Protocolo de revisión

Se toman en cuenta los siguientes elementos para efectuar la búsqueda de las fuentes por utilizar:

1.6.3. Preguntas de investigación

Se pretende con el presente plan de gestión de riesgos de la información, contestar la siguiente pregunta:

¿Qué elementos son necesarios para desarrollar el plan de gestión de riesgos de seguridad de la información física y lógica para la Dirección General de Migración y Extranjería?

1.6.4. Criterio de inclusión

Se incluyen las siguientes palabras como parámetros de inclusión para definir los criterios de inclusión de fuentes bibliográficas:

- Gestión de riesgos.
- Seguridad de la información.
- Continuidad del negocio.
- Confidencialidad.
- Disponibilidad.
- Integridad.
- Amenazas.
- Vulnerabilidades.

- Impacto.
- Nivel de riesgo.
- Sistema de gestión de seguridad de la información.

1.6.5. Criterios de exclusión

Algunos criterios utilizados para excluir fuentes de información son:

- Normativas no utilizadas en Costa Rica.

1.6.6. Criterios de calidad

La búsqueda de fuentes presenta una cantidad de documentos referentes a normativas, estándares, mejores prácticas, junto con otros, para el desarrollo del plan de gestión de riesgos, donde se toman en cuenta las fuentes que se recomiendan para la legislación costarricense, en cuanto a gestión de riesgos.

1.6.7. Fuentes consultadas

Se puede hacer referencia a las fuentes consultadas en el Anexo A.

1.6.8. Revisión de fuentes seleccionadas

La revisión de los documentos seleccionados se puede consultar en el Anexo B.

2. Marco conceptual

La importancia en la actualidad sobre la gestión de riesgos para empresas públicas y privadas, es esencial para una eficiente y adecuada operación de sus procesos y servicios, ya sea con fines de lucro o no, todas están expuestas a factores internos y externos que influencian a todas las partes que las integran y se relacionan con ellas y el efecto que genera la incertidumbre de estos factores a los objetivos estratégicos es el riesgo, el cual debe ser gestionado:

> *"Todas las actividades de una organización que implican un riesgo. Organizaciones de gestión de riesgos mediante la identificación de él, analizar y luego evaluar si el riesgo debe ser modificado por el tratamiento del riesgo, a fin de satisfacer sus criterios de riesgo."* (ISO, 2011)

Un aspecto importante es que todas las empresas, indistintamente de su tipo o tamaño, deben gestionar riesgos, lo cual es un proceso que les brinda mecanismos para manejar la incertidumbre a eventos que puedan impactar negativamente sus operaciones, mediante un proceso estructurado y organizado que garantice el tratamiento del riesgo, basándose en los requerimientos de las empresas, mismos que deben ser establecidos en función a los objetivos estratégicos de la organización y que requiere el involucramiento de todas las partes interesadas, tanto internas como externas a estas.

El uso de las tecnologías de información ha venido en crecimiento en casi todos los aspectos de la vida y en el caso del uso de tecnologías de información en las empresas no ha sido la excepción, aspectos como la competitividad, normativas, leyes y cumplimientos obligatorios, han ayudado a que las empresas

actuales hagan parte esencial a su plan estratégico de negocio la gestión de riesgos de seguridad de la información.

> *"Aunque la práctica de la gestión del riesgo ha sido desarrollada con el tiempo y en muchos sectores, a fin de satisfacer las diversas necesidades, la adopción de procesos coherentes dentro de un marco global puede ayudar a garantizar que el riesgo se gestiona de manera eficaz, eficiente y coherente en toda la organización."* (ISO, 2011)

Por lo tanto, la gestión de riesgos de seguridad de la información busca satisfacer las necesidades de las empresas, en cuanto a resguardar uno de los activos más importantes para estas: la información, que puede ser física o digital, pero que requiere el mismo tratamiento con respecto a los riesgos a los que está expuesta, gestión que debe basarse en los principios de seguridad de la información, como lo son la disponibilidad, confidencialidad e integridad.

El uso de marcos de referencia, normativas o estándares internacionales, son recursos de mucha ayuda para que las empresas puedan gestionar los riesgos de seguridad de la información, ya que brindan la hoja de ruta de los aspectos que deben desarrollarse, en este caso, el marco de referencia de ISACA[1], "COBIT 5 para la gestión de riesgos" y la norma técnica de INTECO, específicamente "Gestión de Riesgos, Principios y Directrices", se adaptan a las necesidades sobre gestión de riesgos de seguridad de la información para la Dirección General de Migración y Extranjería, lo que permite el desarrollo de un marco base en el análisis, evaluación y tratamiento del riesgo.

[1] ISACA, es el acrónimo de Systems Audit and Control Association (Asociación de Auditoria y Control de Sistemas de Información) y brinda un marco de referencia, que ayuda a las empresas y líderes de Tecnologías de la Información a maximizar el valor y gestionar los riesgos relacionados con la Tecnología de Información.

En el caso de ISACA, lo presenta de la siguiente manera:

> *"COBIT 5 ofrece un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de la tecnología de información en la empresa (TI). En pocas palabras, COBIT 5 ayuda a las empresas a crear valor óptimo a partir de las TI mediante el mantenimiento de un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y del uso de recursos. COBIT 5 facilita el gobierno y gestión de la TI en forma integral para toda la empresa, teniendo en cuenta el negocio extremo a extremo y las áreas funcionales de la responsabilidad TI y teniendo en cuenta los intereses relacionados con las TI de las partes interesadas tanto internas como externas." (ISACA, 2013)*

COBIT 5 permite a las empresas alcanzar sus objetivos mediante una óptima gestión de los recursos de tecnologías de información, brindando un equilibrio entre la obtención de beneficios en relación con los riesgos a los que estos están expuestos.

En el caso de la norma técnica desarrollada por INTECO, basada en la ISO 31000:2009, se presenta de la siguiente manera:

> *"Mientras todas las organizaciones gestionan el riesgo a diferentes niveles, esta norma establece una serie de principios que necesitan ser cumplidos para que la gestión del riesgo sea efectiva. Esta norma recomienda que las organizaciones desarrollen, implementen y mejoren de manera continua un marco de referencia cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobernanza, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización."* (INTECO. Instituto de Normas Técnicas de Costa Rica, 2011)

INTECO, mediante esta norma, hace referencia a la importancia de desarrollar, implementar y mejorar la gestión de riesgos de las instituciones, basado en los procesos de gobernanza, de la estrategia y planificación, con el fin

de generar cultura dentro de la organización en cuanto a la gestión de riesgos, con el fin de la mejora continua para generar valor agregado a los procesos de las empresas.

El riesgo se define como la combinación de un evento y sus consecuencias (ISO, 2011) y estas consecuencias afectan el logro de los objetivos de las empresas, también se puede definir como el riesgo del negocio asociado al uso, la propiedad, la operación, involucramiento, influencia y adopción de las TI en una empresa (ISACA, 2013).

La eficiente gestión de riesgos permite a las empresas (ISO, 2011):

- Aumentar la posibilidad de alcanzar los objetivos.
- Estimular la gestión proactiva.
- Ser consciente de la necesidad de identificar y tratar el riesgo en toda la organización.
- Mejorar la identificación de oportunidades y de amenazas.
- Cumplir los requisitos legales y reglamentarios pertinentes y las normas internacionales.
- Mejorar los informes obligatorios y voluntarios.
- Mejorar la gobernanza.
- Mejorar la seguridad y la confianza de las partes interesadas.
- Establecer una base fiable para la toma de decisiones y la planificación.
- Mejorar los controles.
- Asignar y utilizar de manera eficaz los recursos para el tratamiento del riesgo.

- Mejorar la eficacia y la eficiencia operacional.
- Aumentar las prestaciones en materia de salud y seguridad, así como la protección ambiental.
- Mejorar la prevención de pérdidas y la gestión de incidentes.
- Minimizar las pérdidas.
- Mejorar el aprendizaje de la organización.
- Mejorar la resiliencia de la organización.

La Figura1, muestra los principios, marco de referencia y el proceso de gestión de riesgos.

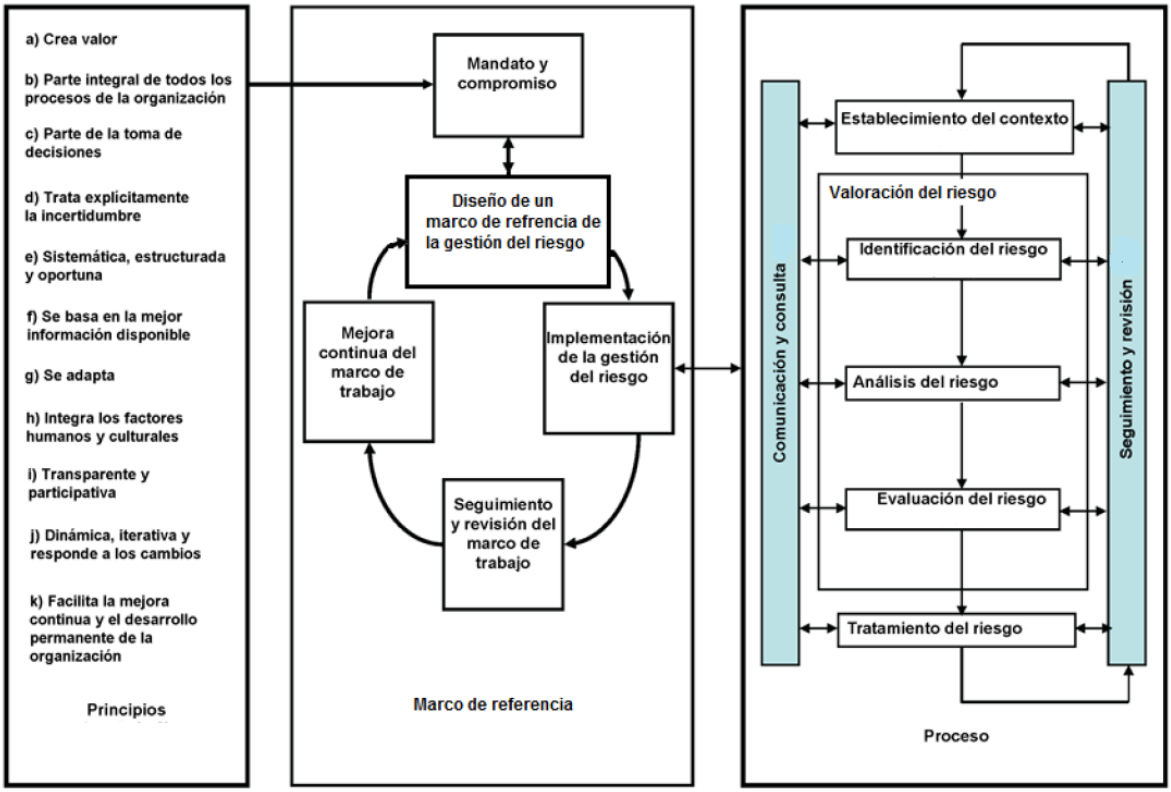

Figura 1. Principios, marco de referencia y el proceso de gestión de riesgos. Según *(ISO, 2011)*

El marco de gestión de riesgos de la ISO 31000[2], posee etapas claramente establecidas. A continuación, se hace referencia a estas etapas para establecer una referencia del proceso del plan de gestión de riesgos de seguridad de la información que se pretende desarrollar para la DGME.

2.1. Establecimiento del contexto.

Se establecen en esta etapa, los parámetros físicos para gestionar el riesgo, así como el alcance y los criterios para todo el proceso, incluyendo los parámetros internos y externos relacionados con la Institución, así como los antecedentes de los riesgos particulares por los que se realiza la valoración.

El establecimiento del contexto externo implica la familiarización con el entorno de la DGME, lo que involucra factores culturales, políticos, legales, reglamentarios, financieros, económicos o de competitividad. Además, los aspectos del contexto interno, como la capacidad de la Institución, en términos de recursos, conocimiento, flujos de información, proceso de toma de decisiones, partes interesadas internas, valores y cultura.

2.2. Principios de la gestión de riesgos.

Las organizaciones deben cumplir para una gestión eficaz de riesgos, en todos los niveles de los siguientes principios. (ISO, 2011)

a) La gestión de riesgo crea y protege el valor.

[2] La Norma ISO 31000 se conoce como el conjunto de elementos que proporcionan los fundamentos y los acuerdos de la organización para el diseño, la implementación, la revisión y la mejora continua de la de gestión de riesgos en toda la organización.

b) La gestión del riesgo es una parte integral de todos los procesos de la organización.
c) La gestión de riesgos es parte de la toma de decisiones.
d) La gestión de riesgos trata explícitamente la incertidumbre.
e) La gestión de riesgo es sistemática, estructurada y oportuna.
f) La gestión del riesgo se basa en la mejor información disponible.
g) La gestión de riesgo es a la medida.
h) La gestión del riesgo integra factores humanos y culturales.
i) La gestión del riesgo es transparente y participativa.
j) La gestión del riesgo es dinámica, iterativa y responde a los cambios.
k) La gestión del riesgo facilita la mejora continua de la organización.

2.3. Valoración del riesgo.

Este es el proceso global de identificación, análisis y evaluación de los riesgos a nivel de la Institución, proporcionando un conocimiento de los riesgos, de sus causas, sus consecuencias y sus probabilidades, proporcionando datos para la toma de decisiones acerca de: (ISO, 2011).

- Si se debería realizar una actividad.
- Como maximizar las oportunidades.
- Si los riesgos necesitan tratarse.
- La elección entre opciones con riesgos diferentes.
- La asignación de prioridades a las opciones de tratamiento del riesgo.

- La selección más apropiada de las estrategias de tratamiento del riesgo que llevarán a los riesgos adversos hasta un nivel tolerable.

2.3. Tratamiento del riesgo.

Esta etapa implica la selección y el acuerdo para disminuir la probabilidad de que los riesgos se materialicen.

2.4. Seguimiento y revisión.

Como parte del proceso, es importante que la gestión de riesgos sea evaluada y se le dé seguimiento de forma continua, con el objetivo de verificar que: (ISO, 2011)

- Las hipótesis establecidas en relación con los riesgos continúan siendo válidas.
- Las hipótesis en que se ha basado la valoración del riesgo, incluyendo los contextos, externo e interno, continúan siendo válidas.
- Se han logrado los resultados previstos.
- Los resultados de la valoración del riesgo están en línea con la experiencia real.
- Las técnicas de valoración del riesgo se han aplicado adecuadamente.
- Los tratamientos del riesgo son efectivos.

2.5. Identificación del riesgo.

Este es el proceso por el cual se reconocen y registran los riesgos, el cual tiene como finalidad identificar qué podría pasar o qué situaciones podrían afectar los logros de la Institución. Incluye, además, las causas y la fuente del riesgo, eventos, situaciones o circunstancias que puedan tener un impacto material sobre los objetivos de la organización, así como los eventos del riesgo y las consecuencias y posibilidades de este.

Otros aspectos que se establecen en esta etapa son los siguientes:

- Perfil de riesgo.
- Determinar la naturaleza del riesgo.
- Establecer los criterios del riesgo.
- Establecer los niveles de riesgo.

2.6. Evaluación del riesgo.

Este es el proceso por el cual se comparan los resultados del análisis de riesgo, con los criterios del riesgo, para determinar si el riesgo y/o su magnitud son aceptables o tolerables. Este, además, ayuda a la toma de decisiones para la etapa del tratamiento del riesgo.

2.7. Tratamiento del riesgo.

Esta etapa tiene como objetivo principal modificar o alterar el riesgo, dentro de sus acciones puede incluir:

- Evitar el riesgo.
- Aceptar o aumentar el riesgo, con el fin de buscar una oportunidad de mejora.
- Eliminar la fuente del riesgo.
- Cambiar la posibilidad.
- Cambiar las consecuencias.
- Compartir el riesgo o transfiriéndolo.
- Mantener el riesgo con base en una decisión informada.
- Establecer controles en busca de modificar el riesgo.
- Incluso, a pesar del tratamiento del riesgo, es importante tener presente el riesgo remanente o riesgo residual, que puede quedar presente debido a riesgos ocultos y no identificados en la etapa de identificación o producto de la tolerancia al riesgo.

2.8. Seguimiento.

Esta etapa permite la verificación, supervisión, observación crítica y la inclusión, de manera continua, de los cambios que se puedan presentar a nivel de desempeño requerido o esperado, de los procesos o servicios de la Institución.

2.9. Revisión.

Se debe llevar a cabo en esta última etapa, una revisión continua para determinar la idoneidad, adecuación y eficacia del plan de gestión de riesgos establecido, y valorar si cumple los objetivos previamente establecidos.

3. Marco metodológico.

3.1. Tipo de investigación evaluativa

Se analizan y evalúan los mecanismos de gestión de riesgos que posee la DGME, por el tipo de plan por realizar y al no tratarse de una investigación pura, para luego desarrollar un plan de gestión que comprenda la identificación, análisis, respuesta y reporte de riesgos de seguridad de la información física y lógica.

3.2. Enfoque

El enfoque por utilizar para el análisis y evaluación de los riesgos es un análisis cualitativo y semicuantitativo, ya que el primero produce resultados válidos que son descriptivos, específicamente “posibilidades”, lo que permita aginar probabilidades al presente plan, y el segundo, ya que permite asignar valores a las escalas que se utilizarían exclusivamente en la evaluación cualitativa y debido a que no se cuenta con datos estadísticos históricos de la DGME para llevar a cabo un análisis meramente cuantitativo.

3.3. Sujetos y fuentes de información

Estos son algunos sujetos y fuentes de información que se analizan para lograr obtener la información apropiada y que permita calidad en los resultados esperados:

- Revisión de documentación histórica o de planes relacionada a continuidad del negocio que posee la DGME.
- Foros de discusión con los dueños de la información y los dueños de los sistemas.
- Foros de discusión con los interesados en la implementación del plan de gestión de riesgos.
- Reuniones con el personal del departamento de GTI (Gestión de tecnologías de información) y sus sub-procesos.
- Reuniones con los jefes de las regionales de la DGME.

3.4. Instrumentos

Se utilizan diversos medios, físicos y lógicos, para obtener la información mediante la revisión de políticas y procedimientos existentes, así como el uso de entrevistas para recopilar datos y algunos otros formularios y matrices que se incluyen en los anexos.

4. Evaluación de los riesgos de seguridad de la información física y lógica.

Es importante determinar los parámetros internos y externos para establecer la política de gestión de riesgos de seguridad de la información física y lógica de la DGME, además, se debe contar con la participación de los colaboradores de la Unidad de Tecnologías de Información.

4.1. Áreas de impacto.

Es importante para la determinación de las áreas de impacto, hacer referencia a los objetivos estratégicos planteados por el Departamento de Tecnologías de Información de la DGME, con base en los procesos y actividades desarrolladas en las áreas funcionales de los servicios que esta brinda, las cuales se muestran en la Tabla 1.

Tabla 1
Áreas de Impacto del riesgo.

Área de impacto	Descripción
Administración y gestión de TI	Analizar el impacto al que están expuestas las funciones y actividades estratégicas de TI.
Infraestructura de las tecnológicas de información.	Analizar el impacto sobre los procesos relacionados con la infraestructura de las TI en la actualidad y en el largo plazo en cuanto a su evolución.
Seguridad y riesgos	Impacto sobre la disponibilidad, confidencialidad e integridad en el cumplimiento de la gestión de TI.
Sistemas de información	El impacto sobre el funcionamiento de los sistemas de la DGME
Administración y gestión de los archivos físicos de la información.	El impacto sobre los almacenes de información física de la Institución.

Esta tabla muestra las áreas de impacto que pueden afectar los riesgos de seguridad de la información de la DGME. Elaboración propia.

En el proceso de evaluación de riesgos es determinante que estos se clasifiquen para facilitar su análisis y evaluación, además, esto permite que la gestión de riesgos se desarrolle en función a los riesgos relevantes para TI y en función a los objetivos estratégicos de la Institución.

5. Identificación de los activos.

Como parte esencial del plan de gestión de riesgos es importante identificar los activos para la evaluación de los riesgos de estos, así como establecer su criticidad y el establecimiento de las dependencias y las funciones críticas.

Esta información se obtuvo del análisis de la infraestructura tecnológica de la DGME, así como de las entrevistas con las partes involucradas en la administración o uso de los activos de información física y lógica de la Institución.

5.1. Identificación de los activos de información.

Se estableció la necesidad de identificar y clasificar los activos lógicos y físicos de información de la DGME y su criticidad; en la Figura 2, se muestran los valores de clasificación de estos activos, basados en su criticidad y disponibilidad requerida, así como la definición de los objetivos de los tiempos de recuperación RTO (Recovery Time Objetive) para las funciones críticas del negocio relacionados con los activos de información de la DGME, esta información fue obtenida del Análisis de Impacto del Negocio BIA que posee la Institución.

Mayor o igual a 1 hora Mayor a 1 hora y hasta 4 horas
Mayor a 4 horas y hasta 1 día Mayor a 1 día y hasta 2 días
Mayor a 2 días y hasta 4 días
No soporta funciones críticas de la Institución.

Figura 2. Tiempo de recuperación para funciones críticas del negocio (RTO).
Definido por el departamento de tecnologías de la información de la DGME.

En la Tabla 2. Se muestran los criterios para la definición de la disponibilidad de los activos de información.

Tabla 2
Criterios para la definición de la disponibilidad.

Nivel	Descripción
Alta	Si la información no está disponible, esto afecta las actividades administrativas, afecta el servicio de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Minutos a Horas".
Media	Si la información no está disponible, esto podría causar pérdida de productividad, pero no interrumpe los servicios de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Horas a Días".
Baja	Si la información no está disponible, esto no impacta severamente las actividades administrativas de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Días a Semanas"

Información obtenida del Análisis de Impacto del negocio BIA de la DGME.

5.2. Identificación y clasificación de los activos lógicos de información.

Se muestra a continuación, la clasificación de los activos esenciales de la DGME, basado en los servicios prestados y la dependencia de estos con otros

procesos de negocio, en la Tabla 3 se muestra la clasificación de los activos de información lógica, indicando su criterio de criticidad y disponibilidad.

Tabla 3
Activos lógicos de información.

Aplicación o sistema	Criticidad	Disponibilidad
Sistema de información	Menor o igual a 1 hora	Alta
Aplicaciones bases de datos	Menor o igual a 1 hora	Alta
Sistema de información WEB	Menor o igual a 1 hora	Alta
Sistema Web Services de Pasaportes	Menor o igual a 1 hora	Alta
Sistema Web Services Impedimentos de Salida	Menor o igual a 1 hora	Alta
Sistema API	Menor o igual a 1 hora	Alta
Sistema de menores	Menor o igual a 1 hora	Alta
Sistema de movimiento migratorio electrónico (SIMMEL).	Menor o igual a 1 hora	Alta
Sistema de Policía	Menor o igual a 1 hora	Alta
Sistema de gestión de migraciones	Menor o igual a 1 hora	Alta
Sistema de Pasaportes (SISPAS).	Menor o igual a 1 hora	Alta
Sistema de refugio	Mayor a 1 hora y hasta 4 horas	Alta
Sistema de visas	Mayor a 1 hora y hasta 4 horas	Alta
Sistema de información SharePoint	Mayor a 1 hora y hasta 4 horas	Alta
Sistema Interpol	Mayor a 1 hora y hasta 4 horas	Alta
Sistema de extranjería (SINEX)	Mayor a 1 hora y hasta 4 horas	Media
Sistema de contraloría de servicios	Mayor a 1 hora y hasta 4 horas	Media
Sistema de correo electrónico institucional (Zimbra)	Mayor a 1 hora y hasta 4 horas	Media
Sistema Cardex	Mayor a 1 hora y hasta 4 horas	Media
Sistema control de accesos	Mayor a 1 hora y hasta 4 horas	Media
Sistema de Bancos	Mayor a 1 día y hasta 2	Media

	días	
Sistema de cheques	Mayor a 1 día y hasta 2 días	Media
Sistema de devolución de depósitos	Mayor a 1 día y hasta 2 días	Baja
Sistema de seguridad	Mayor a 1 día y hasta 2 días	Media
Servidor Carpetas Compartidas Usuarios DGME	Mayor a 2 días y hasta 4 días	Media
Sistema SISCAP	Mayor a 2 días y hasta 4 días	Baja
Sistema Almacén	Mayor a 2 días y hasta 4 días	Baja
Sistema de presupuesto	No soporta función crítica	Baja
Sistema de recursos humanos (Marcas)	No soporta función crítica	Baja
Sistema Gestor Documental SE SUITE	No soporta función crítica	Baja
Sistema SICOP	No soporta función crítica	Baja
Sistema SICOVI	No soporta función crítica	Baja
Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados	No soporta función crítica	Baja
Sistema Visor de pasaportes	No soporta función crítica	Baja
Web Services de SINEX-CARDEX	No soporta función crítica	Baja
Web Services Sistema de Información Policial	No soporta función crítica	Baja
Sistema inventario de equipos y licencias de software	No soporta función crítica	Baja
Sistema Felino	No soporta función crítica	Baja
Equipo jefatura del departamento Financiero	Mayor a 2 días y hasta 4 días	Media
Equipo de la Jefatura de la gestión de Transportes	Mayor a 2 días y hasta 4 días	Media
Equipo de la jefatura de Servicios de Apoyo	Mayor a 2 días y hasta 4 días	Media
Equipo de coordinación Policial Aeropuerto Juan Santamaría	Mayor a 2 días y hasta 4 días	Media
Equipo de jefatura de la gestión de Extranjería	Mayor a 2 días y hasta 4 días	Media
Equipo de jefatura de la gestión de Migraciones	Mayor a 2 días y hasta 4 días	Media
Equipo de jefatura de la	No soporta función crítica	Baja

gestión de Servicio Civil.		
Equipo de jefatura de la gestión Policial de la Regional de Paso Canoas	No soporta función crítica	Baja
Equipo de jefatura de la gestión Policial de la regional de Upala	No soporta función crítica	Baja
Equipo de jefatura de la gestión de Archivo Central	No soporta función crítica	Baja
Equipo de jefatura de la gestión de Recursos Humanos	No soporta función crítica	Baja
Equipo de jefatura de la Gestión Jurídica	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Proveeduría	No soporta función crítica	Baja
Equipo de jefatura de la gestión de Contraloría de Servicios	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Investigaciones	No soporta función crítica	Baja
Equipo de jefatura de la Coordinación Regional	No soporta función crítica	Baja
Equipo de Diana Alfaro, jefe de Evaluación Técnica	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Consulados	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Menores	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Certificaciones	No soporta función crítica	Baja
Equipo de jefatura de la Gestión de Trata y Tráfico	No soporta función crítica	Baja

Información obtenida de las entrevistas realizadas al personal de la DGME.

5.3. Identificación y clasificación de los activos físicos de información.

La clasificación de los activos de información física, al igual que los activos lógicos, es esencial para el análisis de los riesgos de estos, en la Tabla 4, se muestra el inventario de los activos físicos de información.

Tabla 4
Activos físicos de información.

Activo físico	Criticidad	Disponibilidad
Archivo del Departamento de Extranjería	Menor o igual a 1 hora	Alta
Archivo del Departamento de Menores	Menor o igual a 1 hora	Alta
Archivo del Departamento de Policía	Menor o igual a 1 hora	Alta
Archivo Central DGME	Menor o igual a 1 hora	Alta
Archivo del Departamento de Migraciones	Mayor a 1 hora y hasta 4 horas	Alta
Archivo del Departamento de Refugio	Mayor a 1 hora y hasta 4 horas	Alta
Archivo del Departamento de Visas	Mayor a 1 hora y hasta 4 horas	Alta
Archivo del Departamento de Recursos Humanos	Mayor a 1 día y hasta 2 días	Media
Archivo del Aeropuerto Juan Santamaría	Mayor a 1 día y hasta 2 días	Media
Archivo del Departamento de Financiero, Presupuesto, Cheques y depósitos.	No soporta función crítica	Baja
Archivo del Departamento de Almacén	No soporta función crítica	Baja
Archivo del Departamento de Seguridad	No soporta función crítica	Baja
Archivo del Departamento de Transportes	No soporta función crítica	Baja
Archivo del Departamento Administrativo	No soporta función crítica	Baja
Archivo del Departamento de Servidores	No soporta función crítica	Baja
Archivos Departamento CICI	No soporta función crítica	Baja
Archivo Proyectos DGME	No soporta función crítica	Baja
Archivo Soporte Técnico	No soporta función crítica	Baja
Archivo Aeropuerto Daniel Oduber	No soporta función crítica	Baja

Información obtenida de las entrevistas realizadas al personal de la DGME.

