ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

MAESTRIA EN GERENCIA DE SISTEMAS

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: "PROPUESTA DE UN PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL MINISTERIO DEL DEPORTE**"**

AUTOR: URIBE PUPIALES, DANIEL DAVID

DIRECTOR: Mgs. ARROYO CHANGO, RUBÉN DARIO

SANGOLQUI

2018

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, "PROPUESTA DE UN PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL MINISTERIO DEL DEPORTE", fue realizado por el señor Uribe Pupiales Daniel David, el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 22 de mayo del 2018

Nombre del director

C.C.: 1709140907

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***Uribe Pupiales, Daniel David***, con cédula de ciudadanía n° 1716908353, declaro que el contenido, ideas y criterios del trabajo de titulación: ***PROPUESTA DE UN PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL MINISTERIO DEL DEPORTE*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 14 de mayo de 2018

Firma

Daniel Uribe

C.C.:1716908353

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y

TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN

Yo, **Uribe Pupiales, Daniel David,** con cédula de ciudadania n° 1716908353 autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **PROPUESTA DE UN PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL MINISTERIO DEL DEPORTE** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 14 de mayo de 2018

Firma

Daniel Uribe

C.C.:1716908353

DEDICATORIA

Al creador de todas las cosas, el que me ha dado fortaleza para continuar; por ello, con toda la humildad que de mi corazón puede emanar, dedico primeramente mi trabajo a Dios.

De igual forma, dedico el contenido de este trabajo y el esfuerzo realizado para concretar su efectiva culminción tesis a mis padres que ha sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante en los momentos más difíciles.

A mi amada esposa e hijos, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momentos.

Daniel

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.

A mis padres, que con su demostración de padres ejemplares me ha enseñado a no desfallecer ni rendirme ante nada y siempre perseverar a través de sus sabios consejos.

A mi amada esposa, por su apoyo incondicional y por demostrarme la gran fe que tienen en mí.

A la Universidad de las Fuerzas Armadas, por su excelente equipo docente y personal administrativo, gracias por su valiosa guía y asesoramiento a la realización de la misma.

Gracias a todas las personas que ayudaron directa e indirectamente en la realización de este proyecto.

Daniel

INDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo plantea la elaboración de una propuesta del Plan de Continuidad de Negocio de Tecnologías de Información y Comunicación, el mismo que propicie una apropiada gestión de riesgos de la Dirección Tecnológica del edificio matriz del Ministerio del Deporte, el cual busca disminuir la probabilidad de ocurrencia o el impacto que produciría la materialización de fallas en los sistemas y servicios informáticos ante la presencia de ataques o desastres. Se parte de la evaluación previa de cumplimiento a las normas y estándares internacionales, enfatizando la necesidad inmediata de su cumplimiento, tales como, las dispuestas por la Contraloría General del Estado, el Esquema Gubernamental de Seguridad de la Información (EGSI), los estándares internacionales (ISO), etc. La propuesta elabora un prototipo para la administración de equipos, permitiendo así garantizar niveles adecuados disponibilidad de sistemas y servicios tecnológicos, tomando como referencia las normas ISO 22301 e ISO 27001 de Sistemas de Gestión, permitiendo así reducir el impacto, riesgo y tiempo de suspensión de servicios. Finalmente se incluyen las conclusiones y recomendaciones de las lecciones aprendidas, mismas que permite la entrega de lineamientos aplicables a cualquier tipo de organización pública.

Palabras clave:

- **PLAN CONTINUIDAD NEGOCIO**
- **SEGURIDAD INFORMÁTICA**
- **SEGURIDAD DE LA INFORMACIÓN.**

ABSTRACT

The present work defines the elaboration of a proposal for a Business Continuity Plan of Information and Communication Technologies, it conciliates an appropriate management risk of the Technological Direction of the Sport Ministry – Headquarters building, which seeks to reduce the probability of occurrence or the impact that the materialization of failures in computer systems and services in the presence of attacks or disasters would produce. Be part of the prior evaluation of compliance with norms and international standards, emphasizing the immediate need for compliance, such as those provided by the General Comptroller's Office, the Government's Information Security Scheme (EGSI), international standards (ISO), This proposal elaborates a prototype for the equipment administration, thus allowing to guarantee adequate levels of availability of systems and technology services of the Sport Ministry, taking as reference the ISO 22301 and ISO 27001 standards of Information Security Management Systems, which will allow reducing the impact, risk and time of suspension of technological services. Finally, the conclusions and recommendations from the lessons learned during the elaboration of this project are included, which allow the delivery of guidelines applicable to any type of public organization, allowing the safe use of its technological resources.

Keywords:

- **BUSINESS CONTINUITY PLAN**
- **COMPUTER SECURITY**
- **INFORMATION SECURITY**.

CAPÍTULO I: GENERALIDADES

1.1 Antecedentes

El reconocimiento del acceso a la información como un derecho de todo ciudadano y ciudadana, ha llevado a los países de América Latina adoptar progresivamente estándares internacionales sobre temas de Gobierno Electrónico; y en esto Ecuador, ocupa el puesto 74 a nivel mundial y número 10 en América Latina, de acuerdo al ranking emitido por la Organización de Naciones Unidas (ONU). En este sentido las instituciones públicas en su proceso de adaptación al modelo de gobierno electrónico ha sufrido muchos ciberataques; ante esta situación, con el fin de prevenir o disminuir la probabilidad de ocurrencia de este tipo de ataques el estado ecuatoriano a través de la Subsecretaría de Gobierno Electrónico busca controlar que toda institución pública del Estado adopten estándares internacionales de seguridad de la información, obligándoles hacerlo mediante la emisión de Acuerdos ministeriales.

El Ministerio del Deporte, conforme al Art. 13 de la legislación deportiva indica que “El Ministerio Sectorial es el órgano rector y planificador del deporte, educación física y recreación, y le corresponde establecer, ejercer, garantizar y aplicar las políticas, directrices y planes aplicables en las áreas correspondientes para el desarrollo del sector, de conformidad con lo dispuesto en la Constitución, leyes instrumentos internacionales y reglamentos aplicables...” (DEPORTE, LEY DEL DEPORTE, EDUCACION FISICA Y RECREACION, 2015), conforme a lo señalado esta Cartera de

Estado, está enmarcada en dar cumplimiento a lo dispuesto por las normas internacionales en lo referente a garantizar la continuidad del negocio en los sistemas y servicios que ofrece a la ciudadanía.

1.2 Problema

El Ministerio del Deporte es la institución pública encargada de dirigir el deporte ecuatoriano y por lo tanto maneja información legal, financiera, administrativa y de control, de alto grado de sensibilidad, entre la información sensible están los respaldos, acuerdos y resoluciones ministeriales de todas las instituciones deportivas a nivel nacional, así como también sistemas informáticos de gestión de todos los eventos deportivos ejecutados anualmente. Adicionalmente en esta institución se almacenan información sensible sobre subsidios, pensiones, antidopaje y detalles de gastos de los presupuestos asignados anualmente a cada entidad deportiva del Ecuador, todo esto enmarcado en el cumplimiento a los parámetros exigidos en el Marco Regulatorio de Gobierno Electrónico, como el Decreto Ejecutivo 1384 de Interoperabilidad, el Acuerdo 166 del Esquema Gubernamental de Seguridad de la Información (PUBLICA, 2013), Normas 410 de Control Interno de la Contraloría General del Estado, entre otras. Por esta razón, en el caso de existir manipulación o adulteración de ésta información, el impacto o daño al normal desenvolvimiento de ésta Cartera de Estado sería catastrófico y causaría pérdida de imagen y reputación ante la ciudadanía debido a la interrupción en la prestación de sus servicios, con altos niveles de probabilidad de pérdida de información y datos, afectando no solo a esta Cartera de Estado, sino a la

representatividad, credibilidad y reputación de todas las entidades del servicio público en general.

Con este antecedente, se puede decir que el Data Center del Ministerio del Deporte se encuentra expuesto a múltiples riesgos inherentes a su propósito, y a la vez carece de un proceso de administración enfocado en garantizar la continuidad de sus servicios tecnológicos; tampoco se han identificado potenciales amenazas, ni se ha calculado el impacto que tendrían en el normal desenvolvimiento de esta Cartera de Estado en caso de que las amenazas se convirtiesen en realidad, lo cual ha dado lugar a altos niveles de incertidumbre, por lo que no se puede garantizar niveles de servicio ni su continuidad ante desastres de alto impacto, existiendo un alto grado de riesgo de pérdida de información.

Formulación del problema

Ante lo descrito anteriormente, éste trabajo pretende desarrollar el Plan de Continuidad de Negocio busca resolver las siguientes interrogantes:

- ¿Cómo efectuar un Plan de Continuidad del Negocio (BCP), tomando como referencia la norma ISO 22301, enfocada hacia los servicios y sistemas críticos de la Dirección de Tecnologías de Información y Comunicación (DTIC) del Ministerio del Deporte?

- ¿Cómo realizar un análisis de impacto de sistemas y servicios críticos de la DTIC?
- ¿Cómo realizar un análisis de riesgo de sistemas y servicios suministrados por la DTIC?
- ¿Qué estrategias de continuidad de negocio se pueden generar para los sistemas y servicios críticos y los riesgos de alto impacto?
- Cómo tratar los riesgos de impacto alto a través de estrategias?.
- Cuáles son los beneficios de disponer de un BCP[1] en el cumplimiento misional de la DTIC?

1.3 Justificación

La información, procesos y sistemas e infraestructura tecnológica conforman los activos imprescindibles del Ministerio del Deporte; por ende garantizar una correcta planeación, ejecución y evaluación de la seguridad de la información es de esencial importancia. Por este motivo es necesario asegurar la confidencialidad, integridad y disponibilidad de los procesos principales activos informáticos de esta Cartera de Estado, para lo cual es necesario realizar un análisis de amenazas, vulnerabilidades e impacto que permitan identificar los riesgos y su posterior tratamiento que permitan garantizar niveles adecuados de calidad en sus sistemas y servicios que presta a la ciudadanía. El proceso mencionado permitirá:

- Garantizar la continuidad y disponibilidad de sus servicios.