5.4. Identificación de dependencias de los activos críticos de información.

La Tabla 5, muestra la identificación de los activos críticos, así como las relaciones que estos poseen con otros activos de la Institución, tomando en cuenta aspectos como los servidores donde están alojados los sistemas, relaciones de software y hardware, y los activos de redes que interactúan con estos activos.

Lo importante de esta tabla, es que muestra un inventario completo de toda la infraestructura que soporta a los activos lógicos críticos de la información de la DGME, así como, las dependencias entre estos, a continuación, un resumen de los elementos que lo componen, la referencia completa se puede consultar en el Anexo D.

Tabla 5
Dependencias de los activos críticos de información

Sistemas o aplicaciones críticas	Bases de datos críticas	Equipos de comunicaciones y redes críticos	Servidores críticos
• **Sistema de información** • **Sistema de información WEB** • **Sistema Web Services de Pasaportes** • **Sistema Web Services Impediments de Salida** • **Sistema API** • **Sistema de**	• Sybase15.7 • Oracle 10g R2 • SQL Server 2005 y 2008 • Access • MySQL • Extranjeros • General • Sinex-Cardex • Certificaciones • Financiero • Estado • Seguridad • Administrativo • SISPAS • Movimientos • Marcas • Web-Services	• Conexión al poder judicial Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2 • Servidor físico Dirección IP 192.168.121.250 • Sistema Operativo SUN Fire 480-R • Dirección IP 172.16.254.10 Windows 7 SP1 • Dirección IP 172.16.254.11 Windows 7 SP1 • Nombre le equipo CARDEX

menores • **Sistema de movimiento migratorio electrónico (SIMMEL).** • **Sistema de Policía** • **Sistema de gestión de migraciones** • **Sistema de Pasaportes (SISPAS).** • **Sistema de refugio** • **Sistema de visas** • **Sistema de información SharePoint** • **Sistema Interpol** • **Sistema de extranjería (SINEX)** • **Sistema de correo electrónico institucional (Zimbra)** • **Sistema Cardex** • **Sistema control de accesos** • **Sistema de Bancos** • **Sistema de seguridad** • **Servidor de Carpetas compartidas usuarios DGME** • **Sistema SISCAP**	Consulta servicio Interpol • CARDEX	Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505	192.168.121.103 Windows Server 2003 R2 • Nombre del servidor AFIS1 192.168.121.101 Windows 2003 Server R2 • Nombre del servidor AFIS2 192.168.121.102 Windows 2003 Server R2 • Nombre del servidor SINEX-CARDEX 10.10.10.6 Windows Server 2003 Server • Servidor Solaris Versión 9 • Dirección IP 10.10.10.4 Windows Server 2003 • BCR-GDME-GOV-DIGITAL • Servidores PP1 Y PP2 • Dirección IP PP1 10.10.10.5 Windows Server 2003 • Dirección IP PP1 10.10.10.7 • 10.10.10.250 Windows 7 • Base de datos 10.10.10.6 Windows Server 2003 • Dirección IP 10.10.10.4 Windows Server 2003 • BCR-GDME-GOV-DIGITAL • Servidores PC ARINC. Windows XP SP1 • 129.13.0.112 • ROBOT: Servidores (PC) SITA. Windows 7 SP1 • 129.13.0.114 • 129.13.0.178 • Dirección IP 192.168.121.186 • Nombre del servidor: Marcas • Servidor Físico con sistema operativo Windows 2003 SP1

• **Sistema Almacén** • **Sistema de devolución de depósitos** • **Sistema WEB Visor de pasaportes** • **Web Services de SINEX-CARDEX** • **Web Services Sistema de Información Policial**	• Nombre del servidor: Turrialba dirección IP 192.168.121.25 consulta • Servidor SUN x2200(virtual) • Vmware físico versión 5.0 • Servidor Vcenter • Hojas Blade de la 2 a la 7 • 13 servidor • Rango de direcciones IP 10.200.201.17 – 35 • Sistema Operativo Windows 2012 R2 standard • Servidor Virtual • Vcenter • Dirección IP 10.200.201.10 y 10.200.201.11 • Sistema Operativo CentOS Linux • Servidor de procesamiento físico HP Cardex ESX01 (con 4 virtuales). • Servidor de procesamiento físico HP Cardex ESX02 (con 4 virtuales). • Sistema que administra: ESX 5.1. • Sistema operativo Windows 2003 R2 SP2 en los 4 servidores • Rango de direcciones IP 192.168.121.101 Windows Server 2003 R2 SP2 • 192.168.121.103 Windows Server 2003 R2 SP2 • 192.168.121.104 Windows Server 2003 R2 SP2 • Servidor Virtual en SVMware • Dirección IP 192.168.121.32 • Sistema Operativo Windows 2003 Server SP2

	• Servidor Base_NLB1 • Dirección IP 192.168.122.231. • Sistema operativo Windows 2008 R2 SP1 • Servidor Radius Dell 2950

Información obtenida de las entrevistas realizadas al personal de la DGME y análisis de riesgos realizados en la DGME en 2013.

5.5. Identificación de dependencias de las funciones críticas de los activos de información.

La Tabla 6, muestra las relaciones que poseen las funciones críticas del negocio con los activos de información previamente definidos.

Tabla 6
Dependencias de las funciones críticas de los activos de información.

Aplicación o sistema	Funciones críticas
Sistema de información	• Control Migratorio. • Control migratorio y atención a personas menores de edad. • Confeccionar exoneraciones de impuestos de salida. • Expedición de documentos migratorios. • Recepción de Solicitudes Migratorias en las Delegaciones Regionales. • Recepciones y atenciones de denuncias en contra de extranjeros. • Trata y Tráfico de Personas. • Recepción de documentos con público. • Recepción de denuncias – Gestión Operativa Policía Migración. • Recepción de Denuncias – Contraloría de Servicios. • Control migratorio de personas que ingresan y egresan al área de hangares y operativos. • Recepción de solicitudes de refugiados. • Operativos de Control Migratorio. • Valoración e investigación de aprehendidos. • Traslados de aprehendidos. • Confección de Resoluciones de Aprehensión. • Captura de foto y huella para emisión del documento de identidad para emisión de permanencia DIMEX. • Expedición de documentos migratorios. • Expedición de permisos de salida, revocatorias, alertas, modificaciones a los permisos de salida de las personas menores de edad.

	• Brindar atención y seguimiento a posibles víctimas y sobrevivientes de la Trata. • Tramitación de VISAS
Sistema base de datos	• Gestión y administración de todas las bases de datos de los sistemas de la DGME. • Administración de los usuarios de bases de datos. • Conectividad a los servicios web con diversas entidades públicas.
Sistema de información WEB	• Recepción de Denuncias - Contraloría de Servicios. • Realizar control de calidad a los registros de entradas y salidas. • Valoración e investigación de aprehendidos • Expedición de documentos migratorios.
Sistema Web Services de Pasaportes	• Expedición de documentos migratorios.
Sistema Web Services Impedimentos de Salida	• Inclusión, exclusión, modificación y permisos de impedimentos de salida del país, de entrada y de alertas. • Recepción de Denuncias - Contraloría de Servicios
Sistema API	• Investigación sobre Trata y Tráfico de Personas. • Recepción de Denuncias. • Realizar control de calidad a los registros de entradas y salidas. • Control a los impuestos de salida, en coordinación con el Órgano Fiscalizador-DGAC.
Sistema de menores	• Investigación sobre Trata y Tráfico de Personas. • Recepción de Denuncias - Contraloría de Servicios. • Realizar control de calidad a los registros de entradas y salidas. • Valoración e investigación de aprehendidos. • Confección de Resoluciones de Aprehensión. • Expedición de documentos migratorios. • Expedición de permisos de salida, revocatorias alertas, modificaciones a los permisos de salida de las personas menores de edad.
Sistema de movimiento migratorio electrónico (SIMMEL).	• Control Migratorio. • Control Migratorio y atención a personas menores de edad.

	• Confeccionar exoneraciones de impuestos de salida. • Expedición de documentos migratorios. • Trata y Tráfico de Personas. • Inclusión y levantamientos de impedimentos de entradas y salidas del país. • Recepción de documentos con público. • Investigación sobre Trata Tráfico de Personas. • Inclusión, exclusión, modificación y permisos de impedimentos de salida del país, de entrada y de alertas. • Control migratorio de personas que ingresan y egresan al área de hangares y operativos. • Recepción de solicitudes de refugiados. • Realizar control de calidad a los registros de entradas y salidas. • Control a los impuestos de salida, en coordinación con el Órgano Fiscalizador-DGAC. • Operativos de Control Migratorio. • Valoración e investigación de aprehendidos. • Registro de Movimientos Migratorios. • Valoración e investigación de aprehendidos. • Traslados de aprehendidos. • Confección de Resoluciones de Aprehensión. • Captura de foto y huella para emisión del documento de identidad para emisión de permanencia DIMEX. • Expedición de certificaciones de movimientos migratorios. • Brindar atención y seguimiento a posibles víctimas y sobrevivientes de la Trata.
Sistema de Policía	• Control Migratorio. • Control migratorio y atención a personas menores de edad. • Recepciones y atenciones de denuncias en contra de extranjeros. • Trata y Tráfico de Personas. • Recepción de documentos con público. • Investigación sobre Trata y Tráfico de Personas. • Recepción de denuncias - Gestión Operativa Policía Migración. • Recepción de Denuncias - Contraloría de Servicios.

	• Recepción de solicitudes de refugiados. • Operativos de Control Migratorio. • Valoración e investigación de aprehendidos. • Traslados de aprehendidos. • Captura de foto y huella para emisión del documento de identidad para emisión de permanencia. • DIMEX. • Brindar atención y seguimiento a posibles víctimas y sobrevivientes de la Trata. • Operativos institucionales.
Sistema de gestión de migraciones	• Inclusión, exclusión, modificación y permisos de impedimentos de salida del país, de entrada y de alertas. • Expedición de documentos migratorios. • Expedición de permisos de salida, revocatorias, alertas, modificaciones a los permisos de salida de las personas menores de edad. • Expedición de certificaciones de movimientos migratorios.
Sistema de Pasaportes (SISPAS).	• Trámites de pasaportes. • Investigación sobre Trata y Tráfico de Personas. • Expedir documento de pasaporte. • Valoración e investigación de aprehendidos. • Expedición de documentos migratorios.
Sistema de recursos humanos	• Investigación sobre Trata y Tráfico de Personas.
Sistema de refugio	• Investigación sobre Trata y Tráfico de Personas. • Recepción de solicitudes de refugiados. • Expedición de documentos migratorios.
Sistema de visas	• Investigación sobre Trata y Tráfico de Personas. • Incluir en sistema autorizaciones y denegatorias. • Tramitación de VISAS.
Sistema de extranjería (SINEX)	• Control Migratorio. • Control migratorio y atención a personas menores de edad. • Recepción de Solicitudes Migratorias en las Delegaciones Regionales. • Recepciones y atenciones de denuncias en contra de extranjeros. • Trata y Tráfico de Personas.

	• Recepción de documentos con público. • Investigación sobre Trata y Tráfico de Personas. • Recepción de denuncias - Gestión Operativa Policía Migración. • Recepción de Denuncias - Contraloría de Servicios. • Control migratorio de personas que ingresan y egresan al área de hangares y operativos. • Recepción de solicitudes de refugiados. • Operativos de Control Migratorio. • Valoración e investigación de aprehendidos. • Renovación de documentos DIMEX en las Delegaciones Regionales. • Valoración e investigación de aprehendidos. • Traslados de aprehendidos. • Captura de foto y huella para emisión del documento de identidad para emisión de permanencia DIMEX. • Atención del usuario. • Expedición de permisos de salida, revocatorias, alertas, modificaciones a los permisos de salida de las personas menores de edad. • Brindar atención y seguimiento a posibles víctimas y sobrevivientes de la Trata. • Operativos institucionales. • Tramitación de VISAS. • Expedición de certificación de estatus de personas extranjeras. • Administrar el historial de las solicitudes de personas extranjeras.
Sistema de contraloría de servicios	• Realizar el registro inmediato de las inconformidades que presentan los usuarios asignándole inmediatamente un número de control y generando estadísticas para reportes sobre las razones de las inconformidades.
Sistema Gestor Documental SE SUITE	• Sistematización de la Gestión Documental Electrónica de la DGME, con Firma Digital. Tiene las funciones de Manager y Staff Técnico para Ejecutar, Aprobar y Consultar la Correspondencia Institucional.
Sistema de correo electrónico institucional (Zimbra)	• Almacenamiento y gestión de correos electrónicos institucionales
Sistema Cardex	• Recepción de Solicitudes Migratorias en las Delegaciones Regionales. • Valoración e investigación de

	aprehendidos. • Expedir el documento de permanencia legal de una persona extranjera con permanencia legal en el país.
Sistema control de accesos	• Otorgar permisos de control de acceso a las diversas puertas al personal de la DGME.
Sistema de bancos	• Tramitación de VISAS
Sistema de cheques	• Se realiza la confección e impresión de los cheques.
Sistema de seguridad	• Gestionar usuarios de los sistemas de la DGME • Creación de perfiles • Asignar usuarios a los perfiles
Servidor carpetas compartidas usuarios DGME	• Almacenar y compartir los recursos de información lógica, documentos, archivos varios, entre los diversos departamentos, procesos y subprocesos de la DGME.
Sistema SISCAP	• Realizar control de calidad a los registros de entradas y salidas. • Control a los impuestos de salida, en coordinación con el Órgano Fiscalizador-DGAC. • Confección de Resoluciones de Aprehensión
Sistema Almacén	• Registro de entradas y salidas de los productos que administra el almacén de la DGME
Sistema de devolución de depósitos	• Control de depósitos de garantías. • Tramitación de solicitud de devolución de depósitos. • Creación de cheques de devolución de depósitos. • Control de salidas de cheques.
Sistema SICOVI	• Control de viáticos de los funcionarios de la DGME
Sistema de transportes	• Registrar los expedientes de las personas y vehículos de la Institución. • Control de combustible y registro de mantenimientos de las unidades de transporte de la DGME.
Sistema Visor de pasaportes	• Visualización de imágenes de pasaportes de menores con los permisos. • Corrección de fotografías para impresora láser.
Web Services de SINEX-CARDEX	• Recibe las solicitudes de documentación d extranjeros y del Banco BCR y Correos de CR. • Manejo de consultas del centro de llamadas.
Web Services de Información Policial	• Consultas del histórico de pasaportes.

	• Consulta de huellas y fotografías • Consulta de información de extranjeros.
Sistema inventario de equipos y licencias de software ARANDA	• Inventario de software y hardware de la DGME. • Control de activos asignados a los usuarios.
Sistema Felino	• Administración y gestión de los proyectos de la DGME

Información obtenida de las entrevistas realizadas al personal de la DGME y análisis de riesgos realizados en la DGME en 2013.

6. Identificación de los riesgos.

6.1. Establecimiento de los criterios de evaluación de riesgos.

Se definen a partir de esta etapa, diversos criterios de evaluación de los riesgos en cuanto a los siguientes aspectos:

- Identificación de las amenazas.
    - Factores de riesgo.
    - Categoría de los riesgos.
- Identificación de las vulnerabilidades.
    - Tipos de vulnerabilidades.
- Definición del impacto.
- Definición de la probabilidad de ocurrencia.
- Determinación del riesgo potencial.

6.2. Identificación de las amenazas.

Se debe hacer referencia a los escenarios de riesgos que pueden presentarse en la DGME, así como a los orígenes de las amenazas para identificar las amenazas a las que están expuestos los activos lógicos y físicos de información.

En la Tabla 7, se muestran algunos escenarios y factores de riesgo determinado por los orígenes de las amenazas que se pueden presentar en la DGME.

Tabla 7
Factores de riesgo de seguridad de la información.

Factor de riesgo	Descripción
Tecnológicos, habilidades y conocimientos	Son todos aquellos factores relacionados con el uso de instrumentos de tecnologías de la información, así como las capacidades y conocimientos individuales.
Condiciones financieras	Cambios en el presupuesto de la Institución.
Relación con otras instituciones y empresas.	Relaciones de las DGME, con organismos internacionales, proveedores, instituciones y empresas a nivel nacional.
Comportamiento humano	Son todas aquellas actitudes que tienen las personas internas o externas a la Institución y que interactúan con ella.
Naturales	Todos aquellos eventos naturales que puedan afectar a la Institución.
Normativos y legales	Cambios en requerimientos legales y de regulación nacional e internacional en los que se desarrolla DGME.
Disposiciones de Gobierno	Factores relacionales a cambios gubernamentales.
Estratégicos	Factores relacionados con cambios en la estrategia y sus objetivos en la Institución.

Esta tabla muestra los factores de riesgos que pueden presentarse en la DGME

Otros aspectos para tomar en cuenta para el análisis de los riesgos, en cuanto a la definición de las amenazas, es la categoría de los mismos. En la Tabla 8, se presentan algunas de las categorías identificadas para el presente plan.

Tabla 8
Categorías del riesgo de seguridad de la información.

Categorías de riesgo	Descripción
Riesgo estratégico	Riesgos relacionados con el cambio en los objetivos estratégicos de la DGME.
Riesgos operativos	Riesgos relacionados con las situaciones que afecten el logro de objetivos estratégicos de la Institución.
Riesgos legales	Riesgos relacionados con el cambio o cumplimiento de aspectos legales establecidos en los objetivos de

	la Institución.
Riesgos ambientales	Riesgos relacionados con aspectos ambientales que afecten los activos y funciones críticas de la Institución.
Riesgos tecnológicos	Riesgos relacionados con el uso de las tecnologías que puedan interrumpir el funcionamiento de las funciones críticas de la Institución.
Riesgo financiero	Riesgos relacionados con las actividades financieras que afecten las responsabilidades y sus obligaciones.
Riesgos humanos	Riesgos relacionados con aspectos del comportamiento humano.
Riesgos comerciales	Riesgos relacionados con aspectos que interactúan con otras empresas o proveedores.
Riesgos naturales	Riesgos relacionados con fenómenos de la naturaleza

Esta tabla muestra las categorías de los riesgos que se pueden presentar en la DGME.

No todos los tipos de amenazas o escenarios de riesgo afectan a todos los activos, parte del presente plan es determinar las amenazas para cada activo de la DGME.

6.3. Identificación de las vulnerabilidades.

Las vulnerabilidades son las debilidades o defectos en los controles, diseño, ejecución o procedimiento de seguridad de un activo, los cuales aprovechan las amenazas para afectar la disponibilidad generando un fallo o violación de la política de seguridad de la información. Una amenaza por sí sola, no genera un daño directo, requiere de la presencia de una vulnerabilidad para que genere daño, por lo que es importante que se consideren todas las vulnerabilidades relacionadas en forma directa o indirecta al activo. En la Tabla 9, se presentan una serie de posibles tipos de vulnerabilidades que pueden afectar a la DGME.

Tabla 9
Vulnerabilidades de seguridad de la información.

Tipo de vulnerabilidad	Descripción
Ambientales o físicas	Aspectos relacionados con desastres naturales, ubicación de las oficinas, capacidad técnica, materiales almacenados, etc.
Económica	Recorte de presupuestos o mal manejo de recursos públicos
Socioeducativa.	Aspectos relacionados con las relaciones y comportamiento humano.
Política o institucionales	Aspectos relacionados con proceso de la Institución, así como a la burocracia, corrupción y la falta de un plan estratégico de negocio.
Tecnológicas	Aspectos relacionados con deficiencias en las tecnologías, vulnerabilidades digitales, entre otros.
Ideológicas y culturales	Aspectos relacionados con la visión de conceptos y prejuicios que poseen las personas.

Esta tabla muestra los posibles tipos de vulnerabilidades que se pueden presentar en la DGME.

Para la identificación de los riesgos y sus vulnerabilidades se presenta un resumen de los datos más relevantes, haciendo referencia al Anexo E, donde se pueden visualizar todos los riesgos y vulnerabilidades detectados en los procesos de análisis visual, visitas a las regionales y análisis de vulnerabilidades en los activos lógicos críticos definidos anteriormente.

A continuación, se muestran las regionales visitadas para el análisis de los riesgos y vulnerabilidades detectadas.

- Regional de los Chiles.
- Regional de Tablillas.
- Regional de Upala.
- Regional de Ciudad Quesada.

- Regional de Sixaola.
- Regional de Sarapiquí.
- Regional de Guápiles.
- Regional de Limón.
- Aeropuerto Juan Santamaría.
- Regional de Sabalito.
- Regional de Paso Canoas.
- Regional de Quepos.
- Regional de Golfito.
- Regional de Pérez Zeledón.
- Aeropuerto Daniel Oduber
- Oficinas Centrales de La Uruca.
- Regional de Peñas Blancas

A continuación, se muestran en resumen los datos más relevantes dentro del análisis de los riesgos detectados y sus vulnerabilidades.

6.4. Resumen de los riesgos detectados.

La Figura 3, muestra que se detectaron 340 riesgos en la DGME y su distribución por oficina regional.

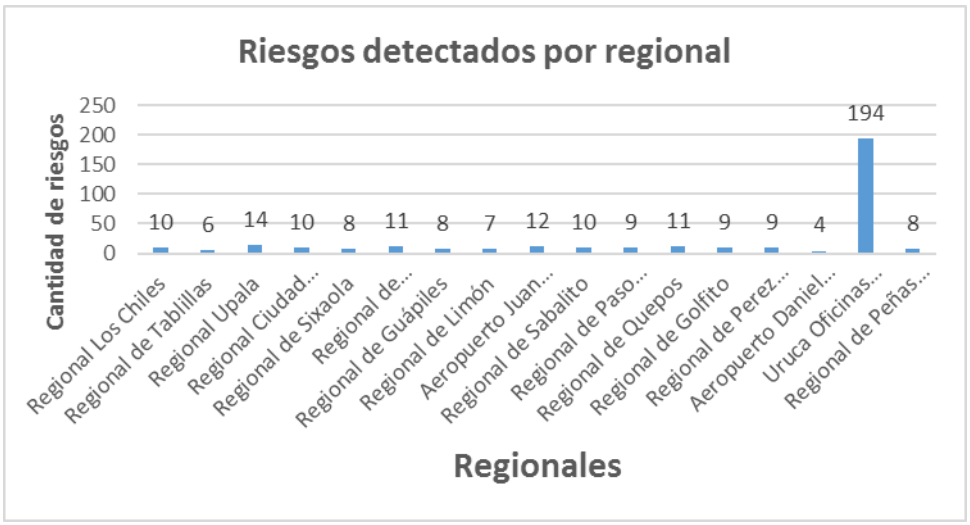

Figura 3. Riesgos de seguridad de la información por Regional detectados en la DGME.
Confección propia.

En total, se detectaron 340 riesgos, es importante recalcar que la mayoría de estos fueron detectados en las oficinas centrales de La Uruca, debido a la gran cantidad de activos lógicos y físicos de la información críticos que ahí se encuentran ubicados.

La Figura 4, muestra los riesgos detectados según la categoría del riesgo.

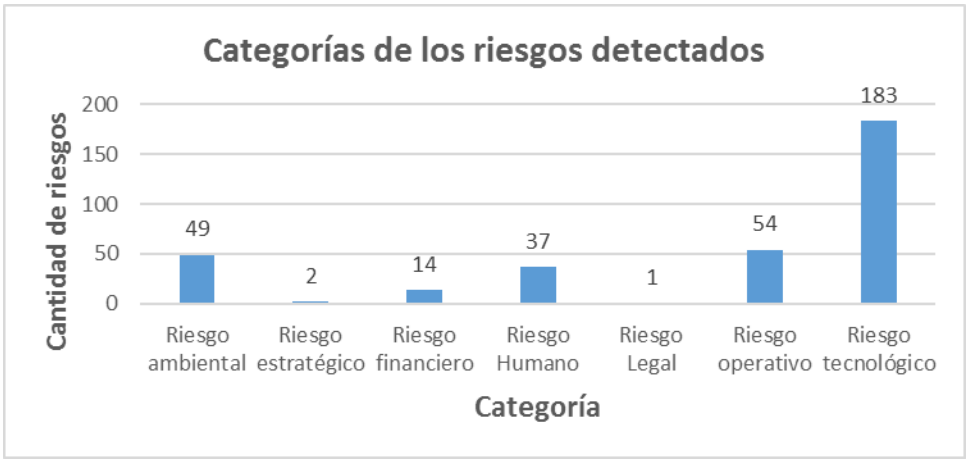

Figura 4. Categorización de los riesgos detectados en la DGME.
Confección propia.

En esta Figura 4 es importante acotar el hecho de que algunos riesgos pueden poseer varias categorías, por ejemplo, por la figura pública y las funciones que cumple la DGME para la ciudadanía costarricense y extranjera, la materialización de los riesgos puede traducirse en riesgos de categoría legal y estratégicos, debido al impacto que estos pueden tener, traduciéndose en demandas legales o recursos de amparo que afectan significativamente los objetivos estratégicos de la Institución.

En la Figura 5, se muestran los riesgos detectados por el origen del riesgo en sí mismo, siendo estos internos o externos a la Institución.

Figura 5. Orígenes de los riesgos detectados en la DGME.
Confección propia.

6.5. Definición del impacto.

El impacto está definido por la criticidad del activo que se analice, en la Tabla 10 se muestran los criterios de impacto en relación con la afectación o interrupción de los activos críticos de la DGME, así como, a las funciones críticas

de la misma. Estos criterios fueron definidos en conjunto con el proceso de seguridad de la información de la DGME, quienes definieron utilizar criterios cualitativos, debido a que no se cuenta con datos históricos que permitiesen determinar criterios cuantitativos más exactos al momento de analizar los riesgos y sus vulnerabilidades.

Tabla 10
Estados cualitativos del riesgo (Impacto).

Estados para riesgos cualitativo	Descripción	Criterio cualitativo
Muy bajo	No existen daños ni pérdidas importantes para la DGME.	2
Bajo	En algunos casos, puede impactar las operaciones de la DGME; pero las pérdidas en imagen, confianza, financieras u otros, no se ven comprometidos.	4
Moderado	Se pueden presentar pérdidas significantes para la DGME, deben ser tratados de manera inmediata para evitar que los aspectos críticos colmo los operativos y legales sean afectados al corto plazo.	6
Alto	El impacto a las operaciones es mayor, puede afectar el cumplimiento de los objetivos de las partes afectadas, se pueden presentar demandas legales por la prestación de los servicios, así como verse expuesta la DGME a pérdidas financieras importantes, afectando la imagen y percepción de confianza de la Institución.	8
Crítico	No se pueden cumplir con los objetivos institucionales, pudiendo ser sancionada y presentarse pérdidas financieras, de imagen y el no cumplimiento de las responsabilidades	10

Estos estados cualitativos del riesgo fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

6.6. Definición de los criterios de probabilidad de ocurrencia.

La probabilidad es la posibilidad de que una determinada amenaza se materialice, en la presencia o no de controles de seguridad y es importante

recalcar que el análisis de la probabilidad y el impacto determinan el nivel de riesgo de un activo. En la Tabla 11 se presentan los criterios de probabilidad para la DGME.

Tabla 11
Estados cualitativos del riesgo (Probabilidad).

Estados para riesgos cualitativo	Descripción	Probabilidad cualitativa %
Poco probable	Su ocurrencia depende de que ciertos criterios excepcionales se presenten.	20%
Probablemente no suceda	Probabilidad de ocurrencia en algunos casos.	40%
Probable	Puede ocurrir en la mitad de los casos	60%
Altamente Probable	Probabilidad de ocurrencia en la mayoría de los casos	80%
Seguramente suceda	La certeza de que ocurra se puede dar en 100% de los casos	100%

Estos estados cualitativos del riesgo fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

6.7. Determinación del riesgo potencial.

El riesgo potencial es la medida de daño probable sobre un activo una vez materializada una amenaza, existan o no controles de seguridad, determinada por el impacto y la probabilidad.

Para la determinación del riesgo potencial de los activos se utiliza una plantilla de Microsoft Excel que se calcula automáticamente, esta permitirá evaluar todos los riesgos, ubicándolos en el mapa de calor del riesgo. Esta determinación permitirá la priorización de atención de los riesgos, según sea necesario, basándose en la tolerancia al riesgo establecido por la DGME y su estrategia para

el tratamiento del riesgo, mitigándolo, reteniéndolo, evitándolo o transfiriéndolo. Se puede hacer referencia al Anexo F, para verificar el análisis completo de los riesgos.

La definición de los niveles de riesgo se detalla continuación:

Nivel de riesgo alto (Cuadrantes rojos): Los riesgos que se ubiquen en estos cuadrantes cuentan con probabilidades muy altas de que se materialicen, además de un nivel de impacto considerable para la DGME, debido a que puede afectar de manera considerable a los activos y los servicios que esta presta, por ende, el prejuicio en el cumplimento de los objetivos institucionales.

Nivel de riesgo medio (Cuadrantes amarillos): Los riesgos que se ubiquen en estos cuadrantes cuentan con criterios de probabilidad e impacto que resultan entre moderados o altos, la materialización de estos riesgos puede afectar de forma importante los activos y funciones críticas de la Institución.

Nivel de riesgo bajo (Cuadrantes verdes): Los riesgos que se ubiquen en estos cuadrantes cuentan con criterios de probabilidad e impacto bajos, la materialización de estos riesgos puede impactar de forma mínima el cumplimiento de los objetivos de la Institución.

La Figura 6, muestra el mapa de calor, donde se reflejan los resultados del análisis de riesgos efectuado a los activos físicos y lógicos de la Institución.

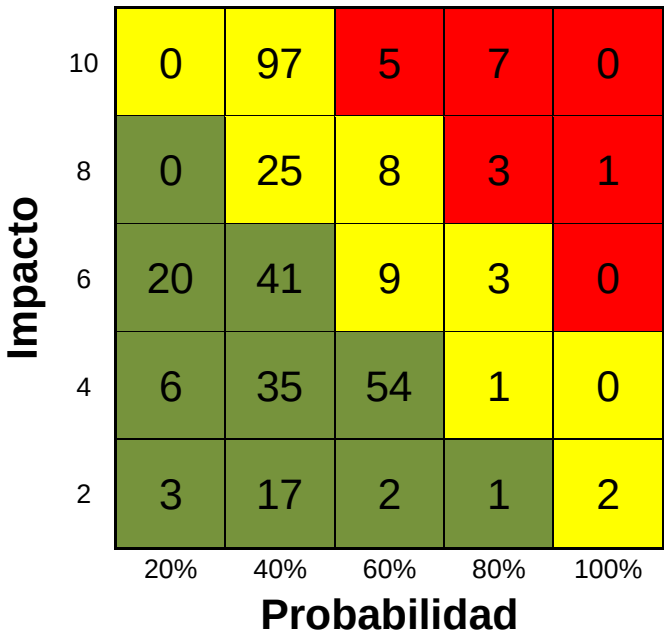

Figura 6. Mapa de calor del análisis de riesgos.
Confección propia.

Analizando la Figura 6, se pueden visualizar los riesgos potenciales detectados según la probabilidad y el impacto anteriormente descritos, en resumen, los riesgos detectados basados en el nivel de riesgo de cada uno se presentan en la Figura 7.

Zona Total: 3	**16**
Zona Total: 2	**145**
Zona Total: 1	**179**
Total de riesgos	**340**

Figura 7. Resumen totalizado de los riesgos detectados según la zona, ubicados en el mapa de calor del análisis de riesgos.
Confección propia

Lo que resulta importante recalcar en la Figura 7, es que los riesgos que deben ser tratados de manera prioritaria son los 16 ubicados en la zona roja de riesgo potencial y los 145 riesgos detectados en la zona amarilla de riesgo potencial y si bien es cierto, los riesgos ubicados en la zona verde de riesgo potencial no son prioritarios para su tratamiento, es importante que se valoren continuamente, al corto, mediano y largo plazo para evitar que estos puedan pasar a niveles de riesgos potenciales más altos y que de esta manera, puedan afectar las funciones críticas de la DGME y por ende, los objetivos estratégicos de la misma.

7. Identificación y análisis de los controles existentes.

Una vez establecidos los riesgos potenciales a los que los activos están expuestos, se valoran los controles existentes para determinar cuáles de estos son claves en la mitigación del riesgo o la amenaza detectada, con el fin de tratar el riesgo según a los requerimientos de la DGME. Para consultar en detalle el análisis de los controles, se puede hacer referencia al Anexo G.

7.1. Clasificación de los controles.

Se presentan en la Tabla 12, los criterios de clasificación de los controles, donde se estableció cuáles son claves para el tratamiento del riesgo y cuáles no lo son, pero que sí pueden brindar medidas de compensación o apoyo a los controles clave de tratamiento del riesgo. Al igual que los criterios de evaluación anteriores, estos fueron definidos en conjunto con el personal del proceso de seguridad de la información de la DGME.

Tabla 12
Criterios de clasificación (CLAVE) de los controles de seguridad.

Criterio	Descripción	Identificador (Color)
Control clave	Este control permite la mitigación adecuada el riesgo o amenaza, siendo indispensable para que el riesgo identificado no se materialice, disminuyendo el impacto a los que el activo de información está expuesto.	Rojo
Control no clave	Estos controles no son claves para la mitigación de los riesgos detectados, pero sí brinda un apoyo fortaleciendo los controles claves.	Verde

Estos criterios de clasificación de los controles fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

En la Figura 8 se muestra la identificación de los controles, definiendo cuáles son claves y cuáles no, para la mitigación de los riesgos identificados.

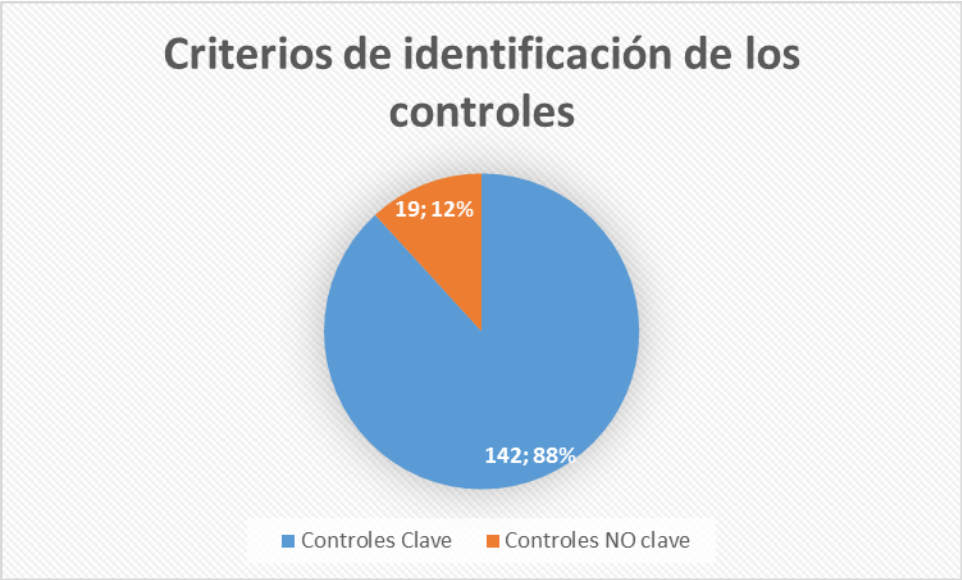

Figura 8. Identificación de los controles Claves y NO Claves de la DGME.
Confección propia.

Como se puede visualizar en la Figura 8, para un tratamiento óptimo del riesgo, es importante verificar que los controles “claves” se ejecuten, debido a que estos permitirán una mitigación adecuada de los riegos o las amenazas identificadas. No menos importantes son los controles “no claves”, que, si bien es cierto, son minoría en la identificación, pero son un complemento en la mitigación de riesgos a los controles “claves”.

7.2. Evaluación de los controles.

Una vez clasificados los controles, se debe evaluar los controles existentes, tomando como referencia su nivel de ejecución, en la Tabla 13 se presentan los criterios de evaluación de estos:

Tabla 13
Criterios de evaluación de los controles.

Criterio de evaluación	Significado	Identificador (Color)

Medida de control inexistente	La efectividad del control es nula para tratar el riesgo.	Rojo
Medida de control pobre	La efectividad del control es inconsistente, ya que no está establecido formalmente y no se da a conocer de manera adecuada a las partes interesadas.	Café
Medida de control adecuada	La efectividad de la media es adecuada y se ejecuta de forma sistemática, pero tiene serios fallos en su divulgación y formalización y no ha sido probada adecuadamente por agentes externos.	Amarillo
Media fuerte de control	La medida se aplica de manera sistemática, se ha probado adecuadamente, pero aún tiene problemas para darse a conocer a las partes interesadas y así su proceso de formalización.	Verde
Medida óptima de control	Se aplica de manera sistematizada, se ha probado y se ha realizado su proceso de divulgación y formalización a todas las partes interesadas.	Verde oscuro

Estos criterios de evaluación de los controles fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

Para la clasificación y evaluación de los controles es importante indicar que solo se evalúan los controles para los riesgos identificados como altos (Rojos) y medios (Amarillos). El detalle de los controles se puede consultar en el Anexo G.

En la Figura 9 se muestra la evaluación de los controles que hace referencia a los criterios anteriormente establecidos.

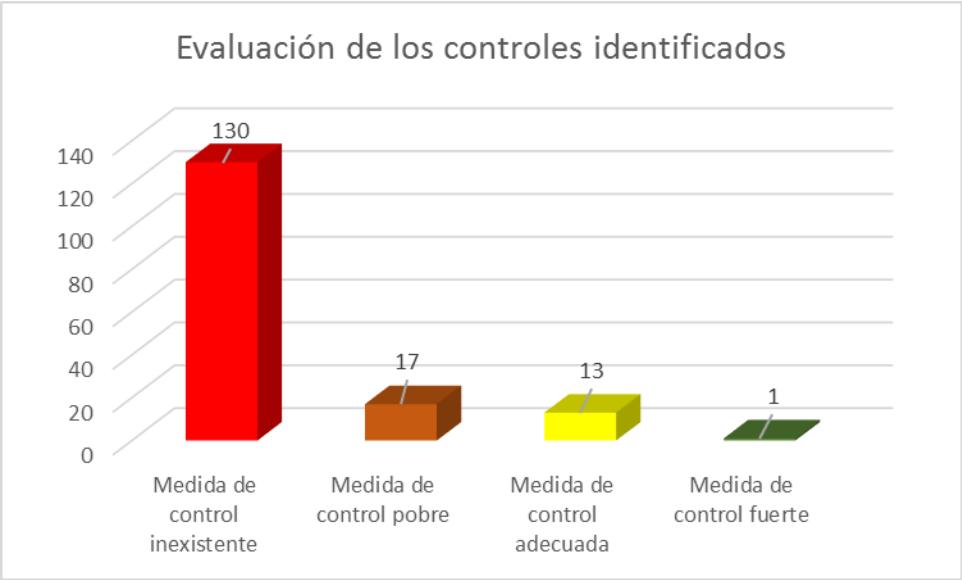

Figura 9. Evaluación de los controles existentes en la DGME.
Confección propia.

Como se puede visualizar en la Figura 9, existe una cantidad muy alta de medidas de control inexistentes y medidas de control pobres, lo que plantea un reto de suma importancia para la DGME, en cuanto al desarrollo de estrategias para el tratamiento óptimo de los riesgos identificados, implementando los controles que se establecen en el presente plan de gestión de riesgos, con el objetivo de llevar estos a niveles más altos como las medidas fuertes de control u óptimas de control. En cuanto a las medidas identificadas como adecuadas, es importante que se trabaje en su divulgación y formalización, para que al igual que las anteriores, puedan llevarse a niveles más altos en cuanto a su evaluación y lograr el tratamiento efectivo de los riesgos identificados.

7.3. Análisis de Costo-Beneficio de los controles.

Se presenta en la Figura 10, la plantilla que mostrará los resultados del análisis de costo-beneficio que se lleva a cabo para cada control, sus detalles completos se pueden consultar en el Anexo G.

Control	Beneficio	Costo	Calificación.

Figura 10. Plantilla para el análisis de Costo-Beneficio del plan de gestión de riesgos.
Definido por el departamento de tecnologías de la información de la DGME

El beneficio se clasifica según la Tabla 14, tomando los valores, Bajo, Medio, Alto, según el beneficio del control aplicado al riesgo detectado.

Tabla 14
Clasificación del beneficio de los controles.

Nivel	Análisis del Beneficio	Descripción
Bajo	**Escaso**	La ejecución o aplicación del control evita en poco o nada la interrupción de servicio o función critica.
Medio	**Intermedio**	La ejecución o aplicación del control evita la interrupción del servicio o función crítica, pero puede requerir de la aplicación de otros controles para aumentar su beneficio.
Alto	**Considerable**	La ejecución o aplicación del control evita en su totalidad la interrupción del servicio o función crítica para la DGME.

Estos criterios de clasificación del beneficio de los controles fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

En la Figura 11, se muestra el análisis del beneficio de los controles.

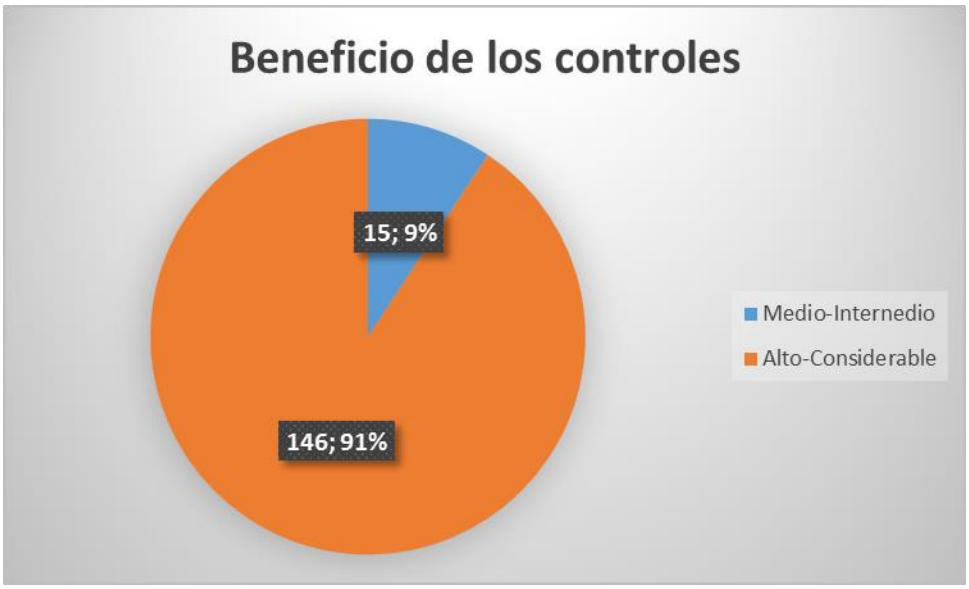

Figura 11. Análisis del beneficio de los controles identificados en la DGME.
Confección propia.

Como se puede visualizar en la Figura 11, el beneficio en la ejecución de los controles establecidos en el presente plan, evitará en su totalidad la interrupción del servicio o función crítica para DGME, con respecto a los 146 controles con beneficio identificados como Altos-Considerable, para el beneficio de los controles identificados como Medio-Intermedio, evitar considerablemente la interrupción de los servicios y funciones críticas de la Institución, pero en algunos casos requerirá la aplicación de otros controles para aumentar su beneficio.

El costo, se clasifica según la Tabla 15, tomando los valores Bajo, Medio, Alto, según el beneficio del control aplicado al riesgo detectado.

Tabla 15
Clasificación del costo de los controles.

Nivel	Análisis del Costo	Descripción
Bajo	**Mínimo**	La inversión en la aplicación del control requiere de un 0 hasta un 1% del total de la partida presupuestaria en que se registra este gasto o inversión.
Medio	**Razonable**	La inversión en la aplicación del control requiere de un

		1 hasta un 5% del total de la partida presupuestaria en que se registra este gasto o inversión.
Alto	**Elevado**	La inversión en la aplicación del control requiere de más de un 5% de la partida presupuestaria en que se registra este gasto o inversión.

Estos criterios de clasificación del costo de los controles fueron definidos en conjunto con el personal del Departamento de Seguridad de la Información de la DGME.

La Figura 12, muestra el resumen del análisis de los costos de los controles.

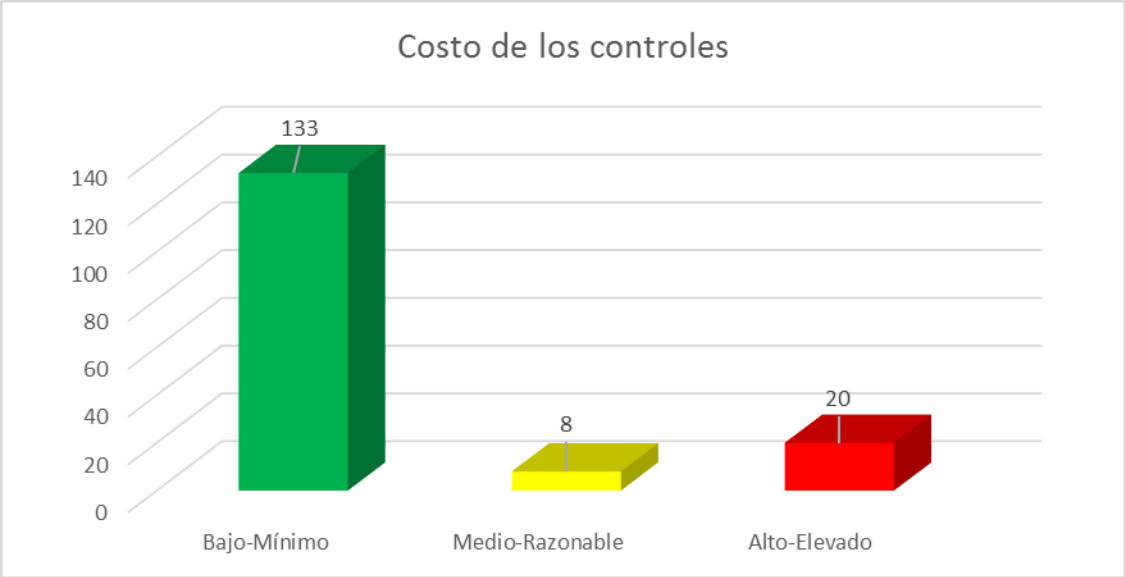

Figura 12. Análisis del costo de los controles identificados en la DGME.
Confección propia.

Lo que refleja el análisis de los costos, como se puede visualizar en la Figura 12, es que la mayoría de los controles, 133 específicamente, tienen un costo identificado como Bajo-Mínimo en su ejecución, esto debido, a que la DGME cuenta con recursos en software y hardware que les permite mitigar de manera óptima los riesgos relacionados con estos controles, los costos identificados como Medio-Razonable y Alto-Elevado, requieren una inversión sustancial, lo que

requiere de un esfuerzo económico considerable por parte de la administración para la ejecución eficiente de estos controles.

Además, para el análisis del costo-beneficio de los controles, se toma en cuenta la información de las partidas presupuestarias del año 2017 de la DGME, mostrados en la Tabla 16.

Tabla 16
Presupuesto de la gestión de las tecnologías de la información 2017.

Código	Partida presupuestaria	Monto	1% del Monto	5% del Monto
1.01.99	Otros alquileres	**1.735.000,00**	17.350,00	86.750,00
1.02.04	Servicio de telecomunicaciones	**93.000.000,00**	930.000,00	4.650.000,00
1.03.07	Servicio de transferencia electrónica de información	**25.000.000,00**	250.000,00	1.250.000,00
1.04.05	Servicios de desarrollo de sistemas informáticos	**55.000.000,00**	550.000,00	2.750.000,00
1.06.01	Seguros	**25.000.000,00**	250.000,00	1.250.000,00
1.08.03	Mantenimiento de instalaciones y obras	**1.500.000,00**	15.000,00	75.000,00
1.08.06	Mantenimiento y reparación de equipo de comunicación	**56.800.000,00**	568.000,00	2.840.000,00
1.08.07	Mantenimiento equipo y mobiliario de oficina	**8.000.000,00**	80.000,00	400.000,00
1.08.08	Mantenimiento Equipo de cómputo	**503.780.000,00**	5.037.800,00	25.189.000,00
2.01.99	Otros productos químicos	**4.400.000,00**	44.000,00	220.000,00
2.03.04	Materiales y productos eléctricos,	**7.500.000,00**	75.000,00	375.000,00

	telefónicos y de cómputo			
2.99.05	Útiles y materiales de limpieza	**1.500.000,00**	15.000,00	75.000,00
5.01.04	Equipo y mobiliario de oficina	**225.000,00**	2.250,00	11.250,00
5.01.05	Equipo y programas de cómputo	**343.293.100,00**	3.432.931,00	17.164.655,00
5.99.03	Bienes intangibles	**393.510.000,00**	3.935.100,00	19.675.500,00

Fuente: Información tomada del presupuesto de la DGME.

Para establecer la clasificación del costo, se toman como parámetros los valores establecidos de beneficio en conjunto con el costo, para determinar el valor del Costo-Beneficio para un riesgo en específico, en la Figura 13, se muestra la fórmula utilizada para esta calificación.

Beneficio	Bajo	Costo razonable	Costo alto	Costo alto
	Medio	Costo positivo	Costo razonable	Costo alto
	Alto	Costo positivo	Costo positivo	Costo razonable
		Bajo	Medio	Alto
	Costo			

Figura 13. Análisis del Costo-Beneficio de los controles identificados en la DGME.
Confección propia.

En la Figura 14, se ilustra el resumen del análisis de costo-beneficio.

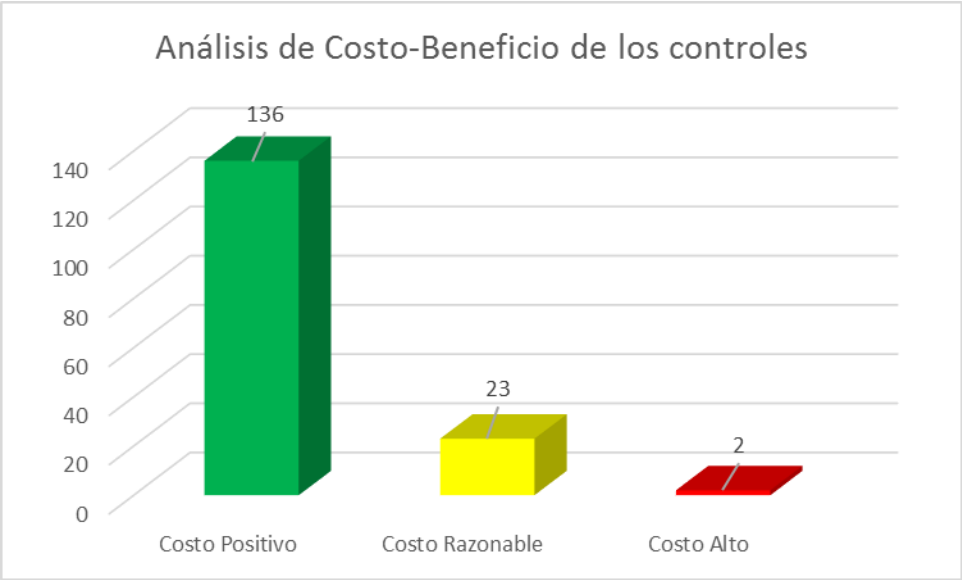

Figura 14. Resumen del análisis de Costo-Beneficio de los controles identificados en la DGME.
Confección propia.

Al analizar los tres gráficos anteriores, se puede determinar una relación lógica en cuanto al análisis del costo-beneficio en la ejecución de los controles propuestos en el presente plan, lo que resulta importante recalcar de la Figura 14 es que la DGME puede mitigar la mayoría de los riesgos con pocos recursos económicos, ya que muchos de estos ya los posee, por lo tanto, el beneficio en la ejecución de estos controles resulta determinante en la mitigación de los riesgos identificados.

8. Identificación de las medidas para el tratamiento de los riesgos.

Una vez establecida la priorización de los riesgos, se determinan las acciones a seguir para tratar los riesgos, las cuales se muestran a continuación.

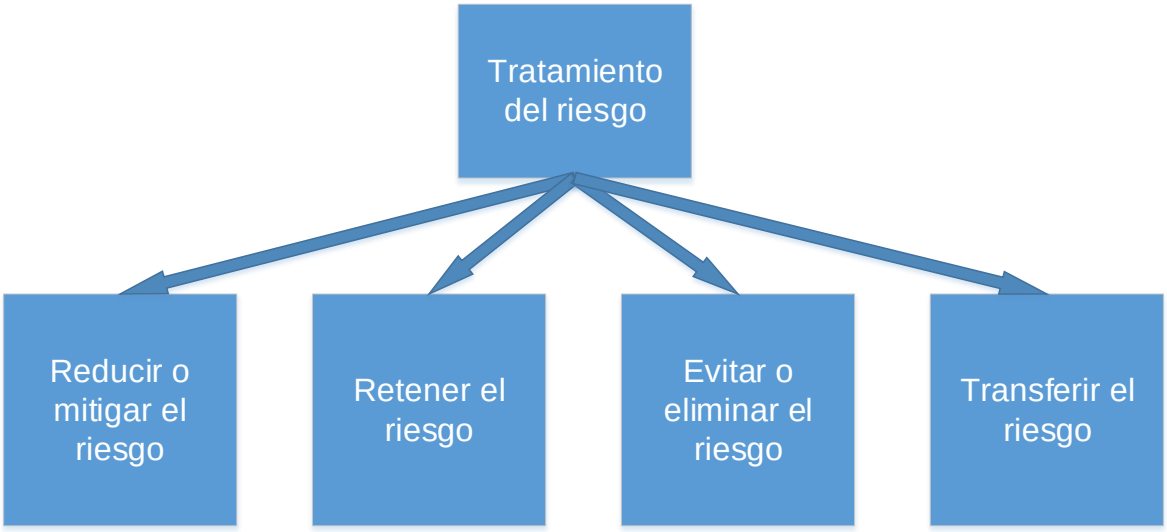

Figura 15. Opciones para el tratamiento de los riesgos.
Según: (ISO, 2011)

8.1. Reducir o mitigar el riesgo.

Este proceso consiste en el establecimiento de los controles que permiten reducir el riesgo, con el objetivo de que el riesgo residual sea aceptado.

8.2. Retener el riesgo.

Este proceso consiste en aceptar el riesgo sin llevar a cabo acciones por parte de la administración de riesgos de la Institución, es importante que queden claramente documentados y que se determinen las responsabilidades, en casos que estos se materialicen.

8.3. Evitar o eliminar el riesgo.

Este proceso consiste en evitar situaciones que pueden materializar un riesgo en específico, puede requerir de modificar el activo que posee el riesgo, lo que conlleva realizar un análisis de riesgos al activo nuevamente.

8.4. Transferir el riesgo.

Este proceso consiste en compartir o transferir el riesgo total o parcialmente con terceros, en la mayoría de los casos la decisión radica en el costo elevado que conlleva que la Institución trate el riesgo por sus propios medios o recursos, pueden estar presente los seguros o contratos para establecer los criterios de la transferencia del riesgo.

9. Establecer los criterios de aceptación del riesgo residual.

Hay que hacer referencia al estado actual de la DGME para determinar diferentes criterios de la aceptación del riesgo residual, en cuanto a la gestión de riesgos de seguridad de la información y los aspectos más importantes que se deben poner en práctica para una administración de la aceptabilidad del riesgo congruente a los objetivos estratégicos de la Institución.

9.1. Sistemas, procesos y objetivos afectados por la exposición del riesgo.

Una vez establecido el análisis del riesgo, como se detalló en el apartado anterior, se ejecuta un estudio donde se analizan los riesgos que se deben atender en primera instancia, determinando cuáles son los procesos y objetivos que están mayormente afectados por los riesgos identificados, una vez determinados, se realiza un procedimiento de priorización y agrupación de estos con el fin de definir el curso a seguir en la administración de riesgos.

9.2. Estado actual de la administración de riesgos de la DGME.

La Institución en la actualidad no cuenta con un departamento de riesgos formalmente establecido y en cuanto a la administración de riesgos de seguridad

de la información, la responsabilidad recae sobre el proceso de seguridad informática, labor que hasta hoy no está documentada ni establecida, por lo tanto, este será uno de los mayores retos para la DGME, implementar el presente plan de gestión de riesgos, para una administración eficiente de los riesgos identificados y la aceptabilidad de los mimos.

Durante esta etapa, se establecen las decisiones relacionadas con los niveles de riesgos aceptados por la DGME y se definen las responsabilidades para con estas decisiones, es importante recalcar que los riesgos aceptados son aquellos que se presenten en el mapa de calor de los riesgos de niveles bajos (verdes) y los que deberán ser atendidos para su tratamiento y mitigación serán los medios y altos (amarillos y rojos). A continuación, se detallan los criterios de aceptabilidad del riesgo.

Nivel de riesgo alto (Cuadrantes Rojos): Los riesgos que se ubiquen en estos cuadrantes deben ser tratados primero, con el objetivo de mitigarlos, disminuyendo su impacto y la probabilidad de que se materialicen, ya que estos representan una afectación a las funciones críticas y a los objetivos estratégicos de la Institución, estos requieren el mayor nivel de inversión y esfuerzo para su tratamiento.