[1] BCP Business Continuity Planning

- Incrementar los niveles de confianza de la ciudadanía.
- Reducción de costos vinculados a incidentes.
- Cumplir con lo dispuesto por los organismos de control tales como la Subsecretaría de Gobierno Electrónico, Normas de control interno de la Contraloría General del Estado, entre otros

Además, la elaboración de la presente propuesta, permitirá al Ministerio del Deporte cumplir con lo dispuesto en:

- El Acuerdo Ministerial No. 166, el cual dispone la implementación del "Esquema Gubernamental de Seguridad de la Información (EGSI)" (PUBLICA, 2013), adaptado de la norma creada por la Organización Internacional para Estandarización (ISO) y publicado por el Servicio Ecuatoriano de Normalización. (SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA SNAP, 2013)
- Lo dispuesto en el Estatuto Orgánico de Gestión Organizacional por Procesos, Resolución Nro. 0034 del Ministerio del Deporte, el mismo que dispone gestionar el plan de contingencia que permita garantizar la continuidad del servicio tecnológico en la institución. (DEPORTE, ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS, 2016)
- Lo manifestado por las Normas Nro. 410 de Control Interno de la Contraloría General del Estado, correspondiendo a la Dirección de Tecnologías de Información y Comunicación "la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una

emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado". (ESTADO, 2010)

- Los lineamientos definidos en el Plan Estratégico de Tecnologías de la Información (PETI) 2015-2016, del Ministerio del Deporte, en el que se menciona la necesidad urgente de diseñar un Plan de Continuidad de Negocio. (ORTEGA, 2015)
- Ley Orgánica de Transparencia y Acceso a la Información Pública. (NACIONAL C. , LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN, 2004)
- Decreto Ejecutivo 1384 de Interoperabilidad. (DELGADO, 2012)
- Decreto Ejecutivo 149 Gobierno Electrónico y Simplificación de Trámites. (SECRETARIA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA, 2013)

En resumen, es prioritario y urgente definir un Plan de Continuidad de Negocio para la Dirección Tecnológica, con el propósito de identificar riesgos a los cuales está expuesto y determinar estrategias o directrices para que se puedan implementar mejores prácticas que coadyuven a la disminución, transferencia y aceptación de riesgos e incrementar la productividad y efectividad del Centro de Datos.

1.4 Objetivos

General:

Elaborar una propuesta de Plan de Continuidad de Negocio (Business Continuity Planning) para contrarrestar las interrupciones de los sistemas y servicios críticos de la Dirección de Tecnologías de la Información y Comunicación, que propicie una correcta gestión de riesgos, tomando como referencia las recomendaciones de la norma ISO 22301, el cual permita garantizar la integridad, confidencialidad y disponibilidad de los sistemas y servicios ofrecidos en el Ministerio del Deporte.

Específicos:

- Evaluar la situación actual del Centro de Datos del Ministerio del Deporte con el fin de identificar sus sistemas y servicios, así como su grado de vulnerabilidad.
- Identificar los sistemas y servicios informáticos críticos de la DTIC.
- Evaluar el impacto operativo que provoca la falta de disponibilidad de los sistemas y servicios informáticos críticos, en la prestación de servicios del Ministerio del Deporte a la ciudadanía.
- Formular una propuesta de administración de riesgos que permita asegurar la conservación de sistemas y servicios críticos de la Dirección de Tecnologías de Información (DTIC).

1.5 Alcance

La presente propuesta de titulación, elabora un modelo de plan de continuidad del negocio para la Dirección Tecnológica de planta central del Ministerio del Deporte de la ciudad de Quito, el entregable será un documento físico el mismo que detallará el Plan de Continuidad de Negocio.

La propuesta contempla los siguientes aspectos:

- Identificación de activos de información
- Tipificación de amenazas potenciales a los servicios críticos
- Tipificación y análisis de riesgos de los servicios críticos de la institución
- Estimación de riesgos
- Tratamiento de riesgos
- Prioridad de recuperación de servicios
- Roles y responsabilidades del equipo de recuperación

La propuesta no contempla los siguientes aspectos:

- Implementación de la propuesta, ya que los recursos económicos que involucre la implementación del mismo deberán ser detallados y solicitados en el Plan Operativo Anual de Tecnologías de Información (POATIC), como parte del proyecto Estratégico (PETI) del siguiente año fiscal, los mismos que pueden ser

aprobados en su totalidad o parcialmente, conforme lo disponga la máxima autoridad (Ministro/a).

- Plan de emergencia para evacuación de edificios.
- Plan de reanudación de infraestructura tecnológica que no forme parte de los servicios críticos.
- Plan de recuperación de Coordinaciones Zonales del Ministerio del Deporte.

1.6 Metodología

El Plan de Continuidad del Negocio certifica que los riesgos y amenazas sean conocidos, aceptados, gestionados y minimizados de forma eficaz, ordenada, metódica cíclica y maleable a cambios.

El análisis de riesgos es un procedimiento de ayuda en la decisión sobre nuevos mecanismos de seguridad, sus resultados constituyen una guía para la organización para la definición de controles y procesos de seguridad más adecuados.

Para el análisis de Impacto de Negocio, se utilizará la herramienta Bussiness Impact Analysis (BIA), utilizada para la identificación de activos, su impacto operacional y tiempos de recuperación. Para el análisis de riesgo, se tomará como referencia las fases proporcionadas por la Metodología de Análisis y Gestión de Riesgos (MAGERIT). (PÚBLICAS M. D., 2014)

El propósito del Plan de Continuidad de Negocio es minimizar el impacto que afecte el normal desenvolvimiento en la prestación de sistemas y servicios proporcionados por la Dirección de Tecnológica. Para la elaboración del presente proyecto, se tomará como referencia la Norma ISO 22301: 2012, la misma que provee una guía completa para el desarrollo del Plan de Continuidad.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

El presente capítulo detalla conceptos y fundamentos teóricos necesarios para la realización de este proyecto. El alcance del estudio permitirá proponer controles y políticas basados en el análisis de servicios y sistemas de información.

2.1 Conceptos Relacionados

A continuación se detallan los conceptos relacionados al desarrollo de la propuesta de trabajo.

Activo: cualquier información proveniente de sistemas, servicios, etc que posee valor para la institución. (INEN, NTE INEN-ISO/IEC 27001, 2011)

Disponibilidad: Propiedad de accesibilidad e cualquier momento para su uso por personas autorizadas. (INEN, NTE INEN-ISO/IEC 27001, 2011)

Confidencialidad: Característica de reserva de acceso a la información. (INEN, NTE INEN-ISO/IEC 27001, 2011)

Integridad: Característica de conservación de exactitud y completitud. (Standardization, Management of information and communications technology security, 2004)

Incidente de seguridad de la información: Suceso imprescindible que puede afectar negativamente el normal desenvolvimiento de los procesos empresariales o institucionales. (Standardization, Information security incident management , 2004)

Riesgo: “efecto de la incertidumbre en la consecución de los objetivos” (ISO_31000, 2009)

Evaluación de riesgos: Procedimiento de estudio de riesgos. (INEN, NTE INEN-ISO/IEC 27001, 2011)

Amenaza: Fuente de incidentes con capacidad de producir daño a sistemas o servicios. (INEN, NTE INEN ISO/IEC 27005, 2012).

2.2 Leyes y documentos de importancia

Ecuador se encuentra enmarcado en un proceso de E-Goberment, para lo cual dispone de una base legal suficiente, con lo que busca que todas las instituciones públicas estén cada vez más cerca y al alcance de sus ciudadanos y ciudadanas, así tenemos:

- **Ley del Sistema Nacional de Registro de Datos Públicos:** Reglamenta la administración de datos públicos y sus formas de acceso. (NACIONAL A. , LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS, 2010)
- **Ley de Comercio Electrónico, Firmas Electrónica y Mensaje de Datos:** Reglamenta el uso de servicios electrónicos y busca brindar protección a usuarios que hacen uso de estos medios digitales. (NACIONAL C. , LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, 2002)
- **Plan Nacional de Desarrollo:** Como parte de su planificación estratégica, provee una estructura al estado con una visión hacia la DESCONCENTRACIÓN, la misma que traslada los servicios ofertados por una institución pública mediante la web, llegando más cerca de la ciudadanía, a la vez que expone a la institución a peligros universales. (DESARROLLO, 2014)

Continuidad del Negocio en el Ministerio del Deporte.

Conforme a lo dispuesto por la SNAP[2] a través del Acuerdo Nro. 166 EGSI[3], toda institución pública debe elaborar un Plan de Continuidad, la responsabilidad es del oficial de seguridad de la información, documento que es de carácter reservado, este documento debe contener las medidas de seguridad, procedimientos, normas, políticas implementadas que buscan garantizar niveles adecuados de integridad, confidencialidad y disponibilidad de los servicios y sistemas informáticos.

2.3 ISO/IEC 22301 / 27001

Estas dos normas internacionales tratan la administración de continuidad de negocio, como un componente esencial en la seguridad de la información, define medidas y procedimientos que permiten contrarrestar interrupciones en procesos críticos para la institución, garantizando su reanudación.

La relación existente entre las normas ISO 22301 e ISO 27001 se detalla en la siguiente tabla.

[2] SNAP “Secretaría Nacional de la Administración Pública”
[3] EGSI “Esquema Gubernamental de Seguridad de la Información”

Tabla 1

Correlación entre ISO 27001 e ISO 22301

ELEMENTO	ISO 27001: Gestión de Riesgos	ISO 22301: Gestión de Continuidad de Negocio
Herramienta o Método	Análisis de Riesgos (AR)	Análisis de Impacto del Negocio (BIA)
Claves	Impacto y Probabilidad	Impacto de Tiempo
Tipos de Incidente	Todo tipo de eventualidades (segmentadas)	Fallos críticos para el negocio (no segmentadas)
Magnitud	Toda, generalmente segmentada	Incidentes estratégico críticos para el negocio.
Enfoque	PREVENTIVO: Gestión de Riesgos para los objetivos del negocio.	CORRECTIVO: Gestión de Incidentes.
Escenarios e Intensidad	Todos (segmentados)/ Toda	El peor escenario(s) / Incidentes súbitos

Fuente: (22301, 2011)

2.4 Metodología del Plan de Continuidad de Negocio (ISO 22301).

Para el diseño de la propuesta del plan de continuidad de TI del Ministerio del Deporte se tomará como referencia la metodología propuesta por la norma ISO 22301, la misma que identifica los niveles de riesgo a los que una organización se encuentra expuesta, define prioridades de recuperación de acuerdo al análisis de tiempos máximo de tolerancia para su restauración.

La norma ISO/IEC 22301 conceptualiza a la continuidad del negocio como la "capacidad estratégica de la organización para permitir la continuidad de la entrega de productos o servicios a niveles aceptables, previamente definidos" (INEN, ISO 22301, 2012).

Según John Sharp [2012, pg. 14] "*Las adiciones en la ISO/IEC 22301 han añadido más profundidad y claridad, mientras que las omisiones no son detrimento de las prácticas de BCM, en general son buenos principios*". (JOHN, 2012)

La siguiente figura muestra el plan logístico propuesto en la norma, que considera los siguientes pasos:

- **Etapa 1** Identificación (Análisis de impacto en el negocio)
- **Etapa 2** Análisis (Evaluación o análisis de riesgos)
- **Etapa 3** Diseño (Selección de estrategias)
- **Etapa 4**: Ejecución (Desarrollo ejecución del Plan)
- **Etapa 5**: Medición (Prueba y Mantenimiento del Plan)

Figura 1 Representación gráfica de la Metodología de continuidad del negocio
Fuente: (ISO 22301), Tomado de la NTC-ISO/IEC 22301

Para el desarrollo de la presente propuesta se desplegarán tres etapas de la metodología que proporciona la ISO 22301, siendo estas; la Identificación, Análisis y Diseño. No se cubrirá las fases de ejecución y medición del Plan de Continuidad de la Dirección Tecnológica, ya que los recursos económicos que involucre su implementación deben ser detallados y solicitados en el Plan Operativo Anual de Tecnologías de Información (POATIC), como parte del proyecto estratégico (PETI) del siguiente año fiscal, los mismos que pueden ser aprobados en su totalidad o parcialmente, conforme lo disponga la máxima autoridad, es decir, el Ministro/a de esta Cartera de Estado.