Nivel de riesgo medio (Cuadrantes amarillos): Los riesgos que se ubiquen en estos cuadrantes no representan una afectación altamente negativa a las funciones críticas y estratégicas de la Institución, por lo que deben establecerse

mecanismos de monitoreo y seguimiento para evitar que estos riesgos puedan convertirse en riesgos altos y al igual que los riesgos de nivel alto, la administración debe trabajar en la mitigación de estos riesgos, con el objetivo de disminuir sus niveles impacto y probabilidad.

Nivel de riesgo bajo (Cuadrantes verdes): Los riesgos que se ubiquen en estos cuadrantes requieren la menor inversión de recursos y esfuerzos para su mitigación, pero al igual que los riesgos ubicados en los cuadrantes medios explicados anteriormente, se debe establecer un plan para su monitoreo y seguimiento, con el objetivo de que estos riesgos no pasen a convertirse en riesgos medios o altos.

9.3. Viabilidad de las medidas para la administración de los riesgos.

Una vez que se identifican las medidas para el tratamiento de los riesgos, se procede a realizar, para cada medida, un análisis de costo beneficio.

Otros criterios de viabilidad que se analizan como medida de administración de los riesgos son los siguientes:

- La capacidad del personal en la aplicación de las medidas establecidas.
- Las necesidades de la Institución, con respecto al interés público y al resguardo de la Hacienda Pública.
- La viabilidad operacional y técnica de los procesos que responden a las funciones críticas de la Institución, así como a los aspectos jurídicos, legales y de cumplimiento regulatorio que posee la DGME.

10. Monitoreo y seguimiento.

Es trascendental para la DGME desarrollar programas, planes de revisión, monitoreo y seguimiento, para el debido mantenimiento del presente plan de gestión de riesgos, algunos aspectos importantes a los que la Institución debe prestar atención especial en este proceso de monitoreo y seguimiento son los siguientes:

- Naturaleza de los servicios que brinda la Institución, tanto a los ciudadanos nacionales como a los extranjeros, debido a que estos pueden ser cambiantes con el paso del tiempo, ya sea por legislaciones nacionales o internacionales sobre temas migratorios.
- Efectividad de las medidas de control, por medio de programas de revisión, con el objetivo de la mejora continua en cuanto a la gestión de riesgos, para evitar la desviación en el cumplimiento de los objetivos estratégicos de la Institución y los objetivos estratégicos de las Tecnologías de la Información. Para esto, la DGME puede apoyarse en el cumplimiento legal que establece la Ley de Control Interno, la implementación del SEVRI y el Manual de Normas Técnicas para la gestión y el control de las Tecnologías de Información.
- Evaluación periódica de los riesgos, por medio de programas de revisión, analizando los riesgos y las medidas de control establecidas, para determinar el grado de efectividad en la mitigación de los mismos.

11. Comunicación y divulgación.

La DGME debe desarrollar planes de comunicación y divulgación como parte del proceso de administración de riesgos de seguridad de la información, por medio de su proceso de seguridad, donde se deben considerar los siguientes aspectos:

- Establecer los mecanismos y canales de comunicación de divulgación que abarquen a toda la Institución.
- Establecer los niveles de información a divulgar, definiendo los sujetos interesados para cada nivel de información.
- Desarrollar dinámicas de divulgación, como talleres y planes de capacitación.
- Definir la estructura para la generación de informes y reportes de seguimiento.

Un objetivo primordial de esta etapa es que la Institución brinde espacios al personal para permitirles evacuar dudas referentes a la administración de riesgos de seguridad de la información.

12. Conclusiones.

Mediante el presente proyecto se diseñó el plan de gestión de riesgos de seguridad de la información física y lógica para la Dirección General de Migración y Extranjería, y se confeccionaron y entregaron todas las herramientas para que su gestión pueda ser permanente (estas herramientas se pueden observar en los anexos).

Se identificaron los riesgos lógicos y físicos a los que están expuestos los activos, procesos y objetivos críticos de la DGME, relacionados con la seguridad de la información física y lógica, mediante un listado de los riesgos que pueden afectar la disponibilidad de los servicios que la Institución brinda, enfocándose en la importancia de la disponibilidad, confidencialidad e integridad de la información.

Se revisaron las políticas y procedimientos actuales para el manejo de los riesgos de seguridad de la información, identificando cuáles de estos pueden ser mejorados y estableciendo otros que brinden un marco metodológico para la administración y la gestión de riesgos.

Se analizaron los riesgos de seguridad de la información identificados en el presente plan, estableciendo su adecuado tratamiento, con el objetivo de reducirlo, mitigarlo, retenerlo, evitarlo, eliminarlo o transfiriendo el mismo.

Se construyó el presente plan de gestión de riesgos de seguridad de la información física y lógica, con base en los objetivos estratégicos de la DGME, así como en los objetivos estratégicos del Departamento de Tecnologías de

Información y a las necesidades en cuanto a la gestión de riesgos para la Institución.

13. Recomendaciones

Establecer un plan para la ejecución de los controles expuestos en el presente plan, como parte de la administración de riesgos que requiere la Institución.

Trabajar de manera prioritaria, en la necesidad de capacitar a los funcionarios de la DGME, en cuanto a la administración de riesgos, así como, generar cultura de seguridad de la información.

Capacitar el personal clave de la DGME, en cuanto al manejo de información física almacenada en las oficinas centrales y regionales.

Establecer procedimientos formales, en cuanto a la documentación de políticas y procedimientos en la administración de los activos críticos para la Institución.

Brindar el mantenimiento y seguimiento continuo, así como la debida divulgación del presente plan de gestión de riesgos, que abarque a todos los funcionarios y partes interesadas de la DGME.

Del análisis de los riesgos detectados se puede recomendar complementariamente:

- Aprovechar las herramientas de hardware y software que posee la Institución, para la mitigación de un alto porcentaje de los riesgos.
- Acelerar la puesta en marcha de algunos contratos con proveedores de servicios, que ayudan a la mitigación de algunos riesgos

identificados que afectan actualmente de manera crítica los servicios que brinda la Institución, en el menor plazo de tiempo posible.

- Realizar de manera prioritaria un plan de mejora de las redes y comunicaciones de la DGME, específicamente en el cableado estructurado.
- Acelerar la puesta en marcha del plan de adquisición de un centro alterno para la DGME, este representa un riesgo muy alto y requiere recursos económicos importantes, así como, el compromiso por parte de la administración de la Institución.
- Establecer y documentar claramente las responsabilidades del personal de la DGME, relacionadas con los procesos y funciones críticas de la seguridad de la información.
- Revisar detalladamente el plan de recuperación de desastres (DRP) y el plan de continuidad del negocio (BCP), debido a que presentan importantes incoherencias en los tiempos de recuperación de operaciones críticas, con respecto a los contratos de proveedores, específicamente, en los tiempos de atención de incidentes.
- Acelerar el proceso de actualización de sistemas operativos obsoletos, por ejemplo, sistemas XP y Windows 2003.
- Adquirir los sistemas informáticos de bases de datos los cuales no cuentan con licencias autorizadas, por ende, no pueden recibir mantenimiento ni actualizaciones por parte del fabricante.

Es importante que la DGME continúe con la implementación de todos los controles aquí establecidos, como parte de la gestión de riesgos que pretende impulsar este plan.

14. Bibliografía

Contraloría General de la República. (7 de junio de 2007). Normas técnicas para la gestión y el control de las Tecnologías de Información. (N-2-2007-CO-DFOE). San Jose, San Jose, Costa Rica.

Direccion General de Migración y Extranjería. (01 de abril de 2017). *Direccion General de Migración y Extranjería*. Obtenido de Direccion General de Migración y Extranjería: www.migracion.go.cr

Extranjería, D. G. (2017). Presupuesto Ordinario 2017. Uruca, San Jose, Costa Rica.

Guía de gestión de riesgos. (01 de abril de 2016). *MINTIC*. Obtenido de Seguridad y privacidad de la información: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

INTECO. Instituto de Normas Técnicas de Costa Rica. (04 de noviembre de 2011). Gestión del riesgo. Principios y directrices. (INTE/ISO 31001:2011). (Inteco, Ed.) San Jose, San Jose, Costa Rica.

ISACA. (2013). COBIT 5 Gestión de Riesgos. *COBIT 5 para Riesgos*. Illinois, USA.

ISO. (30 de marzo de 2011). *International Organization for Standardization*. Obtenido de ISO: https://www.iso.org/home.html

Martínez, E. A. (marzo de 2013). Informe de evaluación y control de riesgos. Uruca, San Jose, Costa Rica.

Solano, O. C. (enero de 2016). Informe de Resultados - Análisis de Impacto. *Consultoría para la implementación de un sistema de Gestión de Continuidad de Negocio (SGCN)*. Uruca, San Jose, Costa Rica.

Solano, O. C. (setiembre de 2016). Plan de Recuperación ante Desastres DGME. *Consultoría para la implementación de un sistema de Gestión de Continuidad de Negocio (SGCN)*. Uruca, San Jose, Costa Rica.

Solano, O. C. (febrero de 2017). Estrategia y programa de seguridad de la infomación Dirección General de Migración y Extranjería. *Consultoría para la implementación de las Normas Técnicas*. Uruca, San Jose, Costa Rica.

15. Anexos

Anexo 1. Lista de fuentes consultadas.

Bases consultadas para la toma de información
Motor de búsqueda: ISO Store **URL:** https://www.iso.org/store.html **Fecha de la consulta:** 30 de marzo, 2017
Motor de búsqueda: INTECO **URL:** https://www.inteco.org/page/homepage **Fecha de la consulta:** 30 de marzo, 2017
Motor de búsqueda: COBIT Online **URL:** http://www.isaca.org/cobit/pages/default.aspx **Fecha de la consulta:** 30 de marzo, 2017

Anexo 2. Lista de fuentes seleccionadas.

Lista de los documentos que se utilizaron
Título: ***COBIT 5 para Riesgos*** ***USA*** **Autor: ISACA** **Tipo: Marco de gestión de riesgos** **Descripción: Este documento es una referencia como recurso educativo para los profesionales de aseguramiento de ISACA.**
Título: Gestión del riesgo. Principios y directrices **Costa Rica** **Autor: INTECO. Instituto de Normas Técnicas de Costa Rica** **Tipo: Marco de gestion.** **Descripción: Este documento presenta una recomendación para la administracion y gestion de riesgos, principios y directrices, el cual es equivalnete a la norma ISO 31000:2009.**
Título: Gestión de Riesgos – Principios y Guías **Suiza** **Autor: ISO Org.** **Tipo: Norma Internacional.** **Descripción: Este documento presenta una recomendación para la administracion y gestion de riesgos, principios y directrices.**

Anexo 3. Detalles del documento.

Nombre del documento: Plan de Gestión de Riesgos de seguridad de la información DGME.

Nombre del archivo: Plan de Gestión de Riesgos de seguridad de la información DGME.docx

Personal fiscalizador de parte de la DGME.

Lic. Oscar Jiménez, encargado del sub-proceso de seguridad de TI.

Lic. Jenny Gamboa, encargada de departamento de TI.

Persona que elabora el Plan de Gestión de Riesgos.

Ing. Bayardo Hernández N, consultor en seguridad de la información.

Anexo 4. Dependencias de los activos críticos de información.

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
Sistema de información	• Cardex • Sistema API • Sistema de extranjería (SINEX) • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema de visas • Sistema de policía • Web Services de SINEX-CARDEX • Web Services • Sistema de Información Policial	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505	Sybase15.7	Extranjeros
Sistemas bases de	• Sistema	• Servidor	Switches	• Sybase	• Movim

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
datos	Cardex • Sistema Web-Services Impedimentos de salida • Sistema API • Sistema de Menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de policía • Sistema de gestión de migraciones • Sistema de Refugio • Sistema de Visas • Sistema de extranjería (SINEX) • Sistema de Bancos • Sistema de Seguridad • Sistema de Almacén • Sistema de devolución de depósitos • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiado • Sistema SICOVI	Solaris versión 9 192.168.120.250 • Servidor físico Dirección IP 192.168.121.250 • Sistema Operativo SUN Fire 480-R254.11 • Dirección IP 172.16.254.10 Windows 7 SP1 • Dirección IP 172.16.254.11 Windows 7 SP1 • Nombre le equipo CARDEX 192.168.121.103 Windows Server 2003 R2 • Nombre del servidor AFIS1 192.168.121.101 Windows 2003 Server R2 • Nombre del servidor AFIS2 192.168.121.102 Windows 2003 Server R2 • Nombre del servidor SINEX-CARDEX 10.10.10.6 Windows	• 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 TippingPoint x505	15.7 • Oracle 10g R2 • SQL Server 2005 y 2008	ientos • Extranjeros • General • Sinex-Cardex • Certificaciones • Financiero • Estado • Seguridad • Administrativo • SISPAS

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
		Server 2003 Server			
Sistema de información WEB	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de pasaportes (SISPAS). • Web Services de Pasaportes • Web Services de SINEX-CARDEX • Web Services • Sistema de Información Policial	• Servidores PP1 Y PP2 • Dirección IP PP1 10.10.10.5 Windows Server 2003 • Dirección IP 10.10.10.4 Windows Server 2003 • BCR-GDME-GOV-DIGITAL	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505	• Sybase 15.7 • Oracle 10g R2	• Movimientos • General • Extranjeros
Sistema Web Services de Pasaportes	• Sistema de gestión de migraciones • Sistema de	• Servidores PP1 Y PP2 • Dirección IP PP1	Switches • 4 equipos Marca: 3Com	• Oracle 10g R2	• Sinex-cardex

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	información • Sistema de información WEB • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema SISCAP • Sistema visor de pasaportes • Web Services Sistema de Información Policial	10.10.10.5 Windows Server 2003 • Dirección IP PP1 10.10.10.7 • 10.10.10.250 Windows 7 • Base de datos 10.10.10.6 Windows Server 2003 • Dirección IP 10.10.10.4 Windows Server 2003 • BCR-GDME-GOV-DIGITAL.	Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema Web Services Impediments de Salida	• Sistema Cardex • Sistema API • Sistema de extranjería (SINEX) • Sistema de información • Sistema de menores	• Dirección IP 172.16.254.10 Windows 7 SP1 • Dirección IP 172.16.254.11 Windows 7 SP1	Switches • Marca: 3Com Modelo: 4400SE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo:	• SQL 2005	• Conexión al Poder Judicial

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	• Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema de visas • Sistema de policía • Sistema SISCAP • Web Services de Pasaportes • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados • Web Services Sistema de Información Policial		2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 5500G • Marca: 3COM Modelo: 4400SE • Marca: 3COM Modelo: 4400SE • Marca: H3C Modelo: 7510		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Marca: HUB Modelo: CentreCom • Marca: 3COM Modelo: 4400 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • Marca: 3COM Modelo: 5232 • Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Cisco 5510 • TippingPoint x505		
Sistema API	• Sistema de extranjería (SINEX) • Sistema de información • Sistema de información WEB • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de policía • Sistema SISCAP • Web Services de • Pasaportes • Web Services • Impedimento s de Salida • Web Services de SINEX-CARDEX • Web Services • Sistema de Información Policial	• Servidores PC ARINC. Windows XP SP1 • 129.13.0.112 • ROBOT: Servidores (PC) SITA. Windows 7 SP1 • 129.13.0.114 • Sybase 129.13.0.178	Switches • Marca: 3Com Modelo: 4400SE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 3100 • Marca: H3C	Sybase 15.7	• Movim ientos

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			Modelo: 5500G • Marca: 3COM Modelo: 4400SE • Marca: 3COM Modelo: 4400SE • Marca: H3C Modelo: 7510 • Marca: HUB Modelo: CentreCom • Marca: 3COM Modelo: 4400 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Marca: 3COM Modelo: 5232 • Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de menores	• Sistema API • Sistema de movimiento migratorio (SIMMEL). • Web Services de Pasaportes • Web Services Impedimentos de Salida • Web Services de SINEX-CARDEX • Sistema Visor de pasaportes	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2 • Servidor AIJS dirección IP 172.16.24.36	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM	Sybase 15.7	• Movimientos • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de movimiento migratorio electrónico (SIMMEL).	• Sistema Cardex • Sistema API • Sistema de extranjería (SINEX) • Sistema de información • Sistema de menores • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema de visas • Sistema de policía • Sistema SISCAP • Web Services de Pasaportes • Web Services de SINEX-CARDEX • Sistema de bancos • Sistema de gestión de migraciones • Sistema devolución de depósitos • Sistema de impresión de Permisos vecinales, Carné	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c	Sybase 15.7	• Movimientos • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	Temporal de Refugiados • Web Services de SINEX-CARDEX • Web Services Sistema de Información Policial		• Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de Policía	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de información • Sistema de movimiento migratorio (SIMMEL). • Sistema de refugio • Sistema de visas • Web Services Sistema de Información Policial	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610	• Sybase 15.7	• Extranjeros • Movimientos • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de gestión de migraciones	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de información • Sistema de información WEB • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema de visas • Sistema de policía • Web Services de Pasaportes SINEX-CARDEX • Sistema de bancos • Sistema de devolución de depósitos • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados • Web Services de SINEX-CARDEX	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2. • Servidor físico Dirección IP 192.168.121.250 • Sistema Operativo SUN Fire 480-R	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505	Sybase 15.7	• Extranjeros • Movimientos • General • SISPAS

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	• Web Services Sistema de Información Policial • Web Services Impedimento s de Salida				
Sistema de Pasaportes (SISPAS).	• Sistema de gestión de migraciones • Sistema de movimiento migratorio (SIMMEL). • Web Services de Pasaportes • Sistema de bancos • Sistema devolución de depósitos • Sistema visor de pasaportes • Web Services de SINEX-CARDEX • Web Services Sistema de Información Policial	• Servidor físic 192.168.121. • Sistema Ope	Switches • Marca: 3Com Modelo: 4400SE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 3100	Oracle 10g R2	SISPAS

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 5500G • Marca: 3COM Modelo: 4400SE • Marca: 3COM Modelo: 4400SE • Marca: H3C Modelo: 7510 • Marca: HUB Modelo: CentreCom • Marca: 3COM Modelo: 4400 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • Marca: 3COM Modelo: 5232 • Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 TippingPoint x505		
Sistema de recursos humanos	Marcas	Servidor antiguo para consultas del sistema anterior • Nombre del servidor: Turrialba • Dirección IP 192.168.121.25 consulta • Servidor SUN x2200(virtual) • Vmware físico versión 5.0 • Sistema operativo Windows XP SP3 Servidor nuevo de Marcas • Dirección IP 192.168.121.186 • Nombre del servidor:	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo:	MySQL y ACCESS	Marcas

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
		Marcas • Servidor Físico con sistema operativo Windows 2003 SP1	2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de refugio	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de información • Sistema de movimiento migratorio (SIMMEL). • Sistema de visas • Sistema de policía • Web Services Impedimentos de Salida • Web Services de SINEX-CARDEX • Sistema de bancos • Sistema de gestión de migraciones • Sistema de devolución de depósitos • Web Services de SINEX-	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca:	Sybase 15.7	• Extranjeros • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	CARDEX • Web Services Sistema de Información Policial		3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de visas	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de información • Sistema de movimiento migratorio (SIMMEL). • Sistema de refugio • Sistema de policía • Sistema de devolución de depósitos • Web Services • Sistema de Información Policial	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2 • No posee alta disponibilidad.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610	Sybase 15.7	• Extranjeros • General • Financiero

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de información SharePoint		• Servidor Vcenter • Hojas Blade de la 2 a la 7 • 13 servidor • Rango de direcciones IP 10.200.201.17 – 35 • Sistema operativo Windows 2012 R2 standard	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
Sistema Interpol	• Sistema Cardex • Sistema API • Sistema de extranjería (SINEX) • Sistema de información • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema de visas • Sistema de policía • Sistema SISCAP • Web Services de Pasaportes • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados • Web Services Sistema de Información Policial	• Dirección IP 172.16.254.10 Windows 7 SP1 • Dirección IP 172.16.254.11 Windows 7 SP1.	Switches • Marca: 3Com Modelo: 4400SE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 2928 POE • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 3100 • Marca: H3C Modelo: 5500G • Marca:		Web-Services Consulta servicio Interpol

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			3COM Modelo: 4400SE • Marca: 3COM Modelo: 4400SE • Marca: H3C Modelo: 7510 • Marca: HUB Modelo: CentreCom • Marca: 3COM Modelo: 4400 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 5500G • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 • Marca: H3C Modelo: 7510 Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • Marca: 3COM Modelo:		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• 5232 • Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 TippingPoint x505		
Sistema de extranjería (SINEX)	• Sistema Cardex • Sistema de información • Sistema de información WEB • Sistema de movimiento migratorio (SIMMEL). • Sistema de refugio • Sistema de visas • Sistema de policía • Web Services Impedimentos de Salida • Web Services de SINEX-CARDEX • Bancos • Sistema de migraciones. • Devolución de depósitos • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados • Web	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco	Sybase 15.7	• Extranjeros • General • Movimientos

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	Services de SINEX-CARDEX • Web Services Sistema de Información Policial		Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de correo electrónico institucional (Zimbra)		• Servidor Virtual • Vcenter • Dirección IP 10.200.201.10 y 10.200.201.11 • Sistema Operativo CentOS Linux	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• TippingPoint x505		
Sistema Cardex	• Sistema de extranjería (SINEX) • Sistema de información • Sistema de información WEB • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de refugio • Sistema de policía • Web Services Impedimentos de Salida • Web Services de SINEX-CARDEX • Bancos • Sistema de migraciones (CORREOS) • Devolución de depósitos • Sistema de impresión de Permisos vecinales. • Web Services de SINEX-CARDEX • Web Services Sistema de Información Policial	• Servidor de procesamiento físico HP Cardex ESX01 (con 4 virtuales). • Servidor de procesamiento físico HP Cardex ESX02 (con 4 virtuales). • Sistema que administra: ESX 5.1. • Sistema operativo Windows 2003 R2 SP2 en los 4 servidores • Direcciones IP´s 192.168.121.101 Windows Server 2003 R2 SP2 • 192.168.121.102 Windows Server 2003 R2 SP2 • 192.168.121.103 Windows Server 2003 R2 SP2 • 192.168.121.104 Windows Server 2003 R2 SP2	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505	SQL Server 2005	• CARDEX • Estado
Sistema control de accesos		• Servidor con la dirección IP 172.24.40.10	Switches • 4 equipos Marca: 3Com		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
		. • Sistema Operativo Windows XP SP3	Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de Bancos	• Cardex • Sistema de extranjería (SINEX) • Sistema de gestión de migraciones • Sistema de información • Sistema de	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G	• Sybase 15.7	• Extranjeros • Financiero • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de visas • Sistema policía • Sistema de migraciones (correos) • Devolución de depósitos • Sistema de refugio		• 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema de seguridad	• Sistema Cardex • Sistema de información • Sistema de información WEB • Sistema de movimiento migratorio (SIMMEL). • Sistema de refugio • Sistema de visas • Sistema de	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C	• Sybase 15.7	• Movimientos • Extranjeros • General • Sinex-Cardex • Certificaciones • Financiero • Estado • Seguri

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	policía • Web Services Impedimentos de Salida • Web Services de SINEX-CARDEX • Bancos • Sistema de migraciones. • Devolución de depósitos • Sistema de impresión de Permisos vecinales, Carné Temporal de Refugiados • Web Services de SINEX-CARDEX • Web Services Sistema de Información Policial		Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		dad • Administrativo • SISPAS •
Servidor de Carpetas compartidas usuarios DGME	• Todos los equipos de usuarios que posean carpetas compartidas	• Servidor Virtual en SVMware • Dirección IP 192.168.121.32 • Sistema Operativo Windows 2003 Server SP2 • Servidor Base_NLB1 • Dirección IP 192.168.122.231. • Sistema operativo Windows 2008 R2 SP1	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo:		

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
		• Servidor Radius Dell 2950	3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema SISCAP	• Sistema API • Sistema de información • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Web Services Sistema de Información Policial	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco	• Sybase 15.7	• Movimientos • General

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		
Sistema Almacén		• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos	• Sybase 15.7	• General • Financiero

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610		
Sistema de devolución de depósitos	• Cardex • Sistema de extranjería (SINEX) • Sistema de gestión de migraciones • Sistema de información • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de visas • Sistema policía • Sistema de migraciones (correos) • Devolución de depósitos • Sistema de refugio	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510	• Sybase 15.7	• Extranjeros • Financiero

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
			• TippingPoint x505		
Sistema WEB Visor de pasaportes	• Pasaportes	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 TippingPoint x505	• Oracle 10g R2	• SISPAS
Web Services de SINEX-CARDEX	• Sistema de gestión de migraciones • Sistema de	• Servidores PP1 Y PP2 • Dirección IP PP1	Switches • 4 equipos Marca: 3Com	• SQL 2008	• SINEX-CARDEX

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	información • Sistema de información WEB • Sistema de menores • Sistema de movimiento migratorio (SIMMEL). • Sistema de pasaportes (SISPAS). • Sistema de refugio • Sistema SISCAP • Sistema visor de pasaportes • Web Services Sistema de Información Policial	10.10.10.5 Windows Server 2003 • Dirección IP PP1 10.10.10.7 • 10.10.10.250 Windows 7 • Base de datos 10.10.10.6 Windows Server 2003 • Dirección IP 10.10.10.4 Windows Server 2003 • BCR-GDME-GOV-DIGITAL	Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G • 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 TippingPoint x505		
Web Services Sistema de Información Policial	• Sistema Cardex • Sistema de extranjería (SINEX) • Sistema de información • Sistema de movimiento migratorio	• Servidor de aplicaciones Dirección IP 192.168.120.15 • Sistema Operativo Windows Server 2003 R2 SP2.	Switches • 4 equipos Marca: 3Com Modelo: 4400SE • 11 equipos Marca: H3C Modelo: 5500G	• Sybase 15.7 • Oracle 10g R2	• SISPAS • Extranjeros

Aplicación o sistema	Aplicaciones que dependen	Servidores que lo contiene	Equipos de comunicación switches y routers.	Base de datos utilizada	Servidor de base de datos
	(SIMMEL). • Sistema de refugio • Sistema de visas • Web Services Sistema de Información Policial		• 2 equipos Marca: H3C Modelo: 2928 POE • 8 equipos Marca: H3C Modelo: 7510 • 2 equipos Marca: H3C Modelo: 3100 • Marca: HUB Modelo: CentreCom Routers • Marca: Cisco Modelo: 2651XM • Marca: H3C Modelo: MSR30-16 • 2 equipos Marca: 3COM Modelo: 5232 • Marca: Cisco Modelo: 2610 • Fortigate 60c • Cisco 5101 • Cisco 5510 • TippingPoint x505		