2.4.1 ETAPA I: IDENTIFICACIÓN

Análisis de Impacto del Negocio.

Para el desarrollo de esta etapa se tomará como referencia la herramienta de Análisis de Impacto de Negocio (conocido como BIA por sus siglas en ingles), la misma que proporciona un marco de criterios, recomendaciones y buenas prácticas en el análisis de riesgos, esta herramienta gestiona los riesgos de una manera documentada, sistemática, estructurada, continua y eficiente.

El BIA permite valorar el impacto operacional que provocaría la interrupción de un proceso o servicio tecnológico, en el cumplimiento o entrega de servicios.

Los pasos o fases que se deben seguir para la aplicación del BIA son los que se describen a continuación.

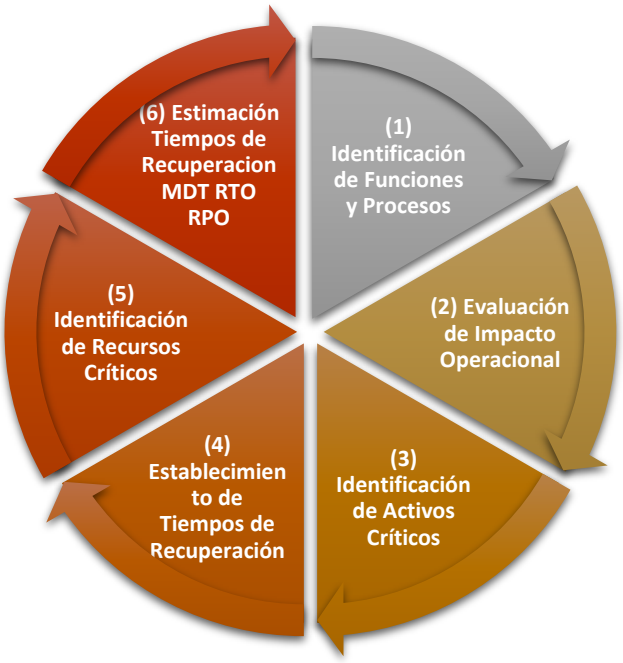


Figura 2 Fases de aplicación BIA
Fuente: (MINTIC,2013)

2.4.1.1 Fase 1: Identificación de Funciones y Procesos

Esta etapa da como resultado un listado de activos de información (sistemas, servicios, roles, procesos) los mismos que serán analizados a profundidad en cada una de las fases siguientes. (BCI, 2013)

2.4.1.2 Fase 2: Evaluación de Impactos Operacionales

En base a los activos de información previamente identificados es necesario valorar el grado de impacto que tendría una paralización al normal desenvolvimiento de los mismos, para la valoración del impacto, se utilizó el siguiente esquema de valoración por niveles:

Tabla 2
Valoración Impacto

NIVEL	DETALLE
A	La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.
B	La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.
C	La operación no es una parte integral del negocio.

Fuente: (Metodología BIA MINTIC)

2.4.1.3 Fase 3: Identificación de Activos críticos

La identificación de activos críticos del Ministerio del Deporte debe basarse en la clasificación de impactos operacionales de la organización, así tenemos:

Tabla 3
Identificación de Procesos Críticos

VALOR	INTERPRETACIÓN DEL PROCESO CRÍTICO
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Fuente: (Metodología BIA MINTIC)

2.4.1.4 Fase 4:
Establecimiento de Tiempos de Recuperación.

Es importante determinar tiempos de recuperación para cada proceso crítico identificado, esto permitirá definir un procedimiento ordenado y oportuno de sistemas y servicios tecnológicos.

Tabla 4

Descripción de tiempos de recuperación

TIEMPO DE RECUPERACIÓN	DESCRIPCIÓN
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio.
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Fuente: (COLOMBIA, 2015)

2.4.1.5 Fase 5: Identificación de Recursos Críticos

La DTIC considera como recursos críticos a todos aquellos sistemas, servicios, infraestructura tecnológica, involucrada en la prestación de servicios a la ciudadanía o en su defecto que permite o facilita la gestión interna de las distintas direcciones del Ministerio del Deporte que coadyuvan al cumplimiento de objetivos misionales de esta Cartera de Estado.

2.4.2 ETAPA II: ANÁLISIS DEL RIESGO

“El análisis del riesgo es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado” (Comercio, 2013).

El análisis de riesgos de la DTIC, se lo realizara tomando como referencia la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (MAGERIT), la misma que es de uso público, no requiere autorización previa para su uso e implementación, ya que el Ministerio de Administración Pública española MAP, lo ha publicado en su portal web, sin restricciones de licenciamiento. (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

MAGERIT, contempla cuatro fases para el análisis de riesgos, la siguiente figura muestra estas cuatro fases:

Figura 3 Fases metodología MAGERIT
Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

2.4.2.1 Fase :1 Identificacion y selección de amenazas

En base al catálogo de activos se debe determinar las amenazas a las que estos se encuentran expuestos, es necesario mantener un enfoque práctico ya que la clasificación de amenazas posee un amplio abanico de clasificación pudiendo ser estos accidentales o deliberados, humanos, técnicos, naturales, etc., existen casos en los que una amenaza afecta más de un activo, por tal razón es importante tomar el tiempo necesario para realizar jun correcto análisis de identificación de amenazas. (PÚBLICAS M. D., 2006)

La siguiente tabla lista un grupo de amenazas comunes que se encuentran presentes en la mayoría de instituciones.

Tabla 5

Identificación amenazas comunes

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	

D=Deliberadas, A=Accidentales

Fuente: (MINTIC, 2013)

Otro grupo de amenazas o los que es necesario brindar un cuidado especial son las amenazas humanas ya que en su gran mayoría son los que poseen mayor probabilidad de ocurrencia o materialización, así la siguiente tabla describe la mayor cantidad de amenazas detectadas:

Tabla 6

Fuentes de amenazas humanas

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema

Fuente: (MINTIC 2013)

2.4.2.2 Fase 2: Identificar vulnerabilidades y salvaguardas

Esta fase analiza el catálogo de activos en busca de sectores o áreas débiles o vulnerables pudiendo ser esta por ejemplo el suministro de energía eléctrica al Data Center, el mismo que debe ser redundante y adicional contar con un sistema de energía ininterrumpido (SAI), para la valoración de la vulnerabilidad es necesario contar con un sistema de valoración cuantitativa o cualitativa.

Tabla 7
Valoración de Vulnerabilidades

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.

Fuente: (MINTIC 2013)

Identificación de controles existentes

Con el fin de evitar duplicidad de controles y por consiguiente gastos innecesarios se debe realizar un correcta determinación de controles y su nivel de eficiencia contemplando su documentación, funcionario responsable de ejecución, periodicidad, aquellas vulnerabilidades que no cuentan con un control eficiente y efectivo serán contemplados como parte del Plan de Tratamiento de Riesgos, para ser reemplazados o repotenciados.

La siguiente tabla proporciona parámetros para la evaluación de controles.

Tabla 8
Valoración de Controles

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer control.			15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta.			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva			30
Seguimiento al control	Están definidos los responsables de la ejecución de control y del seguimiento.			15
	La frecuencia de ejecución del control y seguimiento es adecuada.			25
			TOTAL	**100**

Fuente: (Guía de Riesgos DAFP)

2.4.2.3 Fase 3: Evaluar el riesgo

Para la evaluación de riesgos es indispensable contar con los siguientes insumos:

- Catálogo de activos
- Registro de amenazas
- Catálogo de vulnerabilidades.
- Evaluación de controles

Con estos insumos es posible realizar una valoración de riesgos estimando su probabilidad de ocurrencia así como su grado de impacto en los activos y por consiguiente el grado de afectación negativa en el cumplimiento de objetivos misionales de la institución.

Tabla 9
Cálculo de Probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Fuente: (INCIBE Instituto Nacional de Cibersegurdad)

Tabla 10
Cálculo de impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: (INCIBE Instituto de Cibersegurdad)

Tabla 11
Criterios de aceptación del riesgo

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	DESCRIPCIÓN
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Fuente: (INCIBE Instituto de Cibersegurdad)

Cálculo del riesgo.

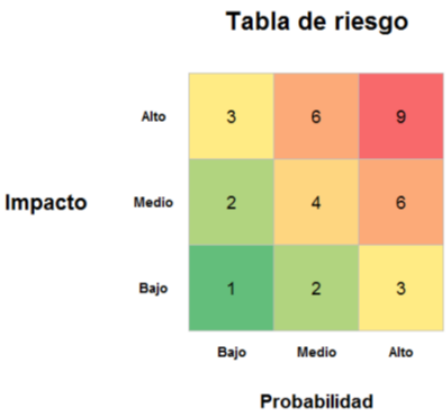
Si se elige el análisis cuantitativo para el cálculo de riesgo, se utilizará la siguiente fórmula:

RIESGO = PROBABILIDAD x IMPACTO.

La siguiente tabla muestra los distintos niveles de riesgo que pueden ser identificadas en función de su impacto y probabilidad de ocurrencia.

Tabla 12
Cálculo de Riesgo

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto



Fuente: (INCIBE Instituto de Cibersegurdad)

2.4.2.4 Fase 4: Tratar el riesgo

Una vez valorado los riesgos en función de las amenazas y vulnerabilidades es posible elaborar o diseñar un plan de tratamiento de riesgos tomando en consideración cuatro tácticas fundamentales:

- **Trasladar el riesgo a un tercero**. Esto se lo realiza mediante la contratación de un servicio ofrecido por un tercero.
- **Eliminar el riesgo**. Esto se logra suprimiendo la fuente de donde se origina o produce el riesgo por ejemplo un equipo de red de terceros.
- **Asumir el riesgo**: Esto se presenta generalmente cuando el costo de mitigar el riesgo es más alto que el coste del activo.
- **Implantar medidas para mitigarlo.**

2.4.3 ETAPA III: DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Gestión de Riesgos ISO 22301

La gestión de riesgos identificados de alto impacto de la DTIC se realizará tomando como referencia la Norma ISO/IEC 22301:2012, la misma que está conformada por 7 Fases con las que permite gestionar la Continuidad del Negocio, siendo éstas las siguientes:

- **Fase 1:** Contexto de la Organización
- **Fase 2:** Liderazgo
- **Fase 3:** Planeación.
- **Fase 4:** Soporte.
- **Fase 5:** Operación
- **Fase 6:** Evaluación del Desempeño
- **Fase 7:** Mejoramiento

Se eligió como referencia la Norma Internacional ISO/IEC 22301:2012 debido a que toma en consideración los aspectos de gestión como un sistema, permitiendo la identificación de entradas, actividades y salidas de cada Fase, la siguiente figura describe de manera gráfica cada una de las entradas, actividades y salidas de cada Fase.

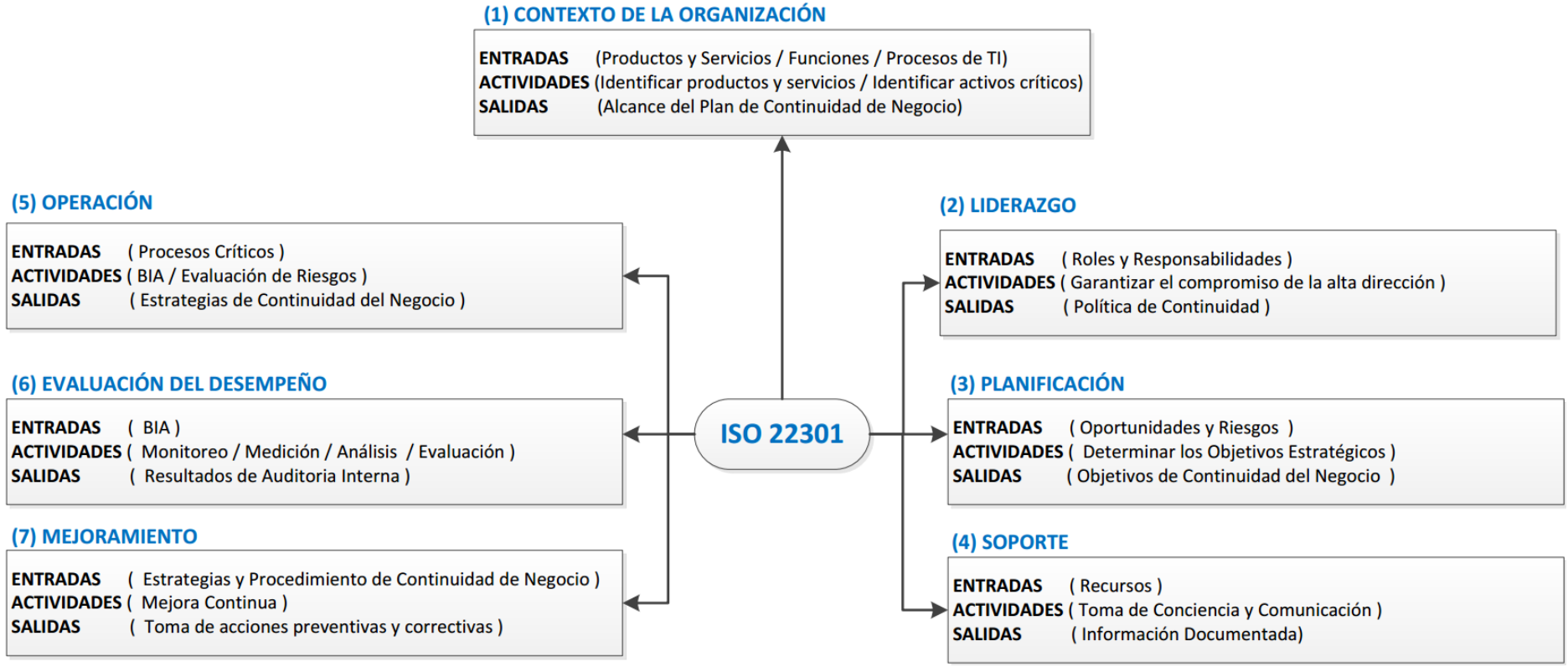


Figura 4 Procesos ISO/IEC 22301:2012
Fuente: (ISO /IEC 22301:2012)

A continuación se describe cada una de la Fases de la Norma ISO 22301:2012

2.4.3.1 Fase 1: Contexto de la Organización

La aplicación de esta norma será en la Dirección Tecnológica por lo tanto la información detallada ara referencia a los sistemas y servicios proporcionados por la misma.

Entendimiento a la Organización y su Contexto

El Ministerio del Deporte conforme a lo dispuesto a la ley del deporte posee lineamientos claros de su razón de ser y sus objetivos misionales, para cumplir con los objetivos inherentes a su propósito hace uso de una estructura organizacional que le permita establecer un modelo de gestión. (NORMALIZACIÓN, 2012)

Entendimiento de las Necesidades y Expectativas

La identificación de necesidades y expectativas permite tomar en consideración todos los escenarios involucrados que deben formar parte en el documento entregable del plan de continuidad tecnológico, las partes interesadas serán parte importante en el desarrollo del proyecto ya que su compromiso facilita la obtención de información necesaria para las distintas etapas del mismo.

2.4.3.2 Fase 2: Liderazgo

ISO 22301 enfatiza la necesidad de un liderazgo por parte de la alta dirección comprometida en proporcionar los recursos necesarios, nombrar a los responsables de la Gestión de Continuidad de Negocio y el establecimiento de políticas. (INEN, ISO 22301, 2012)

Existe un compromiso de la alta dirección para garantizar:

- Que los objetivos y políticas de la Continuidad del Negocio son compatibles con la estrategia de la organización y se integran a sus procesos de negocio.
- La provisión de recursos necesarios, orientando y apoyando a las personas en la comunicación de la importancia del sistema.
- Que el sistema obtiene los resultados esperados y fomente el mejoramiento continuo.
- La política de continuidad de negocio, debe estar disponible, ser comunicada y revisada a intervalos definidos ante cambios significativos. Así mismo, los roles, responsabilidades y autoridad en la organización, deben asegurar que el plan satisfaga todos los requerimientos legales e informar el desempeño del plan sistema a la Alta Dirección.

2.4.3.3 Fase 3: Planificación

El desarrollo de esta Fase es crucial y determinante en la implementación del Plan de Continuidad, las acciones para cubrir riesgos y oportunidades deben ser:

- Determinar los riesgos y oportunidades que deben ser tratados con el fin de alcanzar el logro planteado.
- Disminuir los riesgos
- Los objetivos de la continuidad de negocio se pueden alcanzar:
    - Asegurando que se establecen y se comunican las funciones y los niveles pertinentes.
    - Siendo consistente con la política definida.
    - Considerando el nivel mínimo aceptable por la organización.
    - Monitoreando y actualizando, según sea apropiado.
    - Determinado responsabilidades, actividades a realizar, recursos necesarios y evaluación de resultados.

2.4.3.4 Fase 4: Soporte

El Plan de Continuidad se fundamenta en el uso eficiente de los recursos para ello es necesario:

- Determinar y proporcionar los recursos necesarios.
- Asegurar que las personas sean competentes, considerando la educación, formación y experiencia, tomando acciones para que ellas adquieran dicha competencia.
- Toma de conciencia, conocer su rol durante los incidentes de interrupción y las consecuencias de su incumplimiento.
- Determinar las comunicaciones internas y externas necesarias (qué, cuándo, a quién) garantizando la disponibilidad de los medios de comunicación.
- Información documentada, respecto al desarrollo, actualización, control (distribución, almacenamiento, versiones), disponibilidad y protección (acceso y modificación).

2.4.3.5 Fase 5: Operación

Debe existir una planificación, ejecución y control de los procesos necesarios para implementar las acciones definidas, cambios planificados e imprevistos.

Respecto al análisis de impacto en el negocio y apreciación del riesgo debemos establecer, implementar y mantener un proceso formal y documentado realizando una evaluación de riesgo. (INSTITUTE, 2010)

Análisis de impacto:

- Identificación de actividades que apoyan la prestación de productos y servicios.
- Evaluación de los impactos del tiempo de interrupción.
- Identificación de las dependencias y recursos.

Evaluación de riesgo:

- Identificar los riesgos de interrupción de activos, sistemas, información, personas y proveedores.
- Analizar y evaluar los riesgos relacionados con la interrupción que requieran el tratamiento.
- La estrategia de continuidad de negocio, debe estar basada en el resultado del análisis de impacto y la evaluación del riesgo, cumplir con los tiempos definidos, así como mitigar, responder y gestionar los impactos.

- Se debe estabilizar, continuar, reanudar y recuperar las actividades, determinando los recursos necesarios para su implementación, y establecer medidas proactivas para reducir la probabilidad de interrupción.

El desarrollo e implementación de procedimientos de continuidad debe:

- Establecer, implementar y mantener procedimientos documentados para responder una interrupción, determinando la forma de continuar o recuperar las actividades dentro de un plazo predeterminado. Estos procedimientos abarcan la estructura organizacional de respuesta a incidente y los protocolos de comunicación.
- Realizar una revisión y ejercicios de informes formales de evaluación del ejercicio (mejoramiento continuo) e intervalos planificados, o ante cambios significativos (organización o entorno).

2.4.3.6 Fase 6: Evaluación del Desempeño

Realizar una evaluación de procedimientos de continuidad:

- En forma periódica mediante revisiones, ejercicios, informes post-incidentes y evaluaciones de desempeño, reflejando los cambios significativos en los procedimientos en forma oportuna.
- Cumplimiento de requisitos legales y reglamentarios.
- Permite tomar medidas proactivas, antes de que se produzca una no conformidad.

La auditoría interna permite:

- La objetividad, imparcialidad y competencia para el proceso.
- Definir los criterios y alcance de cada auditoría, conservando evidencias.
- Intervalos planificados para informar si el SGCN está en conformidad con los requisitos propios establecidos por la organización y por esta norma.

2.4.3.7 Fase 7: Mejoramiento

- Identificar las no conformidades para controlarlas y corregirlas.
- Revisar la eficacia de las acciones correctivas establecidas.
- Mantener evidencias.
- Mejorar continuamente la idoneidad, adecuación y eficacia del SGCN.

2.4.4 ETAPA IV: EJECUCIÓN

La puesta en marcha del Plan de Continuidad de Negocio, de sus siglas en inglés (BSP), contempla los siguientes aspectos:

- Puesta en marcha del plan de continuidad del negocio
- Conformación de equipos
- Fases de alerta del plan
- Fase de Alerta
- Táctica de aviso del desastre
- Procedimiento de ejecución del plan.
- Modo de comunicación de ejecución del plan.
- Fase de Transición.
- Especificaciones para la puesta en marcha del centro de datos de recuperación.
- Fase de Recuperación.
- Fase de vuelta a la normalidad.

2.4.5 ETAPA V: MEDICIÓN

El Plan de continuidad de negocio es la respuesta de la Dirección tecnológica ante escenarios de riesgo con afectación crítica, conforme existan cambios o incremento de servicios o sistemas tecnológicos, será necesario actualizar la información del Plan de continuidad, el mismo que deberá ser probado y medido con el fin de garantizar su eficiencia y versatilidad en el tratamiento de riesgos.

CAPÍTULO III: DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

El plan de continuidad será desarrollado conforme lo descrito en cada una de las etapas proporcionadas por el estándar internacional ISO 22301, permitiendo identificar información relevante del Ministerio del Deporte tales como sus sistemas y servicios tecnológicos críticos, identificación de amenazas, vulnerabilidad y riesgos, para terminar con el diseño de estrategias que permitan disminuir los riesgos a un nivel aceptable para la organización.

3.1 ETAPA I: IDENTIFICACION

3.1.1 Estudio de la Organización

El Presidente de la República en el año 2007 mediante Decreto Ejecutivo No. 6 creó el Ministerio del Deporte, el mismo que asumió las competencias de la Secretaria Nacional del Deporte, obteniendo así su constitución jurídica, fundamentando su accionar en la siguiente base jurídica:

Constitución de la República del Ecuador: el Art. 24 menciona que todo ciudadano/a tiene derecho a distraerse y ejercitarse en sus momentos de óseo. El Art. 381 indica que el Estado impulsará la actividad deportiva de tipo formativo, barrial y parroquial; promoviendo la práctica del ejercicio.