Anexo 5. Definición de los riesgos y sus vulnerabilidades

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R001	Fallo de enlace principal de red	Existe un rack de comunicación con gabinete, el cual se mantiene con la lleve puesta y puede tener acceso a este fácilmente	Riesgo tecnológico	Cualquier persona que este al interior en las instalaciones puede desconectar los cables o el enlace que posee la regional a oficinas centrales de la DGME y no existe enlace redundante.	Caída del enlace de red de los sistemas de la DGME, así como la afectación de los servicios y operaciones críticas que brinda la regional.	Regional Los Chiles	Interno
R002	Acceso físico no autorizado	No existen dispositivos de control de acceso a ninguna de las oficinas de la regional.	Riesgo humano	Cualquier persona no autorizada puede ingresar a cualquier oficina de la regional, ya que estas a aparte de carecer de control de acceso, siempre se mantienen abiertas y sin ningún tipo de bloqueo.	Afectación o daño del hardware de la Institución, así como pérdida de información física, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Los Chiles	Externo
R003	Fallo de red de los equipos institucionales de los usuarios	El cableado estructurado de la mayoría de los equipos es deficiente	Riesgo tecnológico	La exposición del cableado de red de los equipos y una mala manipulación de estos	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Los Chiles	Interno
R004	Peligro de incendio	Existe una gran cantidad de cajas de papel en condiciones que promueven la posibilidad de un incendio.	Riesgo ambiental	Se encuentran en la planta baja y no existe ningún sistema de supresión de incendios en este lugar.	Perdida humana y de toda la infraestructura de la regional, así como de la información física que esta posee, así como la	Regional Los Chiles	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					afectación de los servicios y operaciones críticas que brinda la regional		
R005	Fallo en el suministro eléctrico	Fallo en el fluido eléctrico	Riesgo operativo	Caída en el sistema eléctrico de la zona de los Chiles de San Carlos	Afectación servicio y operaciones críticas que brinda la regional.	Regional Los Chiles	Externo
R006	Ingreso de personal no autorizado	Inexistencia de sistemas de control de acceso	Riesgo humano	Entrada forzada de personas a las instalaciones de la regional.	Daño o afectación de los recursos de hardware de la regional, así como robo o daño de la información física, así como la afectación de los servicios y operaciones críticas que brinda la regional.	Regional Los Chiles	Externo
R007	Robo de información confidencial	La información física almacenada no se mantiene bajo llaves en los archiveros que la contienen	Riesgo humano	Cualquier persona o usuario de la regional, puede acceder a la información que almacena la regional	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Los Chiles	Externo
R008	Acceso físico no autorizado	Algunas paredes de la regional son de Gypsum, así como algunas ventanas no cuentan con verjas o portones.	Riesgo humano	Entrada forzada de personas a las instalaciones de la regional.	Daño o afectación de los recursos de hardware de la regional, así como robo o daño de la información física, así como la afectación de los servicios y operaciones críticas que brinda la regional.	Regional Los Chiles	Externo
R009	Alta humedad	La alta humedad puedo generar	Riesgo ambiental	Ante los altos niveles de humedad puede	Daño o afectación de los recursos de	Regional Los Chiles	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		deterioro de los activos de los activos de información física de la regional.		generar pérdida de información física en papel, así como el deterioro del hardware informático, no existen detectores de humedad.	hardware de la regional, así como robo o daño de la información física, así como la afectación de los servicios y operaciones críticas que brinda la regional.		
R010	Fallo de equipos informáticos	La ubicación de algunos equipos como UPS no están ubicadas en lugares óptimos para su correcto funcionamiento	Riesgo tecnológico	La UPS de rack que soporta todos los equipos de la regional está ubicada en un estante metálico	Daño o afectación de los recursos de hardware de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional.	Regional Los Chiles	Externo
R011	Fallo de enlace principal de Red	Existe un rack de comunicación con gabinete, el cual se mantiene con la lleve puesta y puede tener acceso a este fácilmente	Riesgo tecnológico	Cualquier persona que esté en el interior en las instalaciones puede desconectar los cables o el enlace que posee la regional a oficinas centrales de la DGME y no existe enlace redundante.	Caída del enlace de red de los sistemas de la DGME, así como la afectación de los servicios y operaciones críticas que brinda la regional.	Regional de Tablillas	Interno
R012	Acceso físico no autorizado	No existen dispositivos de control de acceso a ninguna de las oficinas de la regional.	Riesgo humano	Cualquier persona no autorizada puede ingresar a cualquier oficina de la regional, ya que estas a aparte de carecer de control de acceso, siempre se mantienen abiertas y sin ningún tipo de bloqueo.	Afectación o daño del hardware de la Institución, así como pérdida de información física, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Tablillas	Externo
R013	Peligro de incendio	Existe una gran cantidad de cajas de papel en condiciones	Riesgo ambiental	Estos archivos se encuentran ubicados en diversos lugares	Pérdida humana y de toda la infraestructura	Regional de Tablillas	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		que promueven la posibilidad de un incendio.		donde están almacenados de manera adecuada, los extintores no se les dan mantenimiento desde 2014	de la regional, así como de la información física que esta posee, así como la afectación de los servicios y operaciones críticas que brinda la regional		
R014	Fallo en el suministro eléctrico	Fallo en el fluido eléctrico	Riesgo operativo	Caída en el sistema eléctrico de la zona de los Chiles de San Carlos	Afectación servicio y operaciones críticas que brinda la regional. La UPS está en mal estado y no se posee planta eléctrica.	Regional de Tablillas	Externo
R015	Robo de información confidencial	La información física almacenada no se mantiene bajo llaves en los archiveros que la contienen	Riesgo humano	Cualquier persona o usuario de la regional, puede acceder a la información que almacena la regional	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Tablillas	Externo
R016	Fallo en equipos informáticos	Daño en equipos informáticos de usuarios finales, ya que existen aires acondicionados sobre estos equipos	Riesgo tecnológico	En caso de que un aire acondicionado derrame agua sobre uno de los equipos puede dañarlo	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Tablillas	Interno
R017	Inundaciones	La oficina se encuentra a 200 metros del río	Riesgo ambiental	Se han presentado crecidas del río que han llegado hasta la regional	Pérdida de equipos de hardware, así como pérdida de información física, y en los casos más críticos podría presentar pérdidas humanas	Regional Upala	Externo
R018	Fallo en el fluido eléctrico	Fluido eléctrico falla constantement	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la	Daño en el hardware de los equipos	Regional Upala	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		e		zona de Upala	informáticos y de los equipos de comunicación		
R019	Acceso físico no autorizado	No hay sistemas de control de acceso a la regional	Riesgo humano	Cualquier persona puede ingresar al edificio y sus oficinas.	Daño, robo de activos informáticos, así como la posibilidad de pérdida de archivos físicos.	Regional Upala	Externo
R020	Daño o pérdida de información física	Aires acondicionados instalados sobre archiveros de información física	Riesgo legal	En caso de que los aires acondicionados derramen aguda pueden dañar los archivos físicos de información.	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Upala	Interno
R021	Fallo de hardware	Ubicación de los equipos de comunicación	Riesgo tecnológico	Los equipos de comunicación se encuentran sobre un archivero y puede ser manipulado fácilmente	Fallo en el router o switch de comunicación	Regional Upala	Interno
R022	Incendio	Archiveros físicos ubicados en lugares no adecuados	Riesgo ambiental	Los archivos están almacenados en estantes cubiertos por una cortina de tela	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Upala	Interno
R023	Robo de hardware	Las instalaciones físicas de la regional no cuentan con medidas de seguridad necesarios para persuadir a delincuentes	Riesgo financiero	Se han presentado robos de equipos informáticos de usuarios en los últimos años y no se cuenta con alarma contra intrusiones	Pérdida de equipos informáticos, así como la información lógica de estos	Regional Upala	Externo
R024	Acceso físico no autorizado	Equipos de atención al cliente pueden ser manipulados por personal no autorizado	Riesgo operativo	El mostrador de servicio al cliente posee una puestilla que se mantiene abierta y es de fácil acceso por personal no	Pérdida o daño de equipo informático	Regional Upala	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				autorizado			
R025	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular el equipo	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional Upala	Interno
R026	Fallo en equipos informáticos	Equipos instalados a nivel del suelo	Riesgo operativo	En caso de inundación los equipos este puede alcanzar los equipos fácilmente	Daño al hardware y software de los equipos de usuarios	Regional Upala	Interno
R027	Incendio y material peligroso para el hardware	Debido a que no existe una barrera física entre los equipos y otros materiales, el equipo se expone a materiales de alto riesgo.	Riesgo operativo	Los equipos están ubicados en condiciones no adecuados, con archivos, papel cartón entre otros.	Destrucción o daño de los activos: inmobiliarios, infraestructura tecnológica, documentos, entre otros, de la oficina afectada.	Regional Upala	Interno
R028	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional Upala	Externo
R029	Falla de hardware de red de los equipos de usuarios	Por la ubicación del switch de comunicaciones, este puede ser manipulado y dañado.	Riesgo tecnológico	Debido a la ubicación del switch este puede ser manipulado por cualquier funcionario de la regional	Se puede apagar el equipo fácilmente, o desconectar físicamente cualquiera de las estaciones de trabajo	Regional Upala	Interno
R030	Pérdida de información física	Ubicación de algunos archivos físicos de información en lugares no adecuados	Riesgo humano	En el escritorio de servicio al cliente, mantiene expedientes migratorios que son de fácil acceso a personas no autorizadas	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Upala	Externo
R031	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee ni planta eléctrica	Daño en el hardware de los equipos informáticos y de los equipos	Regional Ciudad Quesada	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				ni UPS	de comunicación y estaciones de trabajo		
R032	Daño o pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Algunos archivos físicos están ubicados en lugares de servicio al público y no hay barreras que impidan el acceso a estas áreas	Daño o pérdida de información crítica de la regional	Regional Ciudad Quesada	Externo
R033	Fallo de hardware	Los accesos a los equipos de comunicación no poseen control de acceso	Riesgo humano	La puerta principal a la oficina donde están ubicados los equipos de comunicación se mantiene abierta.	Daño o apagado de los equipos de comunicación.	Regional Ciudad Quesada	Interno
R034	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional Ciudad Quesada	Externo
R035	Acceso físico no autorizado	Inexistencia de mecanismos de control de acceso.	Riesgo humano	Se observa que no existe en ninguna puerta de acceso de todas las oficinas de la regional ningún dispositivo de control de acceso	Robo o pérdida de hardware y archivos físicos.	Regional Ciudad Quesada	Externo
R036	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional Ciudad Quesada	Externo
R037	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional Ciudad Quesada	Interno
R038	Ingreso de personal no autorizado	Existen accesos a la regional fáciles de vulnerar por delincuentes.	Riesgo humano	Se observa que se puede tener acceso fácilmente al interior de la regional desde una propiedad que funciona como	Robo o pérdida de hardware y archivos físicos.	Regional Ciudad Quesada	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				parqueo contiguo al edificio			
R039	Fallo de cableado de red de datos	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional Ciudad Quesada	Interno
R040	Alta humedad	Inexistencia de sensores de humedad	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humedad en ninguna oficina de la regional	Daño o pérdida de información crítica de la regional	Regional Ciudad Quesada	Externo
R041	Exceso de polvo en el ambiente	Ingreso de polvo a las instalaciones de la regional	Riesgo ambiental	Por las condiciones ambientales donde se encuentra ubicada la regional existe mucho polvo en el ambiente y este ingresa a las instalaciones	Daño del equipo informático, especialmente el servidor de conexión a aplicaciones de la DGME	Regional de Sixaola	Externo
R042	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Sixaola	Externo
R043	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica y una UPS que se descarga en 10 minutos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Sixaola	Externo
R044	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público	Robo o pérdida de hardware.	Regional de Sixaola	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		fácil acceso		y a los equipos de comunicación			
R045	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error, cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Sixaola	Interno
R046	Falla de hardware de red de los equipos de usuarios	El cableado estructurado de la mayoría de los equipos es deficiente	Riesgo tecnológico	La exposición del cableado de red de los equipos y una mala manipulación de estos	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Sixaola	Interno
R047	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Algunos archivos físicos están ubicados en lugares de servicio al público y no hay barreras que impidan el acceso a estas áreas	Daño o pérdida de información crítica de la regional	Regional de Sixaola	Externo
R048	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Sixaola	Interno
R049	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Sarapiquí	Externo
R050	Alta temperatura	Inexistencia de sistemas de enfriamiento	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene a temperaturas muy altas y no existen sistemas de aire acondicionado.	Daño de los activos físicos y lógicos de información	Regional de Sarapiquí	Externo
R051	Acceso físico no autorizado	Inexistencia de cámaras de seguridad	Riesgo humano	No existen cámaras de seguridad en toda	Robo o pérdida de hardware y archivos	Regional de Sarapiquí	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		CCTV		la regional, además, no hay guardas de seguridad en horarios de trabajo	físicos.		
R052	Ingreso de personal no autorizado	Existen accesos a la regional fáciles de vulnerar por delincuentes.	Riesgo humano	Se observa que se puede tener acceso fácilmente al interior de la regional desde una propiedad que funciona como parqueo contiguo al edificio	Robo o pérdida de hardware y archivos físicos.	Regional de Sarapiquí	Externo
R053	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Sarapiquí	Externo
R054	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica y una UPS que tarda 10 minutos en descargarse.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Sarapiquí	Externo
R055	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Sarapiquí	Interno
R056	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Sarapiquí	Interno
R057	Pérdida de información física	Archivos físicos de información no están almacenados adecuadament	Riesgo operativo	El manejo de alguna información física en cuanto a su ubicación no es la	Daño o pérdida de información de la regional	Regional de Sarapiquí	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		e		adecuada			
R058	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Sarapiquí	Interno
R059	Inundación	La oficina está ubicada en una zona geográfica propensa a las inundaciones	Riesgo ambiental	Se han presentado crecidas del río que han amenazado con llegar a las instalaciones de la regional	Pérdida de equipos de hardware, así como pérdida de información física y en los casos más críticos, podría presentar pérdidas humanas	Regional de Sarapiquí	Externo
R060	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Guápiles	Externo
R061	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Guápiles	Externo
R062	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica y una UPS que tarda 10 minutos en descargarse.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Guápiles	Externo
R063	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Guápiles	Interno
R064	Falla de hardware de red de los	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos	Pérdida de comunicación de los equipos y los sistemas	Regional de Guápiles	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	equipos de usuarios			mal ubicados o instalados de manera no adecuada	de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional		
R065	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	El manejo de alguna información física en cuanto a su ubicación no es la adecuada	Daño o pérdida de información de la regional	Regional de Guápiles	Externo
R066	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Guápiles	Interno
R067	Ingreso de personal no autorizado	Existen accesos a la regional fáciles de vulnerar por delincuentes.	Riesgo humano	Se observa que se puede tener acceso fácilmente al interior de la regional desde una propiedad que funciona como parqueo contiguo al edificio	Robo o pérdida de hardware y archivos físicos.	Regional de Guápiles	Externo
R068	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Limón	Externo
R069	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Limón	Externo
R070	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica y la mayoría de los equipos no cuentan con UPS.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Limón	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R071	Fallo en el enlace de comunicaciones	El equipo está ubicado en un rack que se mantiene con la llave puesta.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Limón	Interno
R072	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Limón	Interno
R073	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	El manejo de alguna información física en cuanto a su ubicación no es la adecuada	Daño o pérdida de información de la regional	Regional de Limón	Externo
R074	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Limón	Interno
R075	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en todas las oficinas de la DGME, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Aeropuerto Juan Santamaría	Externo
R076	Acceso lógico no autorizado	Los usuarios no bloquean la interface de usuario de los equipos mientras están ausentes	Riesgo operativo	Se observó un equipo con los accesos a los sistemas de la DGME activos y el usuario ausente	Modificación no autorizada de la información de alguno de los sistemas de la DGME	Aeropuerto Juan Santamaría	Externo
R077	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de las oficinas	Robo o pérdida de hardware.	Aeropuerto Juan Santamaría	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		fácil acceso		administrativas y operaciones.			
R078	Acceso físico no autorizado a bodega de archivos	Las paredes de la oficina de archivo están hechas de material de fácil acceso	Riesgo humano	Se observa que las paredes están hechas de Gypsum.	Robo de archivos físicos	Aeropuerto Juan Santamaría	Externo
R079	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información del aeropuerto, así como la afectación de los servicios y operaciones críticas que brinda la regional	Aeropuerto Juan Santamaría	Interno
R080	Incendio	Presencia de material inflamable almacenado en diversas oficinas	Riesgo ambiental	Se pueden observar cajas de vestimenta, cartón y papel almacenados de manera inadecuada, con equipos informáticos y cableado eléctrico	Pérdida de información, así como la afectación de los servicios y operaciones críticas que brinda el aeropuerto, así como posible afectación de vidas humanas.	Aeropuerto Juan Santamaría	Externo
R081	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica y no todos los equipos cuentan con UPS.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Aeropuerto Juan Santamaría	Externo
R082	Exceso de polvo en el ambiente	Equipos informáticos ubicados en lugares con alta afectación de polvo del medio ambiente	Riesgo ambiental	En lo equipos de entrada migratoria se observan grandes cantidades de polvo.	Daño y afectación en el funcionamiento de los equipos informáticos.	Aeropuerto Juan Santamaría	Externo
R083	Acceso físico no autorizado en rack de comunicac	Los equipos de comunicación están en gabinetes sin control de	Riesgo tecnológico	Por error cualquier persona accidental o intencionalmente puede manipular	Daño en el hardware de los equipos informáticos y de los equipos	Aeropuerto Juan Santamaría	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	iones	acceso		los equipos, ya que el gabinete se mantiene abierto o con las llaves de acceso puestas.	de comunicación		
R084	Robo o pérdida de archivos físicos	Archivos físicos de información no están almacenados adecuadamente	Riesgo financiero	El manejo de alguna información física en cuanto a su ubicación no es la adecuada	Daño o pérdida de información física del aeropuerto	Aeropuerto Juan Santamaría	Externo
R085	Material contaminante en el centro de datos	Presencia de polvo de material de construcción sobre el gabinete principal en el centro de datos.	Riesgo ambiental	Se puede observar material de construcción en polvo sobre el cableado y el gabinete principal	Afectación o daño en el funcionamiento en los equipos informáticos y el cableado estructurado.	Aeropuerto Juan Santamaría	Externo
R086	Fallo del enlace principal de comunicaciones	Cableado y equipos eléctricos ubicados en conjunto con la fibra óptica	Riesgo operativo	Se observan regletas y cableado eléctrico a un lado de la fibra óptica principal.	Degradación o daño del enlace de comunicaciones principal del aeropuerto	Aeropuerto Juan Santamaría	Interno
R087	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Sabalito	Externo
R088	Alta temperatura	Inexistencia de sistemas de enfriamiento	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene a temperaturas muy altas y no existen sistemas de aire acondicionado.	Daño de los activos físicos y lógicos de información	Regional de Sabalito	Externo
R089	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Sabalito	Externo
R090	Ingreso de personal no autorizado	Existen accesos a la regional fáciles de vulnerar por delincuentes.	Riesgo humano	Se observa que se puede tener acceso fácilmente al interior de la regional desde una propiedad que	Robo o pérdida de hardware y archivos físicos.	Regional de Sabalito	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				funciona como parqueo contiguo al edificio			
R091	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Sabalito	Externo
R092	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica ni equipos UPS.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Sabalito	Externo
R093	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Sabalito	Interno
R094	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Sabalito	Interno
R095	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	El manejo de alguna información física en cuanto a su ubicación no es la adecuada	Daño o pérdida de información de la regional	Regional de Sabalito	Externo
R096	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Sabalito	Interno
R097	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se	Daño de los activos físicos y lógicos de	Regional de Paso Canoas	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				mantiene niveles de humedad muy altos.	información		
R098	Acceso físico no autorizado	Las paredes de la oficina de archivo están hechas de material de fácil acceso	Riesgo humano	Se observa que las paredes están hechas en su mayoría de madera	Robo de archivos físicos	Regional de Paso Canoas	Externo
R099	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de las oficinas administrativas.	Robo o pérdida de hardware.	Regional de Paso Canoas	Externo
R100	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y a pesar de poseer planta eléctrica la UPS está en mal estado.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Paso Canoas	Externo
R101	Fallo en el enlace de comunicaciones	Inexistencia de controles de acceso al gabinete principal	Riesgo operativo	El gabinete de comunicaciones y servidores se mantiene abierto.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Paso Canoas	Interno
R102	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado y en mal estado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Paso Canoas	Interno
R103	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Algunos archivos físicos están ubicados en lugares de servicio al público y no hay barreras que impidan el acceso a estas áreas	Daño o pérdida de información crítica de la regional	Regional de Paso Canoas	Externo
R104	Incendio	No hay sensores ni	Riesgo ambiental	La regional almacena mucha	Daño de los activos físicos y	Regional de Paso Canoas	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		sistemas contra incendios		información física y no hay sensores de humo en ninguna oficina de la regional	lógicos de información		
R105	Inundaciones	Existen problemas con el control de las aguas de lluvia	Riesgo ambiental	La regional posee importantes goteras debido a su mal estado.	Daño de los activos físicos y lógicos de información	Regional de Paso Canoas	Externo
R106	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Quepos	Externo
R107	Alta temperatura	Inexistencia de sistemas de enfriamiento	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene a temperaturas muy altas y el sistema de aire acondicionado está dañado.	Daño de los activos físicos y lógicos de información	Regional de Quepos	Externo
R108	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Quepos	Externo
R109	Ingreso de personal no autorizado	Existen accesos a la regional fáciles de vulnerar por delincuentes.	Riesgo humano	Se observa que se puede tener acceso fácilmente al interior de la regional desde la propiedad de los dueños que alquilan la oficina a la DGME	Robo o pérdida de hardware y archivos físicos.	Regional de Quepos	Externo
R110	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Quepos	Externo
R111	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica ni equipos UPS.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y	Regional de Quepos	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					estaciones de trabajo		
R112	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Quepos	Interno
R113	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Quepos	Interno
R114	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Se puede observar que la información más antigua se almacena en el cielorraso de la regional y esta posee acceso por el patio de los dueños de la propiedad que alquilan el edificio a la DGME y la puerta de esta no posee candados.	Daño o pérdida de información de la regional	Regional de Quepos	Externo
R115	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Quepos	Interno
R116	Inundación	Ubicación geográfica de la regional	Riesgo ambiental	La oficina de encuentra a 15 metros de un río	Daño de los activos físicos y lógicos de información	Regional de Quepos	Externo
R117	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Golfito	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R118	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Golfito	Externo
R119	Robo o pérdida de equipos informáticos	Inexistencia de sistemas de control de acceso	Riesgo humano	Se observa que se puede tener acceso fácilmente a la oficina.	Robo o pérdida de hardware y archivos físicos.	Regional de Golfito	Externo
R120	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y a pesar de poseer planta eléctrica la UPS está en mal estado.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Golfito	Externo
R121	Fallo en el enlace de comunicaciones	Inexistencia de gabinete de comunicaciones	Riesgo operativo	Los equipos de comunicación se encuentran sobre un rack y puede ser manipulado fácilmente	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Golfito	Interno
R122	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado y en mal estado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Golfito	Interno
R123	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Algunos archivos físicos están ubicados en lugares de servicio al público, y no hay barreras que impidan el acceso a estas áreas	Daño o pérdida de información crítica de la regional	Regional de Golfito	Externo
R124	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores	Daño de los activos físicos y lógicos de información	Regional de Golfito	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				de humo en ninguna oficina de la regional			
R125	Inundación	La oficina se encuentra a 200 metros del río	Riesgo ambiental	Se han presentado crecidas del río que han llegado hasta la regional	Pérdida de equipos de hardware, así como pérdida de información física, y en los casos más críticos podría presentar pérdidas humanas	Regional de Golfito	Externo
R126	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Pérez Zeledón	Externo
R127	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en toda la regional, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Regional de Pérez Zeledón	Externo
R128	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de servicio al público.	Robo o pérdida de hardware.	Regional de Pérez Zeledón	Externo
R129	Fallo en fluido eléctrico	Fluido eléctrico falla constantemente	Riesgo operativo	Los cortes en el fluido eléctrico son constantes en la zona y no posee planta eléctrica.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación y estaciones de trabajo	Regional de Pérez Zeledón	Externo
R130	Fallo en el enlace de comunicaciones	El equipo está ubicado en un lugar no adecuado, no posee gabinete.	Riesgo operativo	Por error cualquier persona accidental o intencionalmente puede manipular los equipos	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Pérez Zeledón	Interno
R131	Falla de hardware de red de los	Instalación del cableado estructurado inadecuado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos	Pérdida de comunicación de los equipos y los sistemas	Regional de Pérez Zeledón	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	equipos de usuarios			mal ubicados o instalados de manera no adecuada	de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional		
R132	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	El manejo de alguna información física en cuanto a su ubicación no es la adecuada	Daño o pérdida de información de la regional	Regional de Pérez Zeledón	Externo
R133	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional	Daño de los activos físicos y lógicos de información	Regional de Pérez Zeledón	Interno
R134	Alta temperatura	Inexistencia de sistemas de enfriamiento	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene a temperaturas muy altas y el sistema de aire acondicionado está dañado.	Daño de los activos físicos y lógicos de información	Regional de Pérez Zeledón	Interno
R135	Acceso físico no autorizado	Inexistencia de cámaras de seguridad CCTV	Riesgo humano	No existen cámaras de seguridad en las oficinas de aeropuerto, además, no hay guardas de seguridad en horarios de trabajo	Robo o pérdida de hardware y archivos físicos.	Aeropuerto Daniel Oduber	Externo
R136	Pérdida de información física	Inexistencia de oficina de archivo físico	Riesgo humano	No hay destinado un lugar para el almacenamiento de la información	Puede presentarse por la manipulación de la información mal manejo ya sea con o sin intención la pérdida de la información.	Aeropuerto Daniel Oduber	Interno
R137	Robo o pérdida de equipos informático	Ubicación de equipos computacionales en lugares no	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de	Robo o pérdida de hardware.	Aeropuerto Daniel Oduber	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	s	adecuados de fácil acceso		control de entradas.			
R138	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Aeropuerto Daniel Oduber	Externo
R139	Ataque digital de aplicación (FID 9310)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de Microsoft SQL ***Image Processing Memory Corruption***	Corrupción de la memoria en el servidor generando un ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R140	Ataque digital de aplicación (FID 9328)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de Microsoft SQL ***File Parsing Remote Code Execution***	Un atacante puede ejecutar código de manera remota como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R141	Ataque digital de aplicación (FID 9329)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de Microsoft SQL ***Image File Buffer Overflow***	Se puede ejecutar código malicioso para generar un desbordamiento de memoria con ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R142	Ataque digital de aplicación (FID 9330)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de Microsoft SQL ***Image File Integer Buffer Overflow***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R143	Ataque digital de aplicación (FID 9335)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de Microsoft SQL ***Image File Buffer Overflow***	Se puede ejecutar código malicioso para generar un desbordamiento de memoria con ataque de denegación de servicio	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R144	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 R2	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R145	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 R2	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***NetBIOS Sessions Using Any Username And Password Are Allowed***	Un atacante puede ingresar de manera abrupta al equipo utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña	Uruca Oficinas Centrales	Externo
R146	Ataque digital de aplicación (FID 12096)	Servidor con vulnerabilidad presente en sus aplicaciones	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***Dell OpenManage 'file' Parameter URI Redirection***	Un atacante puede redireccionar un sitio web utilizando la vulnerabilidad que posee la aplicación DELL OpenManager	Uruca Oficinas Centrales	Externo
R147	Ataque digital de aplicación (FID 17281)	Servidor con vulnerabilidad presente en su protocolo SSLv3	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***SSLv3 Information Disclosure***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R148	Ataque digital de aplicación (FID 17967)	Servidor con vulnerabilidad presente en su protocolo OpenSSL	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***SSL/TLS Export Suites Freak Attack***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R149	Ataque digital de aplicación (FID 18179)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL RC4	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de	Un atacante puede explotar la vulnerabilidad con la intención	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				TLS/SSL RC4 Cipher Suites Information Disclosure	de decodificar texto cifrado en texto plano		
R150	Ataque digital de aplicación (FID 20465)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL Triple-DES	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***SSL/TLS Protocol Triple-DES Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R151	Ataque digital de aplicación (FID 6360)	Servidor con vulnerabilidad presente en el uso de certificados digitales X.509	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***IETF X.509 Certificate Signature Collision***	Un atacante puede legitimar un sitio web para generar colisiones	Uruca Oficinas Centrales	Externo
R152	Ataque digital de aplicación (FID 1859)	Servidor con vulnerabilidad presente en el uso de certificados digitales cifrados	Riesgo tecnológico	El servidor SUPDATE 192.168.120.15 posee la vulnerabilidad de ***Web Server Supports Weak SSL Encryption Certificates***	Un atacante puede interceptar la negociación del protocolo SSL y descubrir las claves de cifrado utilizados en el certificado digital	Uruca Oficinas Centrales	Externo
R153	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 R2	Riesgo tecnológico	El servidor URUCA 192.168.120.11 posee la vulnerabilidad de ***NetBIOS Sessions Using Any Username And Password Are Allowed***	Un atacante puede ingresar de manera abrupta al equipo utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña	Uruca Oficinas Centrales	Externo
R154	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft	Riesgo tecnológico	El servidor PENASBLANCAS 192.160.163.210 posee la vulnerabilidad de ***Security Update***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Windows Server 2008 R2		***for Windows SMB Server***	de denegación de servicio		
R155	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2008 R2	Riesgo tecnológico	El servidor PENASBLANCAS 192.160.163.210 posee la vulnerabilidad de ***NetBIOS Sessions Using Any Username And Password Are Allowed***	Un atacante puede ingresar de manera abrupta al equipo utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña	Uruca Oficinas Centrales	Externo
R156	Ataque digital de aplicación (FID 10385)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SRVARENALWS 172.16.254.10 posee la vulnerabilidad de ***Microsoft Windows Print Spooler Service Impersonation***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R157	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SRVARENALWS 172.16.254.10 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R158	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SRVARENALWS 172.16.254.10 posee la vulnerabilidad de ***NetBIOS Sessions Using Any Username And Password Are Allowed***	Un atacante puede ingresar de manera abrupta al equipo utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña	Uruca Oficinas Centrales	Externo
R159	Ataque digital de aplicación (FID 18213)	Servidor con vulnerabilidad presente en su sistema operativo	Riesgo tecnológico	El servidor SRVARENALWS 172.16.254.10 posee la vulnerabilidad de	Un atacante puede ejecutar código de manera remota y arbitraria	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Microsoft Windows 7 SP1		***Microsoft Windows HTTP.sys Remote Code Execution***	como ataque de denegación de servicio		
R160	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 7 SP1	Riesgo tecnológico	El servidor SRVARENALWS 172.16.254.10 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R161	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 7 SP1	Riesgo tecnológico	El servidor SRVZURQUIWS 172.16.254.11 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R162	Ataque digital de aplicación (FID 9329)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor CARDEX 192.168.121.103 posee la vulnerabilidad de Microsoft SQL ***Image File Buffer Overflow***	Se puede ejecutar código malicioso para generar un desbordamiento de memoria con ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R163	Ataque digital de aplicación (FID 9335)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor CARDEX 192.168.121.103 posee la vulnerabilidad de Microsoft SQL ***Image File Buffer Overflow***	Se puede ejecutar código malicioso para generar un desbordamiento de memoria con ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R164	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 7 SP1	Riesgo tecnológico	El servidor CARDEX 192.168.121.103 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R165	Ataque digital de aplicación (FID 9330)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor AFIS1 192.168.121.101 posee la vulnerabilidad de Microsoft SQL ***Image File Integer Buffer***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				Overflow	de servicio		
R166	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server SP2	Riesgo tecnológico	El servidor AFIS1 192.168.121.101 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R167	Ataque digital de aplicación (FID 9335)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor AFIS2 192.168.121.102 posee la vulnerabilidad de Microsoft SQL ***Image File Buffer Overflow***	Se puede ejecutar código malicioso para generar un desbordamiento de memoria con ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R168	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server SP2	Riesgo tecnológico	El servidor AFIS2 192.168.121.102 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R169	Ataque digital de aplicación (FID 9310)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL Server	Riesgo tecnológico	El servidor CDXCOM 192.168.121.104 posee la vulnerabilidad de Microsoft SQL ***Image Processing Memory Corruption***	Corrupción de la memoria en el servidor generando un ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R170	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server SP2	Riesgo tecnológico	El servidor CDXCOM 192.168.121.104 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R171	Ataque digital de aplicación (FID 5182)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server SP2	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad ***Microsoft Internet Information Services Remote***	Una explotación de esta vulnerabilidad puede generar una denegación de servicio al servicio IIS en	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				DoS	el servidor		
R172	Ataque digital de aplicación (FID 20465)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL Triple-DES	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad de ***SSL/TLS Protocol Triple-DES Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R173	Ataque digital de aplicación (FID 17281)	Servidor con vulnerabilidad presente en su protocolo SSLv3	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad de ***SSLv3 Information Disclosure***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R174	Ataque digital de aplicación (FID 18179)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL RC4	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad de ***TLS/SSL RC4 Cipher Suites Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R175	Ataque digital de aplicación (FID 6360)	Servidor con vulnerabilidad presente en el uso de certificados digitales X.509	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad de ***IETF X.509 Certificate Signature Collision***	Un atacante puede legitimar un sitio web para generar colisiones	Uruca Oficinas Centrales	Externo
R176	Ataque digital de aplicación (FID 1859)	Servidor con vulnerabilidad presente en el uso de certificados digitales cifrados	Riesgo tecnológico	El servidor CORREO 192.168.121.106 posee la vulnerabilidad de ***Web Server Supports Weak SSL Encryption Certificates***	Un atacante puede interceptar la negociación del protocolo SSL y descubrir las claves de cifrado utilizados en el certificado digital	Uruca Oficinas Centrales	Externo
R177	Ataque digital de aplicación (FID 9310)	Servidor con vulnerabilidad presente en su sistema de base de datos Microsoft SQL	Riesgo tecnológico	El servidor 10.10.10.6 posee la vulnerabilidad de Microsoft SQL ***Image Processing***	Corrupción de la memoria en el servidor generando un ataque de denegación de	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Server		***Memory Corruption***	servicio		
R178	Ataque digital de aplicación (FID 21660)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server	Riesgo tecnológico	El servidor 10.10.10.5 posee la vulnerabilidad de Microsoft SQL ***Microsoft Internet Information Services Buffer Overflow***	Una explotación de esta vulnerabilidad puede generar una denegación de servicio al servicio IIS en el servidor, permitiendo al atacante ejecutar código arbitrario.	Uruca Oficinas Centrales	Externo
R179	Ataque digital de aplicación (FID 21660)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server	Riesgo tecnológico	El servidor 10.10.10.4 posee la vulnerabilidad de Microsoft SQL ***Microsoft Internet Information Services Buffer Overflow***	Una explotación de esta vulnerabilidad puede generar una denegación de servicio al servicio IIS en el servidor, permitiendo al atacante ejecutar código arbitrario.	Uruca Oficinas Centrales	Externo
R180	Ataque digital de aplicación (FID 18213)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 7	Riesgo tecnológico	El servidor 10.10.10.250 posee la vulnerabilidad de ***Microsoft Windows HTTP.sys Remote Code Execution***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R181	Ataque digital de aplicación (FID 6533)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Control Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R182	Ataque digital de aplicación (FID 6467)	Servidor con vulnerabilidad presente en su sistema de bases de datos	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de	La explotación de esta vulnerabilidad puede tener un impacto	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Oracle		***Oracle Database Advanced Queuing Component Unspecified***	desconocido para el servidor de base de datos Oracle		
R183	Ataque digital de aplicación (FID 6532)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Help For Web Component Unspecified***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R184	Ataque digital de aplicación (FID 7659)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Listener Component Information Disclosure***	La explotación de esta vulnerabilidad puede permitir al atacante afectar la disponibilidad, integridad y disponibilidad de la información de la base de datos	Uruca Oficinas Centrales	Externo
R185	Ataque digital de aplicación (FID 6458)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database XML DB Component Unspecified***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R186	Ataque digital de aplicación (FID 6469)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Upgrade/Downgrade Component Unspecified***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R187	Ataque digital de aplicación (FID 6476)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Spatial Component Unspecified***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				Vulnerability			
R188	Ataque digital de aplicación (FID 6485)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Ultra Search Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R189	Ataque digital de aplicación (FID 6491)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Export Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R190	Ataque digital de aplicación (FID 6511)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Text Component SQL Injection Vulnerability***	La explotación de esta vulnerabilidad puede permitir al atacante de manera remota ejecutar comandos de SQL	Uruca Oficinas Centrales	Externo
R191	Ataque digital de aplicación (FID 6524)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Vault Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R192	Ataque digital de aplicación (FID 6526)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Multiple Unspecified Vulnerabilities***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R193	Ataque digital de aplicación (FID 6532)	Servidor con vulnerabilidad presente en su sistema de bases de datos	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de	La explotación de esta vulnerabilidad puede tener un impacto	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Oracle		***Oracle Database Help For Web Component Unspecified Vulnerability***	desconocido para el servidor de base de datos Oracle		
R194	Ataque digital de aplicación (FID 6533)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Control Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R195	Ataque digital de aplicación (FID 6534)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Multiple Component Unspecified Vulnerabilities***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R196	Ataque digital de aplicación (FID 6540)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Multiple Component Unspecified Vulnerabilities***	La explotación de esta vulnerabilidad puede tener un impacto desconocido para el servidor de base de datos Oracle	Uruca Oficinas Centrales	Externo
R197	Ataque digital de aplicación (FID 6614)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle April 2009 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R198	Ataque digital de aplicación (FID 6851)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle July 2009 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					ataques al sistema de base de datos		
R199	Ataque digital de aplicación (FID 7070)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Network Foundation Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede permitir al atacante afectar la disponibilidad, integridad y disponibilidad de la información de la base de datos	Uruca Oficinas Centrales	Externo
R200	Ataque digital de aplicación (FID 7071)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Network Authentication Component Unspecified Vulnerability***	La explotación de esta vulnerabilidad puede permitir al atacante afectar la disponibilidad, integridad y disponibilidad de la información de la base de datos	Uruca Oficinas Centrales	Externo
R201	Ataque digital de aplicación (FID 7266)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database October 2009 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R202	Ataque digital de aplicación (FID 7659)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Listener Component Information Disclosure Vulnerability***	La explotación de esta vulnerabilidad puede permitir al atacante afectar la disponibilidad, integridad y disponibilidad de la información de la base de datos	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R203	Ataque digital de aplicación (FID 7661)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Oracle OLAP Component Vulnerability***	La explotación de esta vulnerabilidad puede permitir la divulgación no autorizada de información, modificaciones no autorizadas y la interrupción del servicio.	Uruca Oficinas Centrales	Externo
R204	Ataque digital de aplicación (FID 7818)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database January 2010 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R205	Ataque digital de aplicación (FID 13564)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database April 2012 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R206	Ataque digital de aplicación (FID 14978)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Critical Patch Update April 2013***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R207	Ataque digital de aplicación (FID 12851)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database October 2011 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					base de datos		
R208	Ataque digital de aplicación (FID 14627)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Server January 2013 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R209	Ataque digital de aplicación (FID 9759)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database April 2010 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R210	Ataque digital de aplicación (FID 6014)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle July 2008 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R211	Ataque digital de aplicación (FID 6182)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle October 2008 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R212	Ataque digital de aplicación (FID 15315)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Critical Patch Update July 2013***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					ataques al sistema de base de datos		
R213	Ataque digital de aplicación (FID 6382)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle January 2009 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R214	Ataque digital de aplicación (FID 5570)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Releases July 2007 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R215	Ataque digital de aplicación (FID 5571)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Releases October 2007 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R216	Ataque digital de aplicación (FID 5675)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle January 2008 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R217	Ataque digital de aplicación (FID 5834)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle April 2008 Critical Patch***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				Update	posibles ataques al sistema de base de datos		
R218	Ataque digital de aplicación (FID 10424)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database October 2010 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R219	Ataque digital de aplicación (FID 12395)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database July 2011 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R220	Ataque digital de aplicación (FID 13917)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database July 2012 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R221	Ataque digital de aplicación (FID 14277)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database Server October 2012 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R222	Ataque digital de aplicación (FID 11925)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database***	La falta de este paquete de actualizaciones de Oracle puede representar	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				April 2011 Critical Patch Update	múltiples posibles ataques al sistema de base de datos		
R223	Ataque digital de aplicación (FID 11126)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database January 2011 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R224	Ataque digital de aplicación (FID 13226)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee la vulnerabilidad de ***Oracle Database January 2012 Critical Patch Update***	La falta de este paquete de actualizaciones de Oracle puede representar múltiples posibles ataques al sistema de base de datos	Uruca Oficinas Centrales	Externo
R225	Ataque digital de aplicación (FID 2195)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee el Echo Daemon activo	Este servicio puede ser responsable de ataque de denegación de servicio (DoS).	Uruca Oficinas Centrales	Externo
R226	Ataque digital de aplicación (FID 972)	Servidor con vulnerabilidad presente en su sistema operativo Solaris 9	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee el rexecd activo	La explotación en el uso de este servicio para acceso remoto puede comprometer el funcionamiento del servidor	Uruca Oficinas Centrales	Externo
R227	Ataque digital de aplicación (FID 12848)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad en la configuración de los servicios de escalación de privilegios	Este servicio puede ser responsable de ataque de denegación de servicio (DoS).	Uruca Oficinas Centrales	Externo
R228	Ataque digital de aplicación (FID	Servidor con vulnerabilidad presente en su sistema de	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una	Esta vulnerabilidad permite la ejecución de	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	13638)	bases de datos Oracle		vulnerabilidad de ejecución de código de manera remota	código arbitrario de manera remota en componente de los archivos del TNS Listener.		
R229	Ataque digital de aplicación (FID 10436)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad relacionada a Java Virtual Machine	Esta vulnerabilidad permite la ejecución en la creación de sesiones de usuario con altos privilegios para la ejecución de código arbitrario.	Uruca Oficinas Centrales	Externo
R230	Ataque digital de aplicación (FID 10437)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Oracle Database Server Change Data Capture GSS-API Library Denial Of Service***	Esta vulnerabilidad puede ser responsable de un ataque de denegación de servicio (DoS), por medio GSS-API Library	Uruca Oficinas Centrales	Externo
R231	Ataque digital de aplicación (FID 13997)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Oracle Database CTXSYS.CONTEXT Privilege Escalation Vulnerability***	Esta vulnerabilidad permite la posibilidad de que un atacante modifique el archivo ctxsys.context permitiendo elevar los privilegios a SYSDBA en la base de datos	Uruca Oficinas Centrales	Externo
R232	Ataque digital de aplicación (FID 673)	Servidor con vulnerabilidad presente en su sistema operativo Solaris 9	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee el servicio CHARGUEN activo	La explotación en el uso de este servicio para acceso remoto puede comprometer el funcionamiento del servidor generando un ataque de denegación de	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					servicio (DoS).		
R233	Ataque digital de aplicación (FID 832)	Servidor con vulnerabilidad presente en su sistema operativo Solaris 9	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Allaire JRun 2.x /servlet/SessionServlet***	La explotación de esta vulnerabilidad permite descubrir información sensitiva acerca de las sesiones de HTTP.	Uruca Oficinas Centrales	Externo
R234	Ataque digital de aplicación (FID 10444)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Oracle Database Server Job Queue Remote Code Execution***	Esta vulnerabilidad permite la modificación del archivo SYS.DBMS_IJOB permitiendo al atacante autenticarse para ejecutar código arbitrario y comprometer el servicio de base de datos.	Uruca Oficinas Centrales	Externo
R235	Ataque digital de aplicación (FID 10439)	Servidor con vulnerabilidad presente en su sistema de bases de datos Oracle	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Oracle Database Server Change Data Capture Information Disclosure***	Esta vulnerabilidad permite la modificación del archivo DBMS_CDC_PUBLISH permitiendo al atacante autenticarse para descubrir información sensitiva y manipularla.	Uruca Oficinas Centrales	Externo
R236	Ataque digital de aplicación (FID 790)	Servidor con vulnerabilidad presente en su sistema operativo Solaris 9	Riesgo tecnológico	El servidor SISPAS 192.168.121.250 posee una vulnerabilidad de ***Oracle Solaris Common Desktop Environment (CDE) dtspcd Information Leakage***	La explotación de esta vulnerabilidad permite explotar el servicio DTSPCD permitiendo al atacante acceder información sensitiva.	Uruca Oficinas Centrales	Externo
R237	Ataque	Servidor con	Riesgo	El servidor	La explotación	Uruca	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	digital de aplicación (FID 2638)	vulnerabilidad presente en su sistema de base de datos MYSQL	tecnológico	TURRIALBA 192.168.121.25 posee una vulnerabilidad de ***MySQL ALTER TABLE Password Buffer Overflow***	de esta vulnerabilidad permite a los usuarios con ciertas cuentas ejecutar código arbitrario y comprometer el funcionamiento de la base de datos	Oficinas Centrales	
R238	Ataque digital de aplicación (FID 2900)	Servidor con vulnerabilidad presente en su sistema de base de datos MYSQL	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee una vulnerabilidad de ***MySQL ALTER MERGE tables Denial of Service***	La explotación de esta vulnerabilidad permite al atacante generar una denegación de servicio (DoS)n al servicio de base de datos	Uruca Oficinas Centrales	Externo
R239	Ataque digital de aplicación (FID 1905)	Servidor con vulnerabilidad presente en su sistema de base de datos MYSQL	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee una vulnerabilidad de ***MySQL Database World Writable Files***	La explotación de esta vulnerabilidad permite al atacante de manera remota escribir en los archivos y elevar los privilegios en el host de destino.	Uruca Oficinas Centrales	Externo
R240	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee una vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R241	Ataque digital de aplicación (FID 2200)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee una vulnerabilidad de ***IIS IISHelp Default Pages***	Un atacante puede modificar las páginas creadas de manera predeterminada en el servicio del IIS	Uruca Oficinas Centrales	Externo
R242	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee la vulnerabilidad de	Un atacante puede ingresar de manera abrupta al equipo	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Microsoft Windows Server XP SP3		***NetBIOS Sessions Using Any Username And Password Are Allowed***	utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña		
R243	Ataque digital de aplicación (FID 8211)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server XP SP3	Riesgo tecnológico	El servidor TURRIALBA 192.168.121.25 posee la vulnerabilidad de ***Microsoft IIS Malformed HTTP HOST Header Field Denial Of Service Vulnerability***	Un atacante puede explotar esta vulnerabilidad de denegación de servicio está presente en el servicio de Microsoft IIS., es posible reproducir esta condición enviando una solicitud HTTP POST con un encabezado HOST campo que se compone de un número excesivo de barras diagonales (/). La explotación exitosa podría permitir que un atacante cause una denegación de servicio.	Uruca Oficinas Centrales	Externo
R244	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP1	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R245	Ataque digital de aplicación (FID 4522)	Servidor con vulnerabilidad presente en su sistema operativo	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de	Un atacante puede ejecutar código de manera remota y arbitraria	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		Microsoft Windows Server 2003 SP1		***Microsoft Windows Server Service Vulnerability No Credentials Required***	como ataque de denegación de servicio		
R246	Ataque digital de aplicación (FID 4550)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP1	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de ***Microsoft Server Service Mailslot Heap Overflow Non-Intrusive***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R247	Ataque digital de aplicación (FID 4460)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP1	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de ***Microsoft Server Service SMB Information Disclosure Vulnerability Non-Intrusive***	Un atacante puede acceder y descubrir información sensitiva	Uruca Oficinas Centrales	Externo
R248	Ataque digital de aplicación (FID 10125)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP1	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de ***WampServer lang Parameter Cross Site Scripting Vulnerability***	Un atacante puede ejecutar un Cross Site Scripting en la versión de WampServer instalada en el servidor.	Uruca Oficinas Centrales	Externo
R249	Ataque digital de aplicación (FID 12824)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP1	Riesgo tecnológico	El servidor GTI-MARCAS 192.168.121.186 posee una vulnerabilidad de ***HTTP Server Prone To Slow Denial Of Service Attack***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R250	Ataque digital de aplicación (FID 13638)	Servidor con vulnerabilidad presente en su sistema Microsoft Windows 2012 Server R2	Riesgo tecnológico	El servidor SRVSPAPP 10.200.201.17 posee una vulnerabilidad de ejecución de código de manera remota	Esta vulnerabilidad permite la ejecución de código arbitrario de manera remota en componente de los archivos	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
					del TNS Listener.		
R251	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2003 SP2	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee una vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R252	Ataque digital de aplicación (FID 5182)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows 2003 Server SP2	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad ***Microsoft Internet Information Services Remote DoS***	Una explotación de esta vulnerabilidad puede generar una denegación de servicio al servicio IIS en el servidor	Uruca Oficinas Centrales	Externo
R253	Ataque digital de aplicación (FID 17281)	Servidor con vulnerabilidad presente en su protocolo SSLv3	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***SSLv3 Information Disclosure***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R254	Ataque digital de aplicación (FID 17967)	Servidor con vulnerabilidad presente en su protocolo OpenSSL	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***SSL/TLS Export Suites Freak Attack***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R255	Ataque digital de aplicación (FID 18179)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL RC4	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***TLS/SSL RC4 Cipher Suites Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R256	Ataque digital de aplicación (FID 20465)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL Triple-DES	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***SSL/TLS Protocol Triple-DES Information***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				Disclosure			
R257	Ataque digital de aplicación (FID 1859)	Servidor con vulnerabilidad presente en el uso de certificados digitales cifrados	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***Web Server Supports Weak SSL Encryption Certificates***	Un atacante puede interceptar la negociación del protocolo SSL y descubrir las claves de cifrado utilizados en el certificado digital	Uruca Oficinas Centrales	Externo
R258	Ataque digital de aplicación (FID 6360)	Servidor con vulnerabilidad presente en el uso de certificados digitales X.509	Riesgo tecnológico	El servidor SVMWARE 192.168.121.32 posee la vulnerabilidad de ***IETF X.509 Certificate Signature Collision***	Un atacante puede legitimar un sitio web para generar colisiones	Uruca Oficinas Centrales	Externo
R259	Ataque digital de aplicación (FID 20915)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee la vulnerabilidad de ***Apache Tomcat Multiple Vulnerabilities Prior To 6.0.48***	Un atacante puede explotar esta vulnerabilidad que le permite obtener información sensitiva y ejecutar código arbitrario.	Uruca Oficinas Centrales	Externo
R260	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2008 Server R2 SP1	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R261	Ataque digital de aplicación (FID 19731)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Multiple Vulnerabilities Prior To 6.0.45***	Un atacante puede explotar esta vulnerabilidad que le permite obtener información sensitiva y ejecutar código arbitrario.	Uruca Oficinas Centrales	Externo
R262	Ataque digital de aplicación	Servidor con vulnerabilidades presentes en	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231	Un atacante puede explotar esta	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	(FID 21106)	el servicio Apache Tomcat		posee una vulnerabilidad de ***Apache Tomcat Vulnerability Prior To 6.0.49***	vulnerabilidad que le permite obtener información sensitiva y ejecutar código arbitrario.		
R263	Ataque digital de aplicación (FID 18355)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Response Request Body Denial of Service***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R264	Ataque digital de aplicación (FID 12824)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows Server 2008 Server R2 SP1	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***HTTP Server Prone To Slow Denial Of Service Attack***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R265	Ataque digital de aplicación (FID 14508)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Slowloris HTTP Denial of Service***	La explotación exitosa por un atacante remoto podría resultar en una condición de denegación de servicio.	Uruca Oficinas Centrales	Externo
R266	Ataque digital de aplicación (FID 17281)	Servidor con vulnerabilidad presente en su protocolo SSLv3	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee la vulnerabilidad de ***SSLv3 Information Disclosure***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R267	Ataque digital de aplicación (FID 17880)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Chunked Request Handling Vulnerability***	La explotación de esta vulnerabilidad podría permitir a un atacante eludir ciertas restricciones de seguridad.	Uruca Oficinas Centrales	Externo
R268	Ataque digital de aplicación	Servidor con vulnerabilidad presente en su	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231	Un atacante puede ejecutar código de	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	(FID 17967)	protocolo OpenSSL		posee la vulnerabilidad de ***SSL/TLS Export Suites Freak Attack***	manera remota y arbitraria como ataque de denegación de servicio		
R269	Ataque digital de aplicación (FID 18179)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL RC4	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee la vulnerabilidad de ***TLS/SSL RC4 Cipher Suites Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R270	Ataque digital de aplicación (FID 18384)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Security Manager Bypass***	La explotación exitosa podría permitir a un atacante eludir ciertas restricciones de seguridad y realizar acciones no autorizadas.	Uruca Oficinas Centrales	Externo
R271	Ataque digital de aplicación (FID 20849)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Multiple Vulnerabilities (October 27th 2016)***	La explotación exitosa podría permitir a un atacante recuperar datos confidenciales o escalar privilegios.	Uruca Oficinas Centrales	Externo
R272	Ataque digital de aplicación (FID 21669)	Servidor con vulnerabilidades presentes en el servicio Apache Tomcat	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee una vulnerabilidad de ***Apache Tomcat Vulnerability Prior To 6.0.53***	Un atacante puede explotar esta vulnerabilidad que le permite obtener información sensitiva.	Uruca Oficinas Centrales	Externo
R273	Ataque digital de aplicación (FID 20465)	Servidor con vulnerabilidad presente en su protocolo TLS/SSL Triple-DES	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231 posee la vulnerabilidad de ***SSL/TLS Protocol Triple-DES Information Disclosure***	Un atacante puede explotar la vulnerabilidad con la intención de decodificar texto cifrado en texto plano	Uruca Oficinas Centrales	Externo
R274	Ataque digital de aplicación	Servidor con vulnerabilidad presente en el	Riesgo tecnológico	El servidor BASE_NLB1 192.168.122.231	Un atacante puede interceptar la	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	(FID 1859)	uso de certificados digitales cifrados		posee la vulnerabilidad de ***Web Server Supports Weak SSL Encryption Certificates***	negociación del protocolo SSL y descubrir las claves de cifrado utilizados en el certificado digital		
R275	Ataque digital de aplicación (FID 10385)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SERVER_TOBIAS 172.24.9.11 posee la vulnerabilidad de ***Microsoft Windows Print Spooler Service Impersonation***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R276	Ataque digital de aplicación (FID 21706)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SERVER_TOBIAS 172.24.9.11 posee la vulnerabilidad de ***Security Update for Windows SMB Server***	Un atacante puede ejecutar código de manera remota y arbitraria como ataque de denegación de servicio	Uruca Oficinas Centrales	Externo
R277	Ataque digital de aplicación (FID 13016)	Servidor con vulnerabilidad presente en su sistema operativo Microsoft Windows XP SP3	Riesgo tecnológico	El servidor SERVER_TOBIAS 172.24.9.11 posee la vulnerabilidad de ***NetBIOS Sessions Using Any Username And Password Are Allowed***	Un atacante puede ingresar de manera abrupta al equipo utilizando técnicas de red básicas por medio de Input/Output Sistema (NetBIOS) con cualquier usuario o contraseña	Uruca Oficinas Centrales	Externo
R278	Peligro de incendio	Existe una gran cantidad de cajas de papel en condiciones que promueven la posibilidad de un incendio.	Riesgo ambiental	Existen grandes cantidades de papel de información física en diversos puntos de las oficinas	El almacenamiento inadecuado de la información puede propiciar incendios en diversos puntos de los departamentos de la DGME	Uruca Oficinas Centrales	Externo
R279	Alta humedad	Existe posibilidad de que se presente alta	Riesgo ambiental	En caso de inundación, como se presenta en las épocas lluviosas,	Se pueden presentar corto circuitos eléctricos, fallo	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		humedad en diversos puntos del centro de datos de la DGME		pueden presentarse problemas de humedad en el piso falso del centro de datos	del hardware en el centro de datos		
R280	Alta temperatura	Los equipos del centro de datos generan niveles elevados de temperatura	Riesgo ambiental	En el caso que falle el sistema de control de temperatura del centro de datos	Fallo y daño de los equipos de hardware del centro de datos	Uruca Oficinas Centrales	Externo
R281	Peligro de inundación	Fallo en el sistema de drenajes de aguas llovidas	Riesgo ambiental	En temporada de invierno son frecuentes las inundaciones en las oficinas de la DGME	Daño de hardware del centro de datos	Uruca Oficinas Centrales	Externo
R282	Incumplimiento de la política de seguridad de la Institución	Existen una política documentadas de seguridad de la información; sin embargo, no se encuentra aprobada por la dirección	Riesgo operativo	Esta política de seguridad no ha sido aprobada por la dirección	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Interno
R283	Incumplimiento de la política y procedimientos de la Institución	Falta de documentación de las políticas y procedimientos de seguridad de la información	Riesgo operativo	No se encuentran documentadas las responsabilidades que tiene el personal de seguridad de la información	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Interno
R284	Incumplimiento de la política y procedimientos de la Institución	Falta de conocimiento y capacitación sobre las políticas y procedimientos organizacionales	Riesgo operativo	No todos los funcionarios de la Institución cuentan con el apropiado conocimiento, capacitación, actualización de las políticas y procedimientos organizacionales	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Interno
R285	Incumplimiento de la política y procedimientos de la Institución	Falta de procedimiento documentado para devolución de activos	Riesgo operativo	No existe un procedimiento documentado para la devolución de activos en caso de que el funcionario ya no labore en la Institución	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R286	Colisión de avión y carro, incendios e inundaciones	Ubicación de las instalaciones de las oficinas de la oficina central de la DGME	Riesgo operativo	La Institución se encuentra cerca de edificios o terrenos que pudieran provocar una detención de las actividades diarias como, por ejemplo: aeropuerto, los aviones pasan con frecuencia por encima de las instalaciones de la Institución, autopista a la par, fábrica POPS, cárcel, Rositer Carballo y río Virilla	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Externo
R287	Acceso físico no autorizado	Falta de control de acceso a algunas oficinas de la Institución	Riesgo humano	Algunas puertas de acceso de las oficinas de la Institución no cuentan con control de acceso	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Externo
R288	Acceso físico no autorizado	Inexistencia de mecanismos de alerta	Riesgo ambiental	El edificio no cuenta con los medios suficientes para alertar ante un incidente al personal (alarmas y luces de emergencia)	Interrupción o afectación de las operaciones críticas de la oficina afectada.	Uruca Oficinas Centrales	Externo
R289	Falla de hardware de red de los equipos de usuarios	El cableado estructurado en algunos equipos de usuarios es inadecuado	Riesgo tecnológico	La exposición del cableado de red de los equipos puede provocar falla en las comunicaciones de estos	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la oficina afectada	Uruca Oficinas Centrales	Externo
R290	Acceso físico no autorizado	Controles de acceso insuficientes a centro de datos	Riesgo humano	Para ingresar al centro de datos únicamente se cuenta con un control de acceso de tarjeta magnética	Interrupción o afectación de las operaciones críticas.	Uruca Oficinas Centrales	Externo