Ley del deporte, educación física y recreación: La ley del deporte en su Art. 13 indica que el Ministerio del Deporte es el órgano rector del deporte, y sus competencias deben estar enfocadas en garantizar y aplicar políticas y lineamientos que promuevan la activación deportiva de ciudadanos/as en la obtención de logros deportivos tanto nacionales como internacionales.

Art. 14.- Funciones y atribuciones. - Las competencias del Ministerio del Deporte entre otros están:

- Proporcionar un Sistema Nacional de información Deportiva que permita gestionar eventos de las distintas disciplinas deportivas, en todas sus categorías, organizadas tanto a nivel nacional como internacional; así como también información de deportistas, entrenadores, jueces.
- Garantizar el mantenimiento y buen funcionamiento de la infraestructura pública deportiva.
- Aprobación y regularización de organizaciones deportivas, aprobación de sus Estatutos y directorios conforme a la naturaleza de cada organización.
- Intervención transitoria en organizaciones que reciban recursos públicos.

Plan Nacional de Desarrollo: el Plan Nacional del Buen Vivir es el marco de lineamiento al cual todos los procesos se alinean buscando dar cumplimiento a los objetivos misionales de esta Cartera de Estado.

Tabla 13

Alineación al Objetivo 3 del Plan Nacional del Buen Vivir

Objetivo 3	**Mejorar la Calidad de Vida de la Población**
Política 3.7	Impulsar el uso del tiempo libre en acciones físicas, deportivas y que ayudan a mejorar el estado físico y social de los/las ciudadanos/as.
Estrategia	a) Promover la actividad física de los ciudadanos/as teniendo en cuenta sus condiciones físicas, cultural, étnico, y de género, así como también sus necesidades y habilidades.
	b) Promover la inclusión en la práctica deportiva y actividad física.
	c) Incentivar la práctica de activación física y gimnasia laboral en los sitios de trabajo, que ayuden al mejoramiento de las condiciones físicas, intelectuales y sociales de las y los trabajadores.
	d) Propiciar la formación de ciudadanos/as activos/as mediante actividades recreativas, lúdicas, de liderazgo, deportivas y asociativas niños y niñas, adolescentes y jóvenes.
	e) Promover la práctica de actividades curriculares y extracurriculares de acuerdo a la condición etaria, física, de género y características culturales y étnicas.
	f) Motivar la práctica del deporte en los ciudadanos/as tomando en consideración su condición física, etnia, género en instituciones educativas, instituciones públicas y privadas, y organizaciones de la sociedad civil.

Fuente: (Plan Nacional del Buen Vivir 2013 - 2017; Programación Anual de la Política Pública - SIPeIP 2015. MINDE, 2016)

Tabla 14
Alineación al Objetivo 4 del Plan Nacional del Buen Vivir

Objetivo 4	**Fortalecer las capacidades y potencialidades de la ciudadanía**
Política 4.10	Fortalecer la formación profesional de artistas y deportistas de alto nivel competitivo
Estrategia	a) Promover la participación de deportistas de alto nivel en competencias nacionales, internacionales, olimpiadas y para olimpiadas
	b) Fortalecer la capacitación docente en las distintas disciplinas deportivas y en áreas de gerencia, docencia y
	c) Fortalecer la formación física y psicológica de deportistas especial izados de alto rendimiento.

Fuente: (Plan Nacional del Buen Vivir 2013 - 2017; Programación Anual de la Política Pública - SIPeIP 2015. MINDE, 2016)

Tabla 15
Alineación al Objetivo 5 del Plan Nacional del Buen Vivir

Objetivo 5	**Construir espacios de encuentro común y fortalecer la identidad nacional, las identidades diversas, la plurinacionalidad y la interculturalidad**
Política 5.1|	Promover la democratización del disfrute del tiempo y del espacio público para la construcción de relaciones sociales solidarias entre diversos.
Estrategia	Fortalecer y democratizar los espacios y programas públicos de actividad física, expresión corporal, recreación y mejoramiento de la salud.

Fuente: (Plan Nacional del Buen Vivir 2013 - 2017; Programación Anual de la Política Pública - SIPeIP 2015. MINDE, 2016)

En base a lo anteriormente expuesto se puede indicar que el Ministerio del Deporte fue creado con la misión de promover en la ciudadanía el uso del tiempo libre de una manera saludable mediante la práctica del deporte y la recreación, además promueve la práctica del deporte formativo y profesional para lo cual norma, regula y legaliza a toda organización deportiva como federaciones, clubes, ligas, etc, designando fondos económicos a los distintos organismos deportivos en base a una planificación anual, por lo tanto genera, administra información sensible como Acuerdos Ministeriales, pensiones para deportivas, registros médicos de deportistas, informes de análisis anti dopaje, entre otros.

3.1.2 Estructura organizacional del Ministerio del Deporte

Con el propósito de ejecutar lo dispuesto en las políticas mencionadas, el Ministerio del Deporte conforme a su Estatuto Orgánico, integra a la Dirección Tecnológica dentro de la Coordinación de Planificación y Gestión Estratégica, con la misión de proporcionar servicios tecnológicos institucionales a usuarios internos y externos.

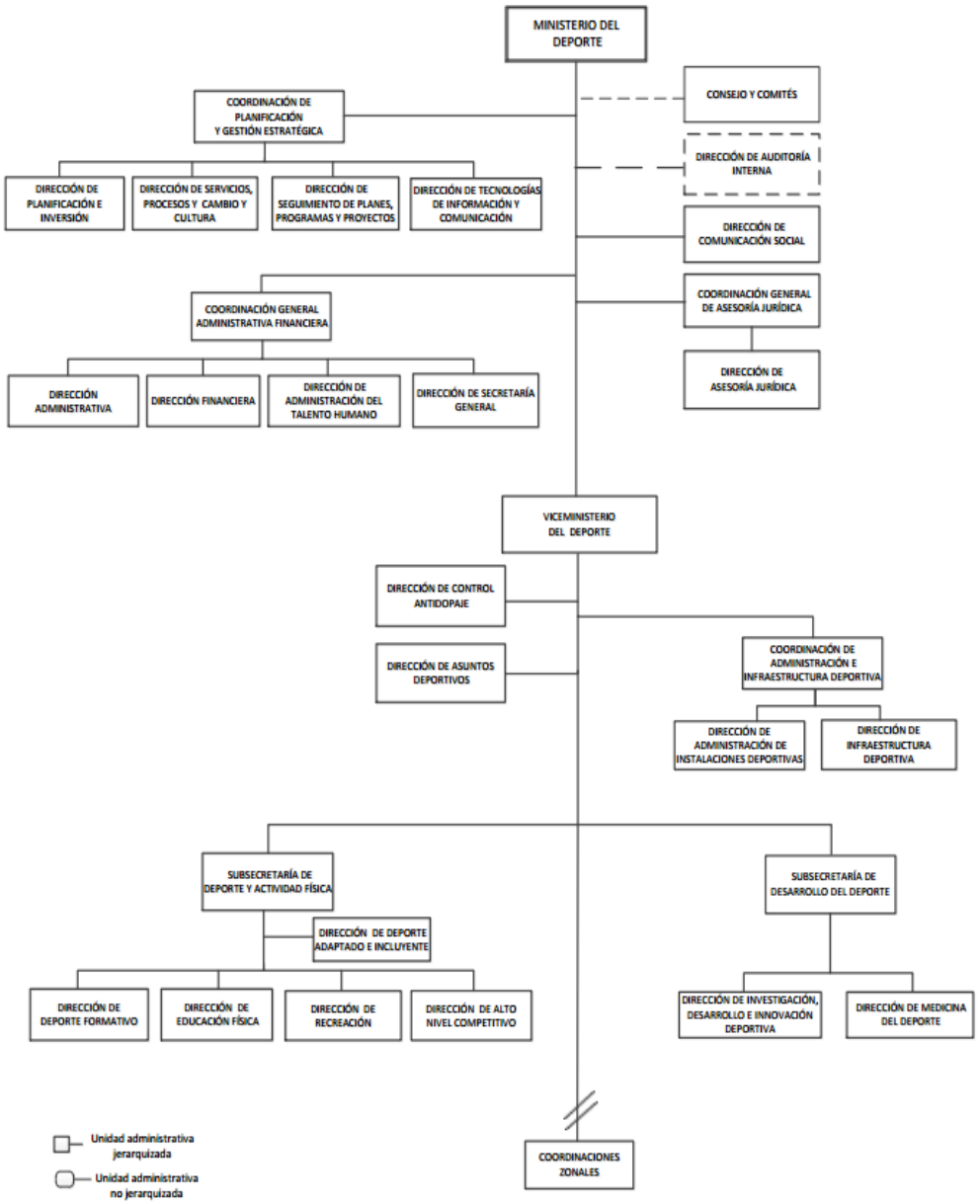


Figura 2 Estructura Administración Central Ministerio del Deporte (MINDE 2016)

3.1.3 Dirección Tecnologías de Información y Comunicación.

La Misión de la Dirección de Tecnologías de Información y Comunicación es diseñar, planear y gestionar procesos y proyectos TIC, mediante la implementación de políticas públicas.

El responsable de la DTIC es el director/a con los siguientes deberes y obligaciones:

- Dirigir, gestionar y evaluar la implementación del "Plan Estratégico de Tecnologías de Información (PETI)", POATIC, plan anual de compras de TIC (PACTIC) alineados al plan estratégico institucional, al cumplimiento del Plan Nacional de Gobierno Electrónico y a las políticas y objetivos gubernamentales;
- Gestionar los proyectos de contingencia que garantice la continuidad del servicio tecnológico en la institución;
- Monitorear y disponer las acciones necesarias para la aplicación del EGSI[4].

La estructura interna organizacional de la Dirección de Tecnológica está conformada por:

[4] EGSI "Esquema Gubernamental de Seguridad de la Información"

Figura 3 Estructura interna organizacional de la Dirección de Tecnologías de Información y Comunicación del Ministerio del Deporte (Estatuto Orgánico de Gestión Organizacional por Procesos)

Gestión Interna de proyectos TIC: es la unidad encargada del cumplimiento de las siguientes responsabilidades

- Portafolio de desarrollo de soluciones tecnológicas propias, adquiridas y adaptadas.
- Sistemas informáticos desarrollados, adquiridos o adoptados.
- Repositorios e inventarios de códigos fuente versionados, aplicativos desarrollados, adquiridos o adaptados.
- Manuales de procedimientos de software desarrollado a la medida y estándares de TI.

Gestión Interna de Infraestructura TI: esta unidad interna de la DTIC, posee las siguientes responsabilidades

- Proyectos tecnológicos.
- Planes de acción y mejoras en la infraestructura, aplicaciones y soporte de los servicios tecnológicos, catálogos de problemas y soluciones para las diferentes aplicaciones.
- Informes de incidentes atribuidos a la arquitectura, gestión y mantenimiento de aplicaciones de sistemas y servicios tecnológicos.
- Diagramas de aplicaciones y arquitecturas.
- Informes periódicos del centro de datos.

Gestión Interna de Soporte a Usuarios: hace referencia al grupo de personas que brindan soporte técnico a través del centro de mesa de ayuda SysAid Help Desk, teniendo las siguientes responsabilidades a su cargo.

- Informes periódicos del número de activos, y planes de reposición de software y hardware.
- Inventario de soporte tecnológico, respaldos y restauraciones.
- Informes de seguimiento y control, así como también de las medidas de prevención y recuperación de servicios de TI.
- Actas de registro de equipos y programas instalados.
- Reportes de análisis estadísticos.

Gestión Seguridad Informática:

Esta Unidad se encuentra contemplada en el Estatuto Orgánico, sin embargo aún no existe responsable de la misma.

3.1.4 Diagnóstico del estado actual de Seguridad de la Información.

El Ministerio del Deporte al ser parte de la Administración Pública Central, genera, utiliza, procesa y almacena información en medios electrónicos, escritos, clasificada como pública, confidencial, reservada por lo tanto debe hacer uso del EGSI en sus procedimientos internos. (PUBLICA, 2013)

Con el propósito de determinar la situación actual de la DTIC, se evaluó la aplicación de la norma NTE[5] ISO[6]/IEC[7] 27002, a continuación se detalla la evaluación de diagnóstico realizada con el apoyo y participación de todos los funcionarios de la DTIC en el periodo comprendido de febrero a junio de 2017, la calificación a la evaluación tomó en consideraron tres parámetros:

- **Documentación:** Normas, políticas, procedimientos formalmente establecidos.
- **Implementación:** La aplicación de lo establecido en la documentación
- **Verificables:** Informes, diagramas de red, reportes, informes, e-mails, etc.

[5] NTE Norma Técnica Ecuatoriana
[6] ISO Organización Internacional de Estandarización
[7] IEC Comisión Internacional Electrotécnica

A continuación, se detalla el banco de preguntas de la encuesta realizada, a todos los funcionarios de la Dirección de Tecnologías de Información y Comunicación, las mismas que han sido estructuradas conforme a la taxonomía descrita en la norma NTE ISO/IEC 27002.

Tabla 16

Política de seguridad de la información

#	PREGUNTA	RESP
1	La DTIC posee políticas de seguridad de información?	SI / NO
2	La DTIC cuenta con contratos de confidencialidad y no propagación de información aprobados de acurdo a la normativa legal?	SI / NO
3	La DTIC mantiene contacto con organizaciones públicas y privadas especializados en seguridad de informática?	SI / NO
4	Se ha identificado y evaluado los riesgos para la información y servicios del MD en los procesos que involucran terceras partes?	SI / NO
5	Se ha identificado los requisitos de seguridad previa a la entrega de servicios a la ciudadanía que utilicen información del MD?	SI / NO
6	Existe socialización a los funcionarios sobre las normas y políticas de seguridad?	SI / NO
7	Se dispone de controles de verificación de efectividad de políticas?	SI / NO

Fuente: (ISO 27002)

Tabla 17

Organización de Seguridad dela Información

#	PREGUNTA	RESP
1	¿Existe un procedimiento de autorización del Oficial de Seguridad de la Información, para el uso de nuevos sistemas o servicios contratados?	SI / NO
2	¿Existen acuerdos de confidencialidad y no divulgación de información, debidamente legalizados?	SI / NO
3	¿Existen procedimientos que especifiquen cuando y a quien notificar un acontecimiento relacionado a seguridad (SNAP, Fiscalía, Bomberos, Policía, ECUSERT, etc.)?	SI / NO
4	¿Existe un análisis de riesgos para la información o servicios que involucran terceras partes?	SI / NO
5	¿Se realiza análisis de seguridad previo a la entrega de servicios a la ciudadanía u otras instituciones gubernamentales?	SI / NO

Fuente: (ISO 27002)

Tabla 18

Gestión de los activos

#	PREGUNTA	RESP
1	¿La DTIC mantiene un inventario actualizado de software y hardware?	SI / NO
2	¿Existe responsables asignados por grupo de activos, quienes deban clasificar, documentar el uso de los mismos?	SI / NO
3	¿Se ha documentado e implementado políticas para la utilización correcta de activos relacionados con servicios de procesamiento?	SI / NO
4	¿Se encuentra reglamentado el uso del correo electrónico institucional?	SI / NO
5	¿La DTIC cuenta con métodos para catalogación y etiquetado de la información?	SI / NO
6	¿El uso de internet y sus aplicaciones se encuentra regulado a través de la asignación de perfiles de usuario?	SI / NO

Fuente: (ISO 27002)

Tabla 19

Seguridad de los recursos humanos.

#	PREGUNTA	RESP
1	¿Se expone de manera explícita las condiciones de confidencialidad y responsabilidades conforme a las funciones de cada funcionario de la DTIC?	SI / NO
2	¿La DTIC dispone de un proceso para retiro de permisos y credenciales de cuentas de usuario, en la desvinculación de un funcionario?	SI / NO
3	¿Se comunica a los funcionarios de la DTIC sobre las prohibiciones y restricciones de test de vulnerabilidades de su infraestructura tecnológica?	SI / NO
4	¿Se dispone de un procedimiento disciplinario para los funcionarios quienes incumplan la política de resguardo de la información?	SI / NO

Fuente: (ISO 27002)

Tabla 20

Seguridad física y del entorno

#	PREGUNTA	RESP
1	¿La permanencia de terceros al Data Center es revisada y supervisada?	SI / NO
2	¿La DTIC cuenta con protección contra fallos de energía eléctrica, el mismo que permita mantener las operaciones y servicios críticos de manera ininterrumpida?	SI / NO
3	¿El acceso a áreas restringidas como el Data Center, está controlado con un sistema de seguridad biométrico?	SI / NO
4	¿Existe documentación respecto al proceso de revisión y evidencia del mantenimiento del sistema automático contra incendios del Data Center?	SI / NO
5	¿Los funcionarios de DTIC están preparados en caso de una emergencia producida por fuego?	SI / NO

Fuente: (ISO 27002)

Tabla 21

Gestión de comunicaciones y operaciones

#	PREGUNTA	RESP
1	¿Se encuentra documentada y formalizada la política o el procedimiento para los tipos de respaldo de información, como códigos fuente, bases de datos, etc.?	SI / NO
2	¿Se realiza revisiones periódica del contenido de software y datos de computadores que gestionan procesos clave de la institución	SI / NO
3	¿Sabe cuál es el procedimiento o acciones a seguir en caso de reportarse una falla en uno los sistemas web administrado por el MD?	SI / NO
4	¿Existen procedimientos definidos y documentados para el resguardo y contención de la información de los servicios críticos del MD?	SI / NO
5	¿Existe documentación asociada a la configuración y control de descargas de archivos maliciosos?	SI / NO

Fuente: (ISO 27002)

Tabla 22

Control de acceso

#	PREGUNTA	RESP
1	¿Existe una apolítica para el uso de servicios de red?	SI / NO
2	¿La DTIC cuenta con procedimientos formales y documentados para la asignación, creación de cuentas, parámetros mínimos de seguridad de contraseña, etc.?	SI / NO
3	¿Se ha realizado una evaluación de riesgos para identificar los segmentos de red donde se encuentren los activos críticos para la institución?	SI / NO
4	¿Se ha documentado y formalizado el procedimiento para la asignación de permisos de accesos para usuarios temporales en la red del ministerio?	SI / NO
5	¿La DTIC cuenta con un procedimiento formal para el registro y baja de accesos?	SI / NO
6	¿Existe claves de acceso individual para el ingreso a las sesiones de usuario?	SI / NO
7	¿Está limitado el número de intentos fallidos en la autenticación de inicios de sección?	SI / NO
8	¿Se ha incorporado medida de seguridad a los equipos móviles?	SI / NO

Fuente: (ISO 27002)

Tabla 23

Adquisición desarrollo y mantenimiento de sistemas

#	PREGUNTA	RESP
2	¿Se ha implementado seguridad en los procesos de desarrollo y ambientes de pruebas?	SI / NO
3	¿Existe un proceso documentado de la entrega de aplicativos a las direcciones requirentes?	SI / NO
4	¿Existe interoperabilidad mediante uso de web cervices gubernamentales?	SI / NO

Fuente: (ISO 27002)

Tabla 24

Gestión de incidentes de seguridad de la información

#	PREGUNTA	RESP
1	¿Saben los funcionarios como reportar un incidente de seguridad de la información?	SI / NO
2	¿Se ha definido las responsabilidades ante un incidente de Seguridad de la Información?	SI / NO
3	¿Existe un procedimiento formal de respuesta a incidentes de seguridad de la información?	SI / NO

Fuente: (ISO 27002)

Tabla 25

Gestión de la continuidad del negocio

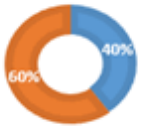
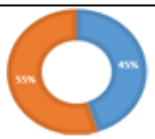
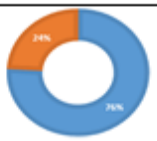
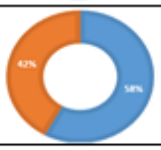
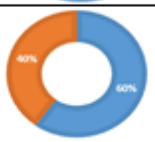
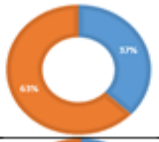
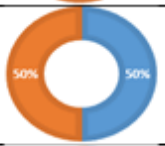
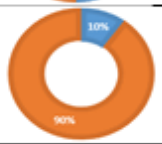
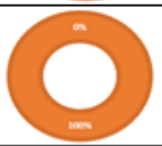
#	PREGUNTA	RESP
1	¿La DTIC cuenta con planes de continuidad de sus operaciones?	SI / NO
2	¿La DTIC realiza pruebas de mantenimiento y evaluación de sus planes de operaciones?	SI / NO
3	¿La DTIC cuenta con análisis de impacto de sus activos de información?	SI / NO
4	¿Existe un a análisis de riesgo aplicado a los activos críticos de la DTIC?	SI / NO

Fuente: (ISO 27002)

Resultados Evaluación de Diagnostico

La siguiente tabla muestra de manera resumida las respuestas a cada pregunta de diagnóstico.

Tabla 26
Resultado encuesta de diagnóstico

ENCUESTA ISO 27002	SI %	NO %	GRÁFICO
Política de seguridad de la información	40	60	
Organización de la seguridad de la información	45	55	
Gestión de los activos	76	24	
Seguridad de los recursos humanos	58	42	
Seguridad física y del entorno	80	20	
Gestión de comunicaciones y operaciones	60	40	
Control de acceso	37	63	
Adquisición desarrollo y mantenimiento de sistemas de información	50	50	
Gestión de los incidentes de seguridad de la información	10	90	
Gestión de la continuidad del negocio	0	100	

Fuente: (Hojas de Encuestas)

En función de la encuesta realizada se puede evidenciar de manera clara que no existe un correcto manejo y aplicación de normas NTE ISO/IEC 27002.

- **Política de seguridad de la información:** A pesar de que por ley el Ministerio del Deporte debe aplicar el uso de estándares nacionales detallados en el Acuerdo Nro. 166, existe un incumplimiento del 60% en su aplicación.
- **Organización de la seguridad de la Información:** el 55% de los encuestados considera que no existe una correcta organización debido a la ausencia de un oficial de seguridad, que cuente con un perfil tecnológico y los conocimientos necesarios para liderar la aplicación de la Norma ISO 27002 en el Ministerio del Deporte.
- **Gestión de los activos:** el 76% de los funcionarios de la DTIC, contesto que si se hace un correcto manejo de activos sin embargo el 24% considera que se debe mejorar en la documentación ya que aunque se aplica las mejores prácticas sus procesos de aplicación no se encuentran documentados, ni existe una designación formal del encargado de su cumplimiento.
- **Seguridad de los recursos humanos**: el 58% de los encuestados considera que existe una correcta gestión en la delegación de funciones y responsables definidos para la asignación de cuentas de usuarios en la entrada y salida de personal del Ministerio del Deporte, el 42% considera que no existe un proceso disciplinario definido a aplicarse en caso de incumplimiento de responsabilidades o violación de las políticas de la DTIC, lo que produce recurrencia en faltas a las disposiciones.