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R291	Acceso físico no autorizado	Puertas de acceso al centro de datos hechas de vidrio	Riesgo humano	Las puertas para ingresar al centro de datos son de vidrio. Existe un techo raso que permite ingresar al centro de datos a través del techo. Tres paredes donde se encuentra el centro de datos son de vidrio.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R292	Peligro de inundación	Ubicación de baños sobre el centro de datos	Riesgo ambiental	Existe un baño en un segundo piso sobre el centro de datos, específicamente, sobre los equipos de respaldo eléctricos UPS del centro de datos	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R293	Falla de hardware	Falta de redundancia en equipos de redes	Riesgo tecnológico	No existe redundancia en equipos de comunicación. Únicamente existe redundancia en el firewall.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R294	Falla en el suministro eléctrico	Falta de redundancia en la planta eléctrica	Riesgo tecnológico	No existe redundancia en la planta eléctrica de las oficinas centrales de la Institución	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R295	Falla en el suministro eléctrico	Dependencia eléctrica del centro de datos	Riesgo tecnológico	El sistema eléctrico del centro de datos no es independiente al del resto del edificio	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R296	Falla de hardware	Cableado estructurado inadecuado	Riesgo tecnológico	El cableado eléctrico y de comunicación no cuenta distribuido de manera adecuada	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R297	Acceso físico no autorizado	Inexistencia de alarmas contra intrusos	Riesgo humano	No hay alarmas de contra intruso.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R298	Falla de software	No existe ambientes de pruebas de	Riesgo tecnológico	No existe un ambiente de prueba o calidad	Interrupción o afectación de las operaciones	Uruca Oficinas Centrales	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
		software		para las aplicaciones de la Institución	críticas		
R299	Falla de hardware	Deficiencias en contratos de hardware con proveedores	Riesgo tecnológico	No existen contratos para suplir equipos dentro de un tiempo definido, por ejemplo se establece la criticidad de algunos sistemas de "menor o igual a una hora", pero el BCP no contempla acciones para operar en contingencia, y además, el DRP indica que el contrato con algunos proveedores establece un plazo de ocho horas para atender los problemas presentados en los servidores críticos, por lo que una hora establecida como tiempo máximo de restablecimiento de la operación en el BCP no podría cumplir con este tiempo de ninguna manera.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R300	Virus informáticos	Equipos servidores sin software antivirus	Riesgo tecnológico	Algunos servidores no tienen instalado el antivirus por requerimientos de las aplicaciones	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R301	Intrusos informáticos	Servidores sin parches de seguridad	Riesgo tecnológico	Los servidores Windows no se la instalan parches de seguridad por requerimientos de las aplicaciones.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R302	Incumplimiento de las	Políticas no publicadas	Riesgo tecnológico	Existen procedimientos de	Interrupción o afectación de	Uruca Oficinas	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	políticas y procedimientos de la Institución	adecuadamente		respaldo, pero no están publicados debido a que no existe una Intranet	las operaciones críticas	Centrales	
R303	Fallo de hardware	Falta de redundancia en servidores críticos	Riesgo tecnológico	El servidor URUCA 192.168.120.11 no posee alta disponibilidad o redundancia	Un fallo o daño en este equipo puede genera la interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R304	Incendio, terremoto, inundación, falla de hardware, intrusos y virus	Falta de mantenimiento al hardware	Riesgo ambiental	La unidad de respaldos y las cintas no reciben revisiones y mantenimientos periódicos	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R305	Incumplimiento de las políticas y procedimientos de la Institución	Falta de políticas y procedimientos	Riesgo operativo	No existen políticas y procedimientos documentados de intercambio de información entre sistemas y terceros	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R306	Fallo en el software	Uso de sistemas operativos obsoletos	Riesgo tecnológico	Existen muchos equipos Windows XP en uso para los usuarios de la Institución	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R307	Fallo en el software	Equipos sin parches de seguridad	Riesgo tecnológico	La mayoría de los equipos de los usuarios y servidores no cuentan con los parches de seguridad de sus sistemas operativos y aplicaciones	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R308	Fallo en el software	Sistemas operativos inadecuados para servidores	Riesgo tecnológico	Algunos servidores de la Institución funcionan con sistemas operativos Microsoft para el uso en estaciones de trabajo, por ejemplo, existen Windows XP y Windows 7 que hacen funciones	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				de servidor			
R309	Fallo en hardware y software	No hay redundancia en la SAN del centro de datos	Riesgo tecnológico	No existe redundancia en cuanto a la información almacenada en la SAN de la Institución en el centro de datos	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R310	Fallo en el software	Software instalado ilegalmente	Riesgo tecnológico	Los servidores de Oracle poseen una versión no autorizada para su uso	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R311	Incendio, terremoto, inundación, falla de hardware, intrusos y virus	Respaldo de servicios críticos inadecuados	Riesgo ambiental	El centro de datos no cuenta con servidores de respaldo que funcionen en caso de fallas en los equipos críticos principales	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Externo
R312	Incumplimiento de las políticas y procedimientos de la Institución	Políticas y procedimientos no aprobados	Riesgo operativo	Existe una política de control de acceso lógico documentada e implementada, sin embargo, aún se encuentra en proceso de aprobación.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R313	Intrusos, virus y accesos no autorizados	Falta de políticas y procedimientos	Riesgo tecnológico	No existe un procedimiento de manejo de incidentes documentado.	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R314	Intrusos, virus y accesos no autorizados	Falta de políticas y procedimientos	Riesgo tecnológico	No existe una mesa de servicio para el tratamiento de incidentes	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R315	Incumplimiento de las políticas y procedimientos de la Institución	Inexistencia de una base de datos del conocimiento.	Riesgo tecnológico	Inexistencia de una base de datos del conocimiento en la atención de incidentes de seguridad	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R316	Fallo en los enlaces de comunicac	Falta de redundancia en los enlaces de comunicación	Riesgo tecnológico	Se cuenta con una única empresa proveedora (ICE), para el manejo de	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	ión	entre oficinas centrales y las regionales		los enlaces de comunicación de toda la Institución			
R317	Humedad	Altos niveles de humedad	Riesgo ambiental	La oficina de archivo central de la Institución no cuenta con sensores de humedad	Daño y pérdida de información física	Uruca Oficinas Centrales	Externo
R318	Peligro de inundación	Exceso de goteras en la oficina de archivo central	Riesgo ambiental	El techo de esta oficina presenta constantes goteras	Daño y pérdida de información física	Uruca Oficinas Centrales	Externo
R319	Acceso físico no autorizado	Puerta de acceso principal abierta	Riesgo humano	Si bien, la puerta al archivo central cuenta con control de acceso de tarjetas magnéticas, esta se mantiene abierta para la entrada y salida de personal practicante, que no posee tarjetas de control de acceso	Daño y pérdida de información física	Uruca Oficinas Centrales	Externo
R320	Acceso físico no autorizado	Ubicación de cámaras de CCTV inadecuada	Riesgo humano	Si bien, al archivo central cuenta con CCTV, la ubicación de las cámaras de seguridad no es la adecuada	Daño y pérdida de información física	Uruca Oficinas Centrales	Externo
R321	Robo de información confidencial	Manipulación y almacenamiento de información física inadecuada	Riesgo operativo	En muchas de las oficinas de la Institución, los usuarios almacenan cajas de información confidencial en sus lugares de trabajo	Daño y pérdida de información física	Uruca Oficinas Centrales	Externo
R322	Incumplimiento de las políticas y procedimientos accesos y permisos	Equipos de usuarios finales no cumplen con requerimientos mínimos de software	Riesgo operativo	Muchos equipos de usuarios finales no están incluidos en el directorio activo de Microsoft Active Directory, ya que estos no cumplen con los requerimientos de sistema operativo mínimos	Instalación de software no autorizado, daño del software, problemas de administración de estos equipos.	Uruca Oficinas Centrales	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
				compatibles.			
R323	Incumplimiento de las políticas y procedimientos de la Institución	Falta de cultura de seguridad y riesgos de la información	Riesgo estratégico	Los funcionarios poseen un conocimiento limitado sobre la gestión de riesgos y seguridad de la información	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R324	Intrusos y virus	Equipos de consulados sin software antivirus	Riesgo tecnológico	Los equipos de los consulados no poseen software antivirus administrado por una consola central	Infección de equipos y afectación de las funciones y operaciones críticas	Uruca Oficinas Centrales	Interno
R325	Intrusos y virus	Existen equipos portátiles que no poseen el software de seguridad	Riesgo tecnológico	Existen equipos portátiles que no poseen el software de seguridad McAfee que posee la Institución.	Infección de equipos y afectación de las funciones y operaciones críticas	Uruca Oficinas Centrales	Interno
R326	Acceso lógico no autorizado	Configuraciones de acceso lógico inadecuadas en equipos informáticos	Riesgo tecnológico	Los equipos de los consulados mantienen contraseñas por defecto en las configuraciones de las Redes Privadas Virtuales (VPN) para el acceso a la red de la DGME	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R327	Fallo en hardware y software	Falta de segmentación de la red	Riesgo tecnológico	No existen políticas de segmentación de las redes lógicas de la Institución, hay equipos servidores en redes de equipos de usuarios	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R328	Incumplimiento de las políticas y procedimientos accesos y permisos	Documentación inadecuada de accesos y privilegios	Riesgo operativo	No hay registros formales por parte de los funcionarios de bases de datos, redes y servidores de los accesos y privilegios que poseen estos	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R329	Incumplimiento de las	Falta de políticas de	Riesgo operativo	Existe personal clave en algunas	Interrupción o afectación de	Uruca Oficinas	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
	políticas y procedimiento	segregación de funciones		funciones del departamento de TI que poseen conocimientos que solo ellos poseen	las operaciones críticas	Centrales	
R330	Fallo en hardware y software	Incumplimiento de mejoras prácticas	Riesgo operativo	El piso falso del centro de datos no cumple con la altura mínima requerida según las mejores prácticas	Interrupción o afectación de las operaciones críticas en caso de inundación o incendios	Uruca Oficinas Centrales	Interno
R331	Incumplimiento de las políticas y procedimiento	Inexistencia de planes de seguridad	Riesgo estratégico	La DGME no cuenta con un plan de Gestión de Seguridad de la Información (SGSI)	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R332	Incumplimiento de las políticas y procedimiento	Monitoreo inadecuado de los servicios prestados por GTI	Riesgo operativo	No existen políticas y procedimientos adecuados para el establecimiento del monitoreo continuo de los servicios que presta GTI a la DGME	Interrupción o afectación de las operaciones críticas	Uruca Oficinas Centrales	Interno
R333	Alta humedad	No hay sensores de humedad	Riesgo ambiental	Por la ubicación geográfica de la regional se mantiene niveles de humedad muy altos.	Daño de los activos físicos y lógicos de información	Regional de Peñas Blancas	Externo
R334	Acceso físico no autorizado	Material de las paredes de la regional	Riesgo humano	Muchas de las paredes de la regional están construidas de material liviano Gypsum	Accesos físicos no autorizados	Regional de Peñas Blancas	Externo
R335	Robo o pérdida de equipos informáticos	Ubicación de equipos computacionales en lugares no adecuados de fácil acceso	Riesgo financiero	Se observa que se puede tener acceso fácilmente a los equipos de las oficinas administrativas.	Robo o pérdida de hardware.	Regional de Peñas Blancas	Externo
R336	Fallo en el enlace de comunicaciones	Inexistencia de controles de acceso al gabinete principal	Riesgo operativo	El gabinete de comunicaciones y servidores se mantiene abierto.	Daño en el hardware de los equipos informáticos y de los equipos de comunicación	Regional de Peñas Blancas	Interno