- **Seguridad física y del entorno:** El 80% considera que existe una correcta seguridad física del Data-Center ya que su acceso está controlado por un sistema biométrico y la permanencia de terceros es revisada y supervisada, el 20 % manifiesta que no existe documentación de revisión del mantenimiento del sistema automático contra incendios del Centro de Datos.
- **Gestión de comunicaciones y operaciones:** El 60% afirma que existe una adecuada gestión de comunicaciones y operaciones ya qiue los equipos de escritorio y laptops son utilizadas con sesiones de usuarios controlados por Active Directory limitando así todo permiso de instalación de aplicaciones no permitidas, el software instalado en los equipos terminales es definido previamente a los perfiles de las distintas direcciones a donde pertenece el equipo, sin embargo el 40% menciona que no existe una política formalizada para los distintos tipos de respaldos de información como códigos fuentes, bases de datos, etc.
- **Control de acceso:** El 63% considera que no existe una correcta gestión de control de acceso ya que aunque existe una política interna de la DTIC, ésta no ha sido aplicada correctamente.
- **Adquisición desarrollo y mantenimiento de sistemas de información:** El 50% afirman que aunque se cuenta con ambientes de pruebas y producción de aplicativos administrados por el Ministerio del Deporte, se debe mejorar los mecanismos de encriptación y gestión del cambio en las fases de desarrollo,

además se debe incrementar una fase de análisis de vulnerabilidades de los aplicativos web en producción.

- **Gestión de continuidad del negocio:** El 100% de los encuestados, considera que no existe una política o procedimiento identificado y socializado, esto se produce por la inexistencia de una metodología que permita el o levantamiento de insumos que genera este documento.

3.1.5 Hallazgos de Evaluación al Ministerio del Deporte

De conformidad con las atribuciones de la “Secretaría Nacional de la Administración Pública”, en referencia al uso del Acuerdo Nro. 166 de seguridad de la información, evaluó al Ministerio del deporte y de acuerdo al informe emitido por la Subsecretaria de Gobierno Electrónico con fecha 7 de julio de 2016 en referencia a la evaluación de aplicación de las Fases I y II del Esquema Gubernamental (EGSI), se obtuvo:

- Con relación al conocimiento de la Política de Seguridad el 74% de los funcionarios no conocen de la misma, al igual que el 76% no conocen de que se trata la Seguridad de la información.
- El mapa de procesos de la institución debe ser difundido, ya que el 62% de los funcionarios que respondieron la encuesta, no tienen conocimientos de los mismos.
- El 60% de los encuestados manifiesta que no ha recibido información relacionada con seguridad de la información.

- El 44% de los encuestados manifiesta que no sabe que procedimiento debe seguir en caso de ocurrir un incidente y el 56% que respondió si a la pregunta no tienen claro el procedimiento a seguir.
- El Oficial de Seguridad y sus funciones no se encuentran difundidas, ya que el 79% de los funcionarios no lo conocen.
- El 75% de los funcionarios no saben dónde encontrar la política, procedimientos o normas de la institución.
- La DTIC, no cuenta con una política de respaldos, los mismos se sacan en base a buenas prácticas, cada administrador de servicio tiene establecido horarios para la generación de respaldos y la extensión de los mismos, este procedimiento no se encuentra documentado, ni existe bitácoras de pruebas de respaldos de bases de datos.
- La institución actualmente realiza el listado de proveedores de servicios tecnológicos con números de contactos, los mismos que son actualizados por una determinada persona, por otro lado, los proveedores tienen la obligación de informar a la entidad si cambia o actualiza los contactos, dicho procedimiento no se encuentra documentado, es decir no se encuentra formalizado a través de un procedimiento.

Conforme a la metodología de evaluación de la Secretaría Nacional, el Ministerio del Deporte obtuvo una calificación en franja amarilla, la misma que corresponde a una evaluación REGULAR.

RANKING	SIGLAS	NOMBRE DE LA INSTITUCION	PERIODO DE EVALUACIÓN	MINISTERIO COORDINADOR	CALIFICACIÓN
17	MD	Ministerio de Deporte	18 al 19 de Mayo del 2016	Ministerio de Coordinación de Desarrollo Social	68,27%

Figura 5 Evaluación de cumplimiento ISO 27002 SNAP
Fuente: (PUBLICA, 2013)

En conclusión, tanto la evaluación realizada por la SNAP, como la encuesta de aplicación del Acuerdo No. 166, evidencian que no existe una correcta aplicación de la norma INEN ISO IEC 27002, y no existe un Plan de Continuidad del Negocio que garantice la prestación de servicios y sistemas tecnológicos.

3.1.6 ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

El “Análisis de Impacto del Negocio BIA”, será utilizado para identificar de forma clara los procesos misionales del Ministerio del Deporte que son soportados o gestionados por un servicio o sistema informático y evaluar su nivel de impacto en el caso de su suspensión parcial o total, para lo cual se planificaron múltiples sesiones de trabajo con las unidades de gestión interna, éstas sesiones de trabajo han permitido recopilar información relevante de los procesos de esta Cartera de Estado, que mantienen relación con sistemas o servicios informáticos.

En esta fase, la aplicación del BIA permite analizar los siguientes requerimientos:

- Identificar los procesos imprescindibles del Ministerio del Deporte en la prestación de servicios a la ciudadanía, los mismos que ante una interrupción deben estar claramente identificados y poseer asignación de prioridad, permitiendo así ser restablecidos a su estado operativo lo antes posible.
- Valorar los tiempos de recuperación, en función de las posibles fallas o irregularidades en los sistemas y servicios críticos y alta prioridad para el normal desenvolvimiento de la infraestructura tecnológica.

3.1.6.1 FASE 1: Identificación de Funciones, sistemas y servicios

Conforme a lo descrito en el fundamento teórico, el primer paso es la identificación de los activos de información de la Dirección Tecnológica, pudiendo estos poseer la siguiente clasificación:

- **Activos de Información**: Archivos, documentación del sistema, manuales, procedimientos, planes, bases de datos.
- **Documentación física impresa:** políticas, convenios de servicios, convenios operacionales, etc
- **Software:** Software arrendado, software propio, herramientas de desarrollo.
- **Hardware:** Infraestructura tecnológica de computación y comunicación.

Para la asignación de nombres únicos, se eligió la siguiente nomenclatura:

- **DTIC:** “Dirección de Tecnologías de Información y Comunicación”
- **GISU:** “Gestión Interna de Soporte a Usuarios”
- **GIP:** “Gestión Interna de Proyectos”
- **GII:** “Gestión Interna de Infraestructura”

Obteniendo así la siguiente matriz de activos de información.

Tabla 27
Matriz de Activos de Información de la DTIC

INFORMACIÓN BÁSICA				RESPONSABLES		
No.	**NOMBRE DEL ACTIVO**	**BREVE DESCRIPCIÓN**	**TIPO Información**	**PROPIETARIO**	**CUSTODIO**	**CUENTA CON UN RESPALDO (SI / NO)**
DTIC-GISU-004	OLYMPO	Sistema Contable Financiero, posee tres módulos; Gestión de Activos Fijos, Gestión de Garantías, Gestión de Vehículos, Gestión de Inventario	SOFTWARE	Direcciones: Servicios Institucionales, Financiero	Gestión Interna de Soporte a Usuarios	SI
DTIC-GISU-005	SLA	Service Level Agreement	SERVICIO	DTIC	GISU	NO
DTIC-GISU-007	PLANES APROBADOS E INFORMES	Planes aprobados e informes de mantenimiento preventivo y correctivo de hardware y software de usuarios finales.	FÍSICO	DTIC	GISU	NO
DTIC-GISU-008	CONSOLA DE ANTIVIRUS SYMANTEC	Suite Antivirus	SERVICIO	DTIC	GISU	NO

C ONTINÚA

DTIC-GISU-009	Sistemas Operativos	Sistemas Operativos de equipos terminales	SOFTWARE	DTIC	DTIC	
DTIC-GISU-010	Equipos de Usuarios	Equipos terminales de escritorio y laptops	HARDWARE	DTIC	Funcionarios	
DTIC-GIP-002	ARQUITECTURA TECNOLÓGICA DE TI	Arquitectura tecnológica de TI con características de escalabilidad y flexibilidad que reducen tiempos de atención en las soluciones, procesos, y proyectos de TI.	HARDWARE	GII	GII	NO
DTIC-GIP-006	REPOSITORIOS E INVENTARIOS	Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados.	INFORMACIÓN	GIP	GIP / Asistente DTIC	NO
DTIC-GIP-011	SISTEMA POR	Aprobación y reforma de estatutos, gestión de organismo deportivos.	SERVICIO WEB	Dirección Jurídica	Alex Naranjo	SI
DTIC-GIP-012	SISTEMAS DE SUBSIDIO MÉDICOS	SISTEMAS DE SUBSIDIO MÉDICOS	SERVICIO WEB	Dirección de Medicina del Deporte	Alex Naranjo	SI

CONTINÚA

DTIC-GIP-013	SEGUIMIENTO A LA SUSCRIPCIÓN Y LIQUIDACIÓN DE CONVENIOS	SEGUIMIENTO A LA SUSCRIPCIÓN Y LIQUIDACIÓN DE CONVENIOS	SERVICIO WEB	Dirección de Seguimiento de Planes Programas y Proyectos	Alex Naranjo	SI
DTIC-GIP-015	PENSIONES VITALICIAS	PENSIONES VITALICIAS	SERVICIO WEB	Dirección de Deportes	Alex Naranjo	SI
DTIC-GIP-017	KLIPFOLIO	KLIPFOLIO	SERVICIO WEB	Coordinación de Planificación	Alex Naranjo	SI
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Otorgamiento de personería jurídica a: * Clubes básicos * Clubes de deporte adaptado y/o paralímpico * Clubes especializados formativos. * Clubes especializados de alto rendimiento. * Personería jurídica a Ligas Deportivas barriales o parroquiales y cantonales. * Reconocimiento deportivo para grupos y organismos de ecuatorianos en el exterior. * Registro de Directorio para organismos deportivos	SERVICIO WEB	Dirección de Deportes	Alex Naranjo	SI