ID Riesgo	Amenaza	Vulnerabilidad	Clasificación / Categoría	Condiciones	Consecuencias	Nombre de la regional	Origen de riesgo
R337	Falla de hardware de red de los equipos de usuarios	Instalación del cableado estructurado inadecuado y en mal estado	Riesgo tecnológico	Se pueden observar los cables de red de algunos equipos mal ubicados o instalados de manera no adecuada	Pérdida de comunicación de los equipos y los sistemas de información de la regional, así como la afectación de los servicios y operaciones críticas que brinda la regional	Regional de Peñas Blancas	Interno
R338	Pérdida de información física	Archivos físicos de información no están almacenados adecuadamente	Riesgo operativo	Algunos archivos físicos están ubicados en lugares de servicio al público, y no hay barreras que impidan el acceso a estas áreas	Daño o pérdida de información crítica de la regional	Regional de Peñas Blancas	Externo
R339	Incendio	No hay sensores ni sistemas contra incendios	Riesgo ambiental	La regional almacena mucha información física y no hay sensores de humo en ninguna oficina de la regional, además, no hay extintores para el control de incendios	Daño de los activos físicos y lógicos de información	Regional de Peñas Blancas	Interno
R340	Inundaciones	Existen problemas con el control de las aguas de lluvia	Riesgo ambiental	La regional posee importantes goteras debido a su mal estado.	Daño de los activos físicos y lógicos de información	Regional de Peñas Blancas	Externo

Anexo 6. Análisis de los riesgos para la DGME

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R001	Fallo de enlace principal de red	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R002	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R003	Fallo de red de los equipos institucionales de los usuarios	20%	2	0,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R004	Peligro de incendio	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R005	Fallo en el suministro eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R006	Ingreso de personal no autorizado	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R007	Robo de información confidencial	40%	4	1,60	01 - ACTIVACIÓN MITIGACIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R008	Acceso físico no autorizado	20%	2	0,40	01 - ACTIVACIÓN MITIGACIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R009	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R010	Fallo de equipos informáticos	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R011	Fallo de enlace principal de Red	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R012	Acceso físico no autorizado	20%	2	0,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R013	Peligro de incendio	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R014	Fallo en el suministro eléctrico	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R015	Robo de información confidencial	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R016	Fallo en equipos informáticos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R017	Inundaciones	80%	4	3,20	00 - EN GESTIÓN	Mitigación no satisfactoria
R018	Fallo en el fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R019	Acceso físico no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R020	Daño o pérdida de información física	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R021	Fallo de hardware	60%	4	2,40	00 - EN GESTIÓN	Gestión
R022	Incendio	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R023	Robo de hardware	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R024	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R025	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R026	Fallo en equipos informáticos	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R027	Incendio y material peligroso para el Hardware	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R028	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R029	Falla de hardware de red de los equipos de usuarios	60%	2	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R030	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R031	Fallo en fluido eléctrico	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R032	Daño o pérdida de información física	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R033	Fallo de hardware	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R034	Robo o pérdida de equipos informáticos	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R035	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						correctivas si el riesgo ocurre)
R036	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R037	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R038	Ingreso de personal no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R039	Fallo de cableado de red de datos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R040	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R041	Exceso de polvo en el ambiente	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R042	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R043	Fallo en fluido eléctrico	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R044	Robo o pérdida de equipos informáticos	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R045	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R046	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R047	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R048	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R049	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R050	Alta temperatura	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R051	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R052	Ingreso de personal no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R053	Robo o pérdida de equipos informáticos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R054	Fallo en fluido eléctrico	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R055	Fallo en el enlace de comunicaciones	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R056	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R057	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R058	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R059	Inundación	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R060	Acceso físico no autorizado	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R061	Robo o pérdida de equipos informáticos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						correctivas si el riesgo ocurre)
R062	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R063	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R064	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R065	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R066	Incendio	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R067	Ingreso de personal no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R068	Acceso físico no autorizado	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R069	Robo o pérdida de equipos informáticos	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R070	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R071	Fallo en el enlace de comunicaciones	20%	4	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R072	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R073	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R074	Incendio	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R075	Acceso físico no autorizado	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R076	Acceso lógico no autorizado	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R077	Robo o pérdida de equipos informáticos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R078	Acceso físico no autorizado a bodega de archivos	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R079	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R080	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R081	Fallo en fluido eléctrico	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R082	Exceso de polvo en el ambiente	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R083	Acceso físico no autorizado en rack de comunicaciones	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R084	Robo o pérdida de archivos físicos	60%	6	3,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R085	Material contaminante en el centro de datos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R086	Fallo del enlace principal de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R087	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R088	Alta temperatura	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R089	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R090	Ingreso de personal no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R091	Robo o pérdida de equipos informáticos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R092	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R093	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R094	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R095	Pérdida de información física	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R096	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R097	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R098	Acceso físico no autorizado	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R099	Robo o pérdida de equipos informáticos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R100	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R101	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R102	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R103	Pérdida de información física	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R104	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R105	Inundaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R106	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R107	Alta temperatura	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R108	Acceso físico no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R109	Ingreso de personal no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R110	Robo o pérdida de equipos informáticos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R111	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R112	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R113	Falla de hardware de red de los equipos de usuarios	60%	2	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R114	Pérdida de información física	80%	2	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R115	Incendio	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R116	Inundación	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R117	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R118	Acceso físico no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R119	Robo o pérdida de equipos informáticos	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R120	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R121	Fallo en el enlace de comunicaciones	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R122	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R123	Pérdida de información física	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R124	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R125	Inundación	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R126	Alta humedad	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R127	Acceso físico no autorizado	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R128	Robo o pérdida de equipos informáticos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R129	Fallo en fluido eléctrico	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R130	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R131	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R132	Pérdida de información física	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R133	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R134	Alta temperatura	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R135	Acceso físico no autorizado	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R136	Pérdida de información física	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R137	Robo o pérdida de equipos informáticos	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R138	Alta humedad	40%	4	1,60	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R139	Ataque digital de aplicación (FID 9310)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R140	Ataque digital de aplicación (FID 9328)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R141	Ataque digital de aplicación (FID 9329)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R142	Ataque digital de aplicación (FID 9330)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R143	Ataque digital de aplicación (FID 9335)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R144	Ataque digital de aplicación (FID 21706)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R145	Ataque digital de aplicación (FID 13016)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R146	Ataque digital de aplicación (FID 12096)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R147	Ataque digital de aplicación (FID 17281)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R148	Ataque digital de aplicación (FID 17967)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R149	Ataque digital de aplicación (FID 18179)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R150	Ataque digital de aplicación (FID 20465)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R151	Ataque digital de aplicación (FID 6360)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R152	Ataque digital de aplicación (FID 1859)	20%	6	1,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R153	Ataque digital de aplicación (FID 13016)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R154	Ataque digital de aplicación (FID 21706)	60%	8	4,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R155	Ataque digital de aplicación (FID 13016)	60%	8	4,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R156	Ataque digital de aplicación (FID 10385)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R157	Ataque digital de aplicación (FID 21706)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R158	Ataque digital de aplicación (FID 13016)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R159	Ataque digital de aplicación (FID 18213)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R160	Ataque digital de aplicación (FID 21706)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R161	Ataque digital de aplicación (FID 21706)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R162	Ataque digital de aplicación (FID 9329)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R163	Ataque digital de aplicación (FID 9335)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R164	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R165	Ataque digital de aplicación (FID 9330)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R166	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R167	Ataque digital de aplicación (FID 9335)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R168	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R169	Ataque digital de aplicación (FID 9310)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R170	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R171	Ataque digital de aplicación (FID 5182)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R172	Ataque digital de aplicación (FID 20465)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R173	Ataque digital de aplicación (FID 17281)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R174	Ataque digital de aplicación (FID 18179)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R175	Ataque digital de aplicación (FID 6360)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R176	Ataque digital de aplicación (FID 1859)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R177	Ataque digital de aplicación (FID 9310)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R178	Ataque digital de aplicación (FID 21660)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R179	Ataque digital de aplicación (FID 21660)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R180	Ataque digital de aplicación (FID 18213)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R181	Ataque digital de aplicación (FID 6533)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R182	Ataque digital de aplicación (FID 6467)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R183	Ataque digital de aplicación (FID 6532)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R184	Ataque digital de aplicación (FID 7659)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R185	Ataque digital de aplicación (FID 6458)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R186	Ataque digital de aplicación (FID 6469)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R187	Ataque digital de aplicación (FID 6476)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R188	Ataque digital de aplicación (FID 6485)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R189	Ataque digital de aplicación (FID 6491)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R190	Ataque digital de aplicación (FID 6511)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R191	Ataque digital de aplicación (FID 6524)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R192	Ataque digital de aplicación (FID 6526)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R193	Ataque digital de aplicación (FID 6532)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R194	Ataque digital de aplicación (FID 6533)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R195	Ataque digital de aplicación (FID 6534)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R196	Ataque digital de aplicación (FID 6540)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R197	Ataque digital de aplicación (FID 6614)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R198	Ataque digital de aplicación (FID 6851)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R199	Ataque digital de aplicación (FID 7070)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R200	Ataque digital de aplicación (FID 7071)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R201	Ataque digital de aplicación (FID 7266)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R202	Ataque digital de aplicación (FID 7659)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R203	Ataque digital de aplicación (FID 7661)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R204	Ataque digital de aplicación (FID 7818)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R205	Ataque digital de aplicación (FID 13564)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R206	Ataque digital de aplicación (FID 14978)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R207	Ataque digital de aplicación (FID 12851)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R208	Ataque digital de aplicación (FID 14627)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R209	Ataque digital de aplicación (FID 9759)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R210	Ataque digital de aplicación (FID 6014)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R211	Ataque digital de aplicación (FID 6182)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R212	Ataque digital de aplicación (FID 15315)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R213	Ataque digital de aplicación (FID 6382)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R214	Ataque digital de aplicación (FID 5570)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R215	Ataque digital de aplicación (FID 5571)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R216	Ataque digital de aplicación (FID 5675)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R217	Ataque digital de aplicación (FID 5834)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R218	Ataque digital de aplicación (FID 10424)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R219	Ataque digital de aplicación (FID 12395)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R220	Ataque digital de aplicación (FID 13917)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R221	Ataque digital de aplicación (FID 14277)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R222	Ataque digital de aplicación (FID 11925)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R223	Ataque digital de aplicación (FID 11126)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R224	Ataque digital de aplicación (FID 13226)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R225	Ataque digital de aplicación (FID 2195)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R226	Ataque digital de aplicación (FID 972)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R227	Ataque digital de aplicación (FID 12848)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R228	Ataque digital de aplicación (FID 13638)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R229	Ataque digital de aplicación (FID 10436)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R230	Ataque digital de aplicación (FID 10437)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R231	Ataque digital de aplicación (FID 13997)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R232	Ataque digital de aplicación (FID 673)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R233	Ataque digital de aplicación (FID 832)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R234	Ataque digital de aplicación (FID 10444)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R235	Ataque digital de aplicación (FID 10439)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R236	Ataque digital de aplicación (FID 790)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R237	Ataque digital de aplicación (FID 2638)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R238	Ataque digital de aplicación (FID 2900)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R239	Ataque digital de aplicación (FID 1905)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R240	Ataque digital de aplicación (FID 21706)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R241	Ataque digital de aplicación (FID 2200)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R242	Ataque digital de aplicación (FID 13016)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R243	Ataque digital de aplicación (FID 8211)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R244	Ataque digital de aplicación (FID 21706)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R245	Ataque digital de aplicación (FID 4522)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R246	Ataque digital de aplicación (FID 4550)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R247	Ataque digital de aplicación (FID 4460)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R248	Ataque digital de aplicación (FID 10125)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R249	Ataque digital de aplicación (FID 12824)	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R250	Ataque digital de aplicación (FID 13638)	40%	8	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R251	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R252	Ataque digital de aplicación (FID 5182)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R253	Ataque digital de aplicación (FID 17281)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R254	Ataque digital de aplicación (FID 17967)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R255	Ataque digital de aplicación (FID 18179)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R256	Ataque digital de aplicación (FID 20465)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R257	Ataque digital de aplicación (FID 1859)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R258	Ataque digital de aplicación (FID 6360)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R259	Ataque digital de aplicación (FID 20915)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R260	Ataque digital de aplicación (FID 21706)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R261	Ataque digital de aplicación (FID 19731)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R262	Ataque digital de aplicación (FID 21106)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R263	Ataque digital de aplicación (FID 18355)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R264	Ataque digital de aplicación (FID 12824)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R265	Ataque digital de aplicación (FID 14508)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R266	Ataque digital de aplicación (FID 17281)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R267	Ataque digital de aplicación (FID 17880)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R268	Ataque digital de aplicación (FID 17967)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R269	Ataque digital de aplicación (FID 18179)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R270	Ataque digital de aplicación (FID 18384)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R271	Ataque digital de aplicación (FID 20849)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R272	Ataque digital de aplicación (FID 21669)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R273	Ataque digital de aplicación (FID 20465)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R274	Ataque digital de aplicación (FID 1859)	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R275	Ataque digital de aplicación (FID 10385)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R276	Ataque digital de aplicación (FID 21706)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R277	Ataque digital de aplicación (FID 13016)	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R278	Peligro de incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R279	Alta humedad	100%	2	2,00	99 - CERRADO	El riesgo ha sido mitigado / La contingencia ha sido satisfactoria
R280	Alta temperatura	100%	2	2,00	99 - CERRADO	El riesgo ha sido mitigado / La contingencia ha sido satisfactoria
R281	Peligro de inundación	80%	10	8,00	00 - EN GESTIÓN	Gestión
R282	Incumplimiento de la política de seguridad de la Institución	40%	6	2,40	00 - EN GESTIÓN	Gestión
R283	Incumplimiento de la política y procedimientos de la Institución	60%	6	3,60	00 - EN GESTIÓN	Gestión
R284	Incumplimiento de la política y procedimientos de la Institución	60%	6	3,60	00 - EN GESTIÓN	Gestión
R285	Incumplimiento de la política y procedimientos de la Institución	60%	6	3,60	00 - EN GESTIÓN	Gestión
R286	Colisión de avión y carro, incendios e inundaciones	40%	10	4,00	00 - EN GESTIÓN	Gestión

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R287	Acceso físico no autorizado	60%	6	3,60	00 - EN GESTIÓN	Gestión
R288	Acceso físico no autorizado	60%	8	4,80	00 - EN GESTIÓN	Gestión
R289	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R290	Acceso físico no autorizado	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R291	Acceso físico no autorizado	60%	10	6,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R292	Peligro de inundación	80%	10	8,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R293	Falla de hardware	60%	8	4,80	00 - EN GESTIÓN	Gestión
R294	Falla en el suministro eléctrico	60%	8	4,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R295	Falla en el suministro eléctrico	60%	8	4,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R296	Falla de hardware	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R297	Acceso físico no autorizado	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R298	Falla de software	80%	10	8,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R299	Falla de hardware	80%	10	8,00	00 - EN GESTIÓN	Gestión
R300	Virus informáticos	40%	8	3,20	00 - EN GESTIÓN	Gestión
R301	Intrusos informáticos	40%	10	4,00	00 - EN GESTIÓN	Gestión
R302	Incumplimiento de las políticas y procedimientos de la Institución	60%	8	4,80	00 - EN GESTIÓN	Gestión
R303	Fallo de hardware	60%	10	6,00	00 - EN GESTIÓN	Gestión
R304	Incendio, terremoto, inundación, falla de hardware, intrusos y virus	40%	6	2,40	00 - EN GESTIÓN	Gestión
R305	Incumplimiento de las políticas y procedimientos de la Institución	40%	6	2,40	00 - EN GESTIÓN	Gestión

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R306	Fallo en el software	60%	6	3,60	00 - EN GESTIÓN	Gestión
R307	Fallo en el software	40%	10	4,00	00 - EN GESTIÓN	Gestión
R308	Fallo en el software	60%	10	6,00	00 - EN GESTIÓN	Gestión
R309	Fallo en hardware y software	40%	10	4,00	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R310	Fallo en el software	60%	10	6,00	00 - EN GESTIÓN	Gestión
R311	Incendio, terremoto, inundación, falla de hardware, intrusos y virus	40%	10	4,00	00 - EN GESTIÓN	Gestión
R312	Incumplimiento de las políticas y procedimientos de la Institución	60%	8	4,80	00 - EN GESTIÓN	Gestión
R313	Intrusos, virus y accesos no autorizados	80%	10	8,00	00 - EN GESTIÓN	Gestión
R314	Intrusos, virus y accesos no autorizados	80%	10	8,00	00 - EN GESTIÓN	Gestión
R315	Incumplimiento de las políticas y procedimientos de la Institución	80%	6	4,80	00 - EN GESTIÓN	Gestión

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R316	Fallo en los enlaces de comunicación	60%	10	6,00	00 - EN GESTIÓN	Gestión
R317	Humedad	60%	6	3,60	00 - EN GESTIÓN	Gestión
R318	Peligro de inundación	80%	6	4,80	00 - EN GESTIÓN	Gestión
R319	Acceso físico no autorizado	60%	6	3,60	00 - EN GESTIÓN	Gestión
R320	Acceso físico no autorizado	40%	6	2,40	00 - EN GESTIÓN	Gestión
R321	Robo de información confidencial	20%	6	1,20	00 - EN GESTIÓN	Gestión
R322	Incumplimiento de las políticas y procedimientos accesos y permisos	80%	6	4,80	00 - EN GESTIÓN	Gestión
R323	Incumplimiento de las políticas y procedimientos de la Institución	60%	6	3,60	00 - EN GESTIÓN	Gestión
R324	Intrusos y virus	80%	8	6,40	00 - EN GESTIÓN	Gestión
R325	Intrusos y virus	80%	8	6,40	00 - EN GESTIÓN	Gestión
R326	Acceso lógico no autorizado	100%	8	8,00	00 - EN GESTIÓN	Gestión
R327	Fallo en hardware y software	80%	10	8,00	00 - EN GESTIÓN	Gestión

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
R328	Incumplimiento de las políticas y procedimientos accesos y permisos	40%	6	2,40	00 - EN GESTIÓN	Gestión
R329	Incumplimiento de las políticas y procedimiento	40%	10	4,00	00 - EN GESTIÓN	Gestión
R330	Fallo en hardware y software	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R331	Incumplimiento de las políticas y procedimiento	40%	8	3,20	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R332	Incumplimiento de las políticas y procedimiento	80%	8	6,40	00 - EN GESTIÓN	Gestión
R333	Alta humedad	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R334	Acceso físico no autorizado	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R335	Robo o pérdida de equipos informáticos	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R336	Fallo en el enlace de comunicaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R337	Falla de hardware de red de los equipos de usuarios	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo

ID Riesgo	Título	Probabilidad (Porcentaje)	Impacto (Numérico)	Exposición (Numérico)	Estado	Motivo
						ocurre)
R338	Pérdida de información física	40%	2	0,80	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R339	Incendio	40%	6	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)
R340	Inundaciones	60%	4	2,40	00 - EN GESTIÓN	Asumido (se toman acciones correctivas si el riesgo ocurre)

Anexo 7. Análisis de los controles.

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R017	Inundaciones	Elaborar un plan para la posibilidad de ubicar la oficina de la regional en un lugar donde no exista el riesgo de inundaciones	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R084	Robo o pérdida de archivos físicos	Reubicar la información física almacenada inadecuadamente y resguardarla en archiveros bajo llaves, especialmente los archivos de CIERRE DE VUELOS	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo
R153	Ataque digital de aplicación (FID 13016)	Deshabilitar la cuenta “Guest" que posean contraseñas en blanco según la referencia CVE-1999-0519	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R154	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R155	Ataque digital de aplicación (FID 13016)	Deshabilitar la cuenta “Guest" que posean contraseñas en blanco según la referencia CVE-1999-0519	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R156	Ataque digital de aplicación (FID 10385)	Aplicar parche de seguridad de la referencia CVE-2010-2729	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R157	Ataque digital de	Aplicar parche de seguridad	Control clave	Medida de control	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
	aplicación (FID 21706)	de la referencia CVE-2017-0143		inexistente			
R158	Ataque digital de aplicación (FID 13016)	Deshabilitar la cuenta “Guest" que posean contraseñas en blanco según la referencia CVE-1999-0519	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R159	Ataque digital de aplicación (FID 18213)	Aplicar parche de seguridad de la referencia CVE-2015-1635	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R160	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R161	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R162	Ataque digital de aplicación (FID 9329)	Aplicar parche de seguridad de la referencia CVE-2008-3014	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R163	Ataque digital de aplicación (FID 9335)	Aplicar parche de seguridad de la referencia CVE-2007-5348	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R164	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R165	Ataque digital de aplicación (FID 9330)	Aplicar parche de seguridad de la referencia CVE-2008-3015	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R166	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R167	Ataque digital de	Aplicar parche de seguridad	Control clave	Medida de control	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
	aplicación (FID 9335)	de la referencia CVE-2007-5348		inexistente			
R168	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R169	Ataque digital de aplicación (FID 9310)	Aplicar parche de seguridad de la referencia CVE-2008-3012	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R170	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R171	Ataque digital de aplicación (FID 5182)	Aplicar parche de seguridad de la referencia CVE-2007-2897	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R172	Ataque digital de aplicación (FID 20465)	Aplicar parche de seguridad de la referencia CVE-2016-2183	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R173	Ataque digital de aplicación (FID 17281)	Aplicar parche de seguridad de la referencia CVE-2014-3566	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R174	Ataque digital de aplicación (FID 18179)	Desactivar la suite RC4 en el protocolo TLS/SSL del servidor según la referencia CVE-2015-2808	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R175	Ataque digital de aplicación (FID 6360)	Aplicar parche de seguridad de la referencia CVE-2004-2761	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R176	Ataque digital de aplicación (FID 1859)	Aplicar parche de seguridad	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R177	Ataque digital de	Aplicar parche de seguridad	Control clave	Medida de control	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
	aplicación (FID 9310)	de la referencia CVE-2008-3012		inexistente			
R178	Ataque digital de aplicación (FID 21660)	Aplicar parche de seguridad de la referencia CVE-2017-7269	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R179	Ataque digital de aplicación (FID 21660)	Aplicar parche de seguridad de la referencia CVE-2017-7269	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R180	Ataque digital de aplicación (FID 18213)	Aplicar parche de seguridad de la referencia CVE-2015-1635	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R181	Ataque digital de aplicación (FID 6533)	Aplicar parche de seguridad de la referencia CVE-2007-5530	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R182	Ataque digital de aplicación (FID 6467)	Aplicar parche de seguridad de la referencia CVE-2008-0340	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R183	Ataque digital de aplicación (FID 6532)	Aplicar parche de seguridad de la referencia CVE-2007-5531	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R184	Ataque digital de aplicación (FID 7659)	Aplicar parche de seguridad de la referencia CVE-2010-0071	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R185	Ataque digital de aplicación (FID 6458)	Aplicar parche de seguridad de la referencia CVE-2008-0339	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R186	Ataque digital de aplicación (FID 6469)	Aplicar parche de seguridad de la referencia CVE-2008-0342	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R187	Ataque digital de aplicación (FID 6476)	Aplicar parche de seguridad de la referencia CVE-2008-	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		0344					
R188	Ataque digital de aplicación (FID 6485)	Aplicar parche de seguridad de la referencia CVE-2008-0347	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R189	Ataque digital de aplicación (FID 6491)	Aplicar parche de seguridad de la referencia CVE-2007-5505	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R190	Ataque digital de aplicación (FID 6511)	Aplicar parche de seguridad de la referencia CVE-2007-5508	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R191	Ataque digital de aplicación (FID 6524)	Aplicar parche de seguridad de la referencia CVE-2007-5512	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R192	Ataque digital de aplicación (FID 6526)	Aplicar parche de seguridad de la referencia CVE-2007-5514	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R193	Ataque digital de aplicación (FID 6532)	Aplicar parche de seguridad de la referencia CVE-2007-5531	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R194	Ataque digital de aplicación (FID 6533)	Aplicar parche de seguridad de la referencia CVE-2007-5530	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R195	Ataque digital de aplicación (FID 6534)	Aplicar parche de seguridad de la referencia CVE-2007-3853	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R196	Ataque digital de aplicación (FID 6540)	Aplicar parche de seguridad de la referencia CVE-2007-3855	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R197	Ataque digital de aplicación (FID 6614)	Aplicar parche de seguridad de la referencia CVE-2009-0972	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R198	Ataque digital de aplicación (FID 6851)	Aplicar parche de seguridad de la referencia CVE-2009-0217	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R199	Ataque digital de aplicación (FID 7070)	Aplicar parche de seguridad de la referencia CVE-2009-1020	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R200	Ataque digital de aplicación (FID 7071)	Aplicar parche de seguridad de la referencia CVE-2009-1019	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R201	Ataque digital de aplicación (FID 7266)	Aplicar parche de seguridad de la referencia CVE-2009-1007	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R202	Ataque digital de aplicación (FID 7659)	Aplicar parche de seguridad de la referencia CVE-2010-0071	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R203	Ataque digital de aplicación (FID 7661)	Aplicar parche de seguridad de la referencia CVE-2009-3415	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R204	Ataque digital de aplicación (FID 7818)	Aplicar parche de seguridad de la referencia CVE-2009-1996	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R205	Ataque digital de aplicación (FID 13564)	Aplicar parche de seguridad de la referencia CVE-2012-0552	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R206	Ataque digital de aplicación (FID 14978)	Aplicar parche de seguridad de la referencia CVE-2013-1534	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R207	Ataque digital de aplicación (FID 12851)	Aplicar parche de seguridad de la referencia CVE-2011-3512	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R208	Ataque digital de	Aplicar parche de seguridad	Control clave	Medida de control	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
	aplicación (FID 14627)	de la referencia CVE-2012-3220		inexistente			
R209	Ataque digital de aplicación (FID 9759)	Aplicar parche de seguridad de la referencia CVE-2010-0853	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R210	Ataque digital de aplicación (FID 6014)	Aplicar parche de seguridad de la referencia CVE-2007-1359	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R211	Ataque digital de aplicación (FID 6182)	Aplicar parche de seguridad de la referencia CVE-2008-2588	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R212	Ataque digital de aplicación (FID 15315)	Aplicar parche de seguridad de la referencia CVE-2013-3751	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R213	Ataque digital de aplicación (FID 6382)	Aplicar parche de seguridad de la referencia CVE-2008-2623	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R214	Ataque digital de aplicación (FID 5570)	Aplicar parche de seguridad de la referencia CVE-2007-2135	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R215	Ataque digital de aplicación (FID 5571)	Aplicar parche de seguridad de la referencia CVE-2007-2135	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R216	Ataque digital de aplicación (FID 5675)	Aplicar parche de seguridad de la referencia CVE-2007-2135	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R217	Ataque digital de aplicación (FID 5834)	Aplicar parche de seguridad de la referencia CVE-2008-1811	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R218	Ataque digital de aplicación (FID 10424)	Aplicar parche de seguridad de la referencia CVE-2010-	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		2390					
R219	Ataque digital de aplicación (FID 12395)	Aplicar parche de seguridad de la referencia CVE-2011-2239	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R220	Ataque digital de aplicación (FID 13917)	Aplicar parche de seguridad de la referencia CVE-2012-1737 CVE-2012-1745 CVE-2012-1746 CVE-2012-1747 CVE-2012-3134	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R221	Ataque digital de aplicación (FID 14277)	Aplicar parche de seguridad de la referencia CVE-2012-3137	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R222	Ataque digital de aplicación (FID 11925)	Aplicar parche de seguridad de la referencia CVE-2011-0792	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R223	Ataque digital de aplicación (FID 11126)	Aplicar parche de seguridad de la referencia CVE-2010-3600	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R224	Ataque digital de aplicación (FID 13226)	Aplicar parche de seguridad de la referencia CVE-2012-0082	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R225	Ataque digital de aplicación (FID 2195)	Aplicar parche de seguridad de la referencia CVE-1999-0103	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R226	Ataque digital de aplicación (FID 972)	Aplicar parche de seguridad de la referencia CVE-2015-5346	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R227	Ataque digital de aplicación (FID 12848)	Aplicar parche de seguridad de la referencia CVE-2011-	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		2301					
R228	Ataque digital de aplicación (FID 13638)	Aplicar parche de seguridad de la referencia CVE-2012-1675	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R229	Ataque digital de aplicación (FID 10436)	Aplicar parche de seguridad de la referencia CVE-2010-2419	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R230	Ataque digital de aplicación (FID 10437)	Aplicar parche de seguridad de la referencia CVE-2010-1321	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R231	Ataque digital de aplicación (FID 13997)	Aplicar parche de seguridad de la referencia CVE-2012-3132	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R232	Ataque digital de aplicación (FID 673)	Aplicar parche de seguridad de la referencia CVE-1999-0103	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R233	Ataque digital de aplicación (FID 832)	Aplicar parche de seguridad de la referencia CVE-2000-0539	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R234	Ataque digital de aplicación (FID 10444)	Aplicar parche de seguridad de la referencia CVE-2010-2411	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R235	Ataque digital de aplicación (FID 10439)	Aplicar parche de seguridad de la referencia CVE-2010-2415	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R236	Ataque digital de aplicación (FID 790)	Aplicar parche de seguridad de la referencia CVE-2007-5530	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R250	Ataque digital de aplicación (FID 13638)	Aplicar parche de seguridad de la referencia CVE-2012-1675	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R251	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R252	Ataque digital de aplicación (FID 5182)	Aplicar parche de seguridad de la referencia CVE-2007-2897	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R253	Ataque digital de aplicación (FID 17281)	Aplicar parche de seguridad de la referencia CVE-2014-3566	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R254	Ataque digital de aplicación (FID 17967)	Aplicar parche de seguridad de la referencia CVE-2015-0204 CVE-2015-1067 CVE-2015-1637	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R255	Ataque digital de aplicación (FID 18179)	Desactivar la suite RC4 en el protocolo TLS/SSL del servidor según la referencia CVE-2015-2808	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R256	Ataque digital de aplicación (FID 20465)	Aplicar parche de seguridad de la referencia CVE-2016-2183	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R257	Ataque digital de aplicación (FID 1859)	Aplicar parche de seguridad	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R258	Ataque digital de aplicación (FID 6360)	Aplicar parche de seguridad de la referencia CVE-2004-2761	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R259	Ataque digital de aplicación (FID 20915)	Aplicar parche de seguridad de la referencia CVE-2016-8735	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R260	Ataque digital de aplicación	Aplicar parche de seguridad de la referencia	Control clave	Medida de control inexistent	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
	(FID 21706)	CVE-2017-0143		e			
R261	Ataque digital de aplicación (FID 19731)	Aplicar parche de seguridad de la referencia CVE-2015-5174	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R262	Ataque digital de aplicación (FID 21106)	Aplicar parche de seguridad de la referencia CVE-2016-8745	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R263	Ataque digital de aplicación (FID 18355)	Aplicar parche de seguridad de la referencia CVE-2014-0230	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R264	Ataque digital de aplicación (FID 12824)	Aplicar parche de seguridad de la referencia CVE-2007-6750	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R265	Ataque digital de aplicación (FID 14508)	Aplicar parche de seguridad de la referencia CVE-2012-5568	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R266	Ataque digital de aplicación (FID 17281)	Aplicar parche de seguridad de la referencia CVE-2014-3566	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R267	Ataque digital de aplicación (FID 17880)	Aplicar parche de seguridad de la referencia CVE-2014-0227	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R268	Ataque digital de aplicación (FID 17967)	Aplicar parche de seguridad de la referencia CVE-2015-0204 CVE-2015-1067 CVE-2015-1637	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R269	Ataque digital de aplicación (FID 18179)	Desactivar la suite RC4 en el protocolo TLS/SSL del servidor según la referencia CVE-2015-	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		2808					
R270	Ataque digital de aplicación (FID 18384)	Aplicar parche de seguridad de la referencia CVE-2014-7810	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R271	Ataque digital de aplicación (FID 20849)	Aplicar parche de seguridad de la referenciaCVE-2016-0762	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R272	Ataque digital de aplicación (FID 21669)	Aplicar parche de seguridad de la referencia CVE-2017-5647	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R273	Ataque digital de aplicación (FID 20465)	Aplicar parche de seguridad de la referencia CVE-2016-2183	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R274	Ataque digital de aplicación (FID 1859)	Aplicar parche de seguridad	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R275	Ataque digital de aplicación (FID 10385)	Aplicar parche de seguridad de la referencia CVE-2010-2729	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R276	Ataque digital de aplicación (FID 21706)	Aplicar parche de seguridad de la referencia CVE-2017-0143	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R277	Ataque digital de aplicación (FID 13016)	Deshabilitar la cuenta "Guest" que posean contraseñas en blanco según la referencia CVE-1999-0519	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R281	Peligro de inundación	Realizar un plan de mejora y corrección de los problemas que se presentan en los drenajes de aguas negras y	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		llovidas que se presentan en las épocas de lluvia					
R283	Incumplimiento de la política y procedimientos de la Institución	Verificar el cumplimiento de las políticas de documentación de las responsabilidades de los funcionarios de seguridad de la información	Control no clave	Medida de control pobre	Medio	Bajo	Costo positivo
R284	Incumplimiento de la política y procedimientos de la Institución	Elaborar un plan de capacitación sobre la cultura de seguridad de la información que abarque a todo el personal de la DGME	Control no clave	Medida de control pobre	Medio	Medio	Costo razonable
R285	Incumplimiento de la política y procedimientos de la Institución	Elaborar un plan sobre el manejo en la devolución de los activos por parte del Departamento de Seguridad de la Información	Control clave	Medida de control adecuada	Alto	Bajo	Costo positivo
R286	Colisión de avión y carro, incendios e inundaciones	Acelerar el plan de adquisición de un centro alterno para la DGME.	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R287	Acceso físico no autorizado	Instalar sistemas de control de acceso con tarjetas magnéticas en las puertas de acceso a lugares donde están presentes activos críticos	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		que aún no cuentan con este sistema					
R288	Acceso físico no autorizado	Instalar sistemas de alertas contra intrusos	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R290	Acceso físico no autorizado	Implementar algún sistema complementario de control de acceso al centro de datos, como el acceso biométrico por huella digital	Control no clave	Medida de control adecuada	Alto	Alto	Costo razonable
R291	Acceso físico no autorizado	Valorar el cambio del tipo de puertas para ingresar al centro de datos.	Control no clave	Medida de control adecuada	Alto	Medio	Costo positivo
R292	Peligro de inundación	Valorar la reubicación de las pilas sanitarias que se encuentran sobre el centro de datos.	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R293	Falla de hardware	Implementar sistemas de alta disponibilidad y redundancia en los activos de hardware críticos en la red de la DGME	Control clave	Medida de control pobre	Alto	Alto	Costo razonable
R294	Falla en el suministro eléctrico	Valorar la opción para implementar una planta eléctrica redundante.	Control no clave	Medida de control adecuada	Alto	Alto	Costo razonable

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R295	Falla en el suministro eléctrico	Implementar un sistema eléctrico en el centro de datos que sea independiente del resto del edificio de la DGME	Control no clave	Medida de control adecuada	Alto	Alto	Costo razonable
R296	Falla de hardware	Elaborar un plan de mejora y reestructuración del cableado estructurado del centro de datos	Control no clave	Medida de control adecuada	Alto	Medio	Costo positivo
R297	Acceso físico no autorizado	Implementar un sistema contra intrusos con alarmas en el centro de datos	Control no clave	Medida de control adecuada	Alto	Medio	Costo positivo
R298	Falla de software	Implementar un ambiente de pruebas para el software que la DGME adquiere y desarrolla	Control no clave	Medida de control inexistente	Alto	Alto	Costo razonable
R299	Falla de hardware	Revisar y modificar los contratos con proveedores con respecto al BCO, DRP y BIA, podría valorarse modificar estos últimos tres en función a los tiempos de respuesta y la inclusión de la operación en contingencia para los servicios y activos críticos que no están establecidos correctamente en estos planes	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R300	Virus informáticos	Instalar software antivirus en todos los servidores que aún no lo tienen instalado	Control clave	Medida de control adecuada	Alto	Bajo	Costo positivo
R301	Intrusos informáticos	Establecer un plan de actualizaciones automáticas con el sistema Microsoft WSUS que posee la DGME y este debería de abarcar a todos los equipos informáticos	Control no clave	Medida de control pobre	Alto	Bajo	Costo positivo
R302	Incumplimiento de las políticas y procedimientos de la Institución	Publicar las políticas de respaldo de los sistemas críticos en la intranet de la Institución	Control no clave	Medida de control adecuada	Medio	Bajo	Costo positivo
R303	Fallo de hardware	Implementar alta disponibilidad para el servidor URUCA 192.168.120.11	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R306	Fallo en el software	Agilizar el proceso de migración de sistemas operativos obsoletos con los que cuentan muchos de los equipos de los usuarios de toda la DGME	Control clave	Medida de control pobre	Alto	Alto	Costo razonable
R307	Fallo en el software	Establecer un plan de actualizaciones automáticas con el sistema Microsoft WSUS que posee la DGME y este debería	Control clave	Medida de control inexistente	Medio	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		de abarcar a todos los equipos informáticos					
R308	Fallo en el software	Implementar un plan de migración de los servidores que poseen sistemas operativos para estación de trabajo	Control clave	Medida de control pobre	Medio	Medio	Costo razonable
R309	Fallo en hardware y software	Adquirir un sistema de almacenamiento SAN como respaldo de la que posee el centro de datos	Control no clave	Medida de control adecuada	Alto	Alto	Costo razonable
R310	Fallo en el software	Adquirir las licencias de Oracle para el servidor de base de datos, para que puedan contar con las actualizaciones y soporte por parte del fabricante	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R311	Incendio, terremoto, inundación, falla de hardware, intrusos y virus	Incluir en el plan de respaldo a todos los servicios críticos de la Institución	Control clave	Medida fuerte de control	Alto	Bajo	Costo positivo
R312	Incumplimiento de las políticas y procedimientos de la Institución	Agilizar el proceso de aprobación de la política de acceso lógico a los sistemas	Control no clave	Medida de control adecuada	Alto	Bajo	Costo positivo
R313	Intrusos, virus y accesos no autorizados	Definir y elaborar las políticas y procedimientos para el manejo de incidentes	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		de seguridad de la información					
R314	Intrusos, virus y accesos no autorizados	Establecer mediante el software Aranda que posee la Institución una mesa de servicio para la atención y el manejo de incidentes	Control no clave	Medida de control inexistente	Medio	Bajo	Costo positivo
R315	Incumplimiento de las políticas y procedimientos de la Institución	Establecer mediante el software Aranda que posee la Institución una base de datos del conocimiento para la atención de incidentes	Control no clave	Medida de control inexistente	Medio	Bajo	Costo positivo
R316	Fallo en los enlaces de comunicación	Agilizar la puesta en marcha del contrato firmado en octubre del 2017 con la empresa Racsa para el establecimiento de los enlaces redundantes para todas las oficinas de la DGME	Control clave	Medida de control pobre	Alto	Alto	Costo razonable
R317	Humedad	Instalar sensores de humedad en el archivo central de la DGME	Control no clave	Medida de control inexistente	Medio	Alto	Costo Alto
R318	Peligro de inundación	Establecer un plan de mejoras y reparaciones en los techos sobre el archivo central de la DGME	Control clave	Medida de control adecuada	Medio	Medio	Costo razonable

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
R319	Acceso físico no autorizado	Mantener la puerta al archivo central cerrada en todo momento, e instalar un sistema de apertura de la misma a distancia.	Control clave	Medida de control inexistente	Alto	Bajo	Costo positivo
R322	Incumplimiento de las políticas y procedimientos accesos y permisos	Agilizar el proceso de inclusión de todos los equipos de la DGME al servicio de Microsoft Active Directory	Control no clave	Medida de control pobre	Medio	Bajo	Costo positivo
R323	Incumplimiento de las políticas y procedimientos de la Institución	Establecer planes de capacitación sobre la gestión de riesgos y seguridad de la información que abarque a toda la Institución	Control clave	Medida de control inexistente	Medio	Bajo	Costo positivo
R324	Intrusos y virus	Agilizar el proceso de instalación del software antivirus McAfee ePo Cloud adquirido por la Institución en noviembre de 2017 en los equipos de consulados	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo
R325	Intrusos y virus	Agilizar el proceso de instalación del software antivirus McAfee ePo Cloud adquirido por la Institución en noviembre de 2017 en los equipos	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo

ID Riesgo	Título	Descripción del control	Clasificación del control	Evaluación del control	Beneficio	Costo	Costo del control
		portátiles					
R326	Acceso lógico no autorizado	Modificar las configuraciones de las VPN de los consulados para que cumplan con los requerimientos de seguridad de acceso lógico	Control clave	Medida de control pobre	Alto	Bajo	Costo positivo
R327	Fallo en hardware y software	Establecer un plan para la segmentación de la redes físicas y lógicas	Control clave	Medida de control pobre	Medio	Alto	Costo Alto
R329	Incumplimiento de las políticas y procedimiento	Establecer planes de transferencia del conocimiento del personal clave de las GTI	Control clave	Medida de control inexistente	Medio	Bajo	Costo positivo
R330	Fallo en hardware y software	Modificar la altura del piso falso del centro de datos para que cumpla con las mejores prácticas	Control no clave	Medida de control adecuada	Alto	Alto	Costo razonable
R331	Incumplimiento de las políticas y procedimiento	Establecer el plan de Gestión de Seguridad de la Información (SGSI)	Control clave	Medida de control inexistente	Alto	Alto	Costo razonable
R332	Incumplimiento de las políticas y procedimiento	Establecer e implementar un plan de monitoreo de los servicios críticos que brinda GTI a la DGME	Control clave	Medida de control pobre	Medio	Medio	Costo razonable

Anexo 8. Formulario de entrevistas a funcionarios de la DGME.

Formulario funciones críticas de los sistemas de información DGME

Resumen.

El siguiente formulario tiene como objetivo establecer las funciones críticas de los sistemas de información que posee la DGME, esto, como parte del Plan de Gestión de Riesgos de Seguridad de la Información Física y Lógica.

Indicaciones.

El objetivo es que se tome 30 minutos para responder el siguiente formulario de la manera más detallada posible, ya que de esto dependerán los controles y mecanismos a definir para gestionar los riesgos de la información de la cual usted es responsable.

Nombre completo:
Puesto:
Departamento, gestión o subproceso:
Provincia:
Nombre de la sucursal:
Teléfono para contacto:

1. De cuál de los siguientes sistemas o activos de información es usted dueño o responsable de la información.

☐ Sistema de información.

☐ Sistemas de bases de datos

☐ Sistemas de respaldos

☐ Sistema de información WEB.

☐ Sistema Web Services de Pasaportes

☐ Sistema Web Services Impedimentos de Salida

- ☐ Sistema API
- ☐ Sistema de menores
- ☐ Sistema de movimiento migratorio electrónico (SIMMEL).
- ☐ Sistema de Policía
- ☐ Sistema de gestión de migraciones
- ☐ Sistema de Pasaportes (SISPAS).
- ☐ Sistema de recursos humanos
- ☐ Sistema de refugio
- ☐ Sistema de visas
- ☐ Sistema de información Microsoft SharePoint
- ☐ Sistema Interpol
- ☐ Sistema de extranjería (SINEX)
- ☐ Sistema de correo electrónico institucional (Zimbra)
- ☐ Sistema Cardex
- ☐ Sistema control de accesos
- ☐ Sistema de Bancos
- ☐ Sistema de seguridad
- ☐ Sistema de correspondencia
- ☐ Sistema SISCAP
- ☐ Sistema Almacén
- ☐ Sistema de devolución de depósitos
- ☐ Sistema de transportes
- ☐ Sistema Visor de pasaportes
- ☐ Web Services de SINEX-CARDEX
- ☐ Web Services Sistema de Información Policial
- ☐ Sistema inventario de equipos y licencias de software ARANDA
- ☐ Sistema Felino

SI es usted dueño o responsable de algún sistema de información que no esté en la lista anterior por favor indicarlo:

2. Si es usted dueño o responsable de alguno de los sistemas anteriores por favor indicar la criticidad que posee el sistema o sistemas, con respecto al servicio que presta a la DGME, **desde el supuesto de fallo o caída de este o estos sistemas** y el tiempo que usted considera que se requiere para que estos vuelvan a estar en funcionamiento y la disponibilidad que estos deben tener para las funciones críticas para la DGME, haga referencia a las siguientes tablas para su criterio.

Criticidad

Mayor o igual a 1 hora Mayor a 1 hora y hasta 4 horas
Mayor a 4 horas y hasta 1 día Mayor a 1 día y hasta 2 días
Mayor a 2 días y hasta 4 días
No soporta funciones críticas de la Institución.

Disponibilidad

Alta	Si la información no está disponible esto afecta las actividades administrativas, afecta el servicio de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Minutos a Horas".
Media	Si la información no está disponible esto podría causar pérdida de productividad, pero no interrumpe los servicios de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Horas a Días".
Baja	Si la información no está disponible, esto no impacta severamente las actividades administrativas de la Institución.
	Esta información tiene un Objetivo de Tiempo de Recuperación de "Días a Semanas"

Nombre del sistema	Criticidad	Disponibilidad

3. Posee su departamento, gestión o subproceso, alguna área destinada para almacenar archivos físicos de información, si es así por favor explique

4. Posee su computadora de uso laboral, información sensible o que usted considere, que en caso de que esta se pierda, se dañe o no esté disponible por algún tiempo, afecte las funciones de su departamento y por ende, el servicio que se presta. **Puede hacer referencia a la tabla de criterio de Disponibilidad de la pregunta 2 para definirlo.**

☐ **ALTA**
☐ **MEDIA**
☐ **BAJA**

5. Por último, podría por favor hacer un resumen de las funciones que desempeña el sistema o sistemas del cual usted es dueño o responsable, trate de ser lo más específico posible.

Aplicación o sistema	**Funciones de la aplicación o sistema**

página en blanco