CONTINÚA

DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	SERVICIO	DTIC	Alex Naranjo	SI
DTIC-GIP-024	SERVIDOR APLICATIVOS WEB DE PRUEBAS	Servidor Aplicativos Web de Producción	SERVICIO	DTIC	Alex Naranjo	SI
DTIC-GIP-025	SISTEMA ECUADOR EJERCÍTATE	Servidor Aplicativos Web de Producción	SERVICIO	Dirección de Recreación	Alex Naranjo	SI
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Servidor Aplicativos Web de Producción	SERVICIO	Dirección de Recreación	Alex Naranjo	SI
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Motores de bases de datos de los sistemas administrados por el Ministerio del Deporte. (SQL Server 2008 R2 / MySql 5.5.40)	SOFTWARE	DTIC	GII	SI
DTIC-GII-001	PLANES DE ASEGURAMIENTO Y DISPONIBILIDAD INFRAESTRUCTURA TECNOLÓGI	Incluye la instalación, configuración y administración de hardware, middleware, base de datos, repositorios, entre otros.	FÍSICO	DTIC	GII	NO

CONTINÚA

DTIC-GII-002	PLANES DE ACCIÓN Y MEJORAS EN LA INFRAESTRUCTURA, APLICACIONES Y SOPORTE DE LOS SERVICIOS TECNOLÓGICOS	Catálogos de problemas y soluciones para las diferentes aplicaciones con prevención de impacto operativo a nivel de seguridad.	FÍSICO	DTIC	GII	NO
DTIC-GII-006	DIAGRAMAS DE APLICACIONES Y ARQUITECTURAS DE SERVIDORES	Redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación, centralización y virtualización.	FÍSICO	DTIC	GII	NO
DTIC-GII-007	INVENTARIO DE PRODUCCIÓN, MANTENIMIENTO DE REDES Y TELECOMUNICACIONES	Incidentes, planes de entrenamiento en aplicativos, respaldos y restauraciones.	FÍSICO	DTIC	GII	NO

CONTINÚA

DTIC-GII-008	PLANES APROBADOS E INFORMES DE MANTENIMIENTO	Preventivo y correctivo de hardware y software que reposa en el centro de datos	FÍSICO	DTIC	GII	NO
DTIC-GII-009	PHP LIST	Envió masivo de e-mails	SERVICIO	DTIC	GII	NO
DTIC-GII-010	VCENTER	VMWare VCENTER Server proporciona una plataforma centralizada para administrar sus entornos VMWare vSphere, lo que le permite automatizar y entregar una infraestructura virtual con confianza.	SOFTWARE	DTIC	GII	NO
DTIC-GII-011	MAIL BOX ZIMBRA	Proporciona servicio de mensajería electrónica	SERVICIO	DTIC	GII	SI
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Gestión de red	SERVICIO	DTIC	GII	SI
DTIC-GII-013	FILE SERVER	Almacenamiento de carpetas compartidas	SERVICIO	DTIC	GII	NO
DTIC-GII-014	CENTRAL TELEFÓNICA	Telefonía IP	SERVICIO	DTIC	GII	NO

CONTINÚA

DTIC-GII-015	ANTI SPAM CORREO	Servicio que bloquea el ingreso y salida de correo no deseado	SERVICIO	DTIC	GII
DTIC-GII-016	SERVIDOR DE CÁMARAS WEB	Circuito cerrado de video vigilancia	SERVICIO	DTIC	GISU
DTIC-GII-017	FIREWALL	Seguridad Perimetral	SERVICIO	DTIC	GII
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Sistema de Gestión de Almacenamiento	HARDWARE	DTIC	GII
DTIC-GII-019	[BACKUP] Sistema de Respaldo HP D2D 4210 FC	Servicio de respaldo	SERVICIO	DTIC	GII
DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000 AMD Opteron 2.3 GHz / 16 Core, 32 Gb Ram. Controladora de discos interna con 512 Mb de memoria cache, dos discos duros internos SAS, 4 puertos de red 1/10 Gbps autosensing. Dospuuertos fibra de 8 Gbps. 2 Switch LAN. 2 Switch SAN. 4 Fuentes de Poder. 6 ventiladores redundantes	HARDWARE	DTIC	GII

CONTINÚA

DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Servidor Controlador Dominio HP PROLIANT DL-380 G6	HARDWARE	DTIC	GII	NO
DTIC-GII-022	Anti Span Correo IBM System X3550 M3	Anti Span Correo IBM System X3550 M3	HARDWARE	DTIC	GII	NO
DTIC-GII-023	Servidor de dministración HP BL 465 GEN8	Servidor de dministración HP BL 465 GEN8	HARDWARE	DTIC	GII	NO
DTIC-GII-024	Racks de Ser	Racks de Servidores	HARDWARE	DTIC	GII	
DTIC-GII-025	Servidores	Conjunto de Equipos con altas prestaciones de procesamiento	HARDWARE	DTIC	GII	
DTIC-GII-026	Switches	Equipos de interconección	HARDWARE	DTIC	GII	
DTIC-GII-027	Red LAN	Red de datos de Área Local	HARDWARE	DTIC	GII	
DTIC-GII-028	Red Inalámbrica	Red inalámbrica de datos de Área Local	HARDWARE	DTIC	GII	
DTIC-GII-029	Enlace de Dato	Servicio de internet proporcionado por la Corporación Nacional de Telecomunicaciones, entre Planta Central y Coordinaciones Zonales,	SERVICIO	DTIC	GII	NO

De acuerdo al listado de activos de información es importante mencionar que la infraestructura más importante para el Ministerio del Deporte es:

INFRAESTRUCTURA TECNOLÓGICA DEL DATA-CENTER

Detalle de equipos instalados.

Para objeto de esta fase de identificación se ha tomado como muestra los equipos principales o más relevantes del cuarto de máquinas, la siguiente figura muestra los equipos principales instalados en el rack del Ministerio del Deporte.

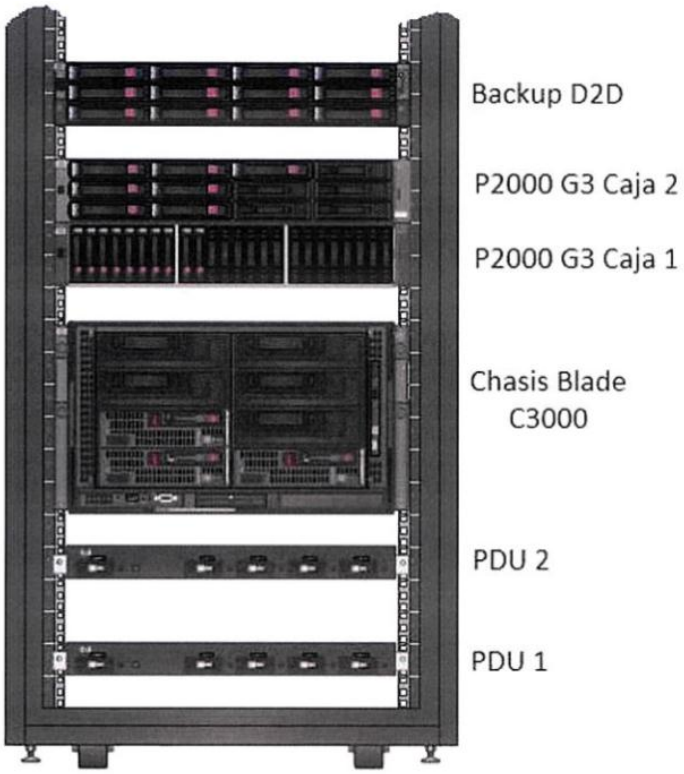


Figura 6 Rack Frontal Data-Center Ministerio del Deporte
Fuente: (Deporte, DTIC)

COMPONENTES DE LOS EQUIPOS

Chasis Blade C3000

Tabla 28
Componentes Chasis C 3000 (DTIC)

COMPONENTE	DESCRIPCIÓN
1 OnBoard Admnistrator	Módulo de Administración del chasis C3000
3 Servidores Blade BL465c Gen 8	Procesador Instalado AMD Opteron 2.30 GHz/16 – core /16MB/115W 32GB de memoria RAM en paletas de 8 GB Controladora de Discos Interna con 512 MB de memoria cache
2 Switch LAN	De 1 Gbps con 2 transceivers Fiber Channel cad uno, incluye cables de fibra.
2 Switch SAN	De 8 Gbps, con 4 transceivers Fiber Channel, incluye cables de fibra.
1 módulo KVM	
4 Fuentes de poder	Fuentes de poder redundante N+1
6 Ventiladores	Sistema de Ventilación Redundante

StorageWorks P2000 G3

Tabla 29
Componentes StoreWorks P2000 G3

COMPONENTE	DESCRIPCIÓN
2 Controladoras FC	2 GB de memoria cache por controladora (4 GB en total)
1 Caja de Discos	Con 10 discos de 500GB 6G SAS 7.2 K 2.5 in tipo SFF
1 Caja de Discos	Con 7 discos 6000GB 6G SAS 15K 3.5 in tipo LFF
2 Switch SAN	De 8 Gbps, con 4 transceiver Fiber Channel

StoreOnce D2D

Tabla 30
Componentes D2D 4106 FC

COMPONENTE	DESCRIPCIÓN
2 Controladoras FC	4 Gb FC (2) Ports por controladora
1 Caja de Discos	Con 12 discos 500 GB 3G 7.2k tipo LFF

Conexiones eléctricas de infraestructura tecnológica

La siguiente figura detalla la instalación de eléctrica del Data-Center

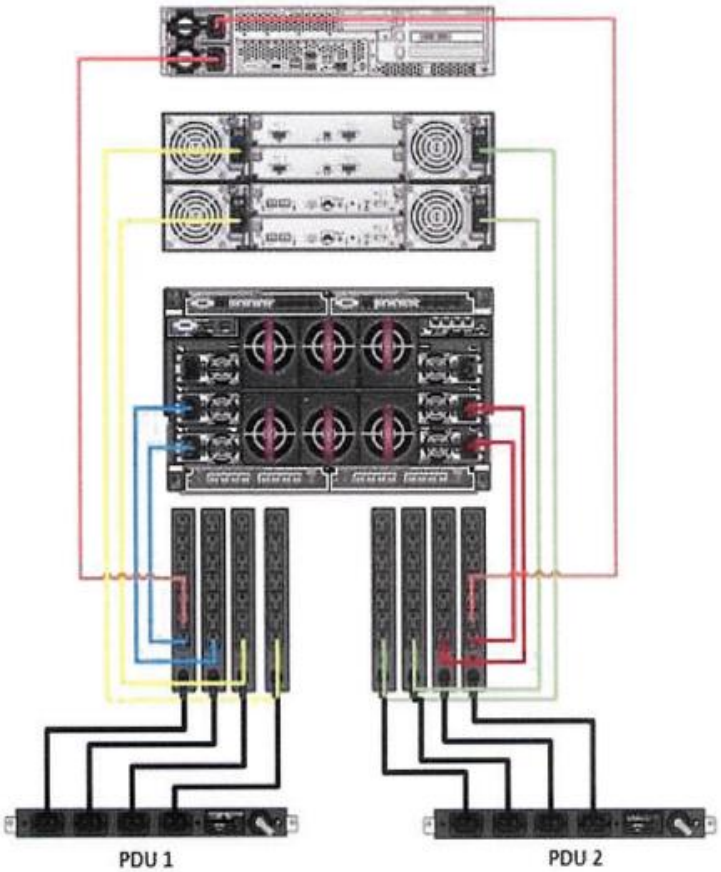


Figura 7 Conexiones eléctricas
Fuente: (Deporte, DTIC)

Conexiones SAN

La siguiente figura muestra la forma en la que se encuentra instalada la infraestructura SAN.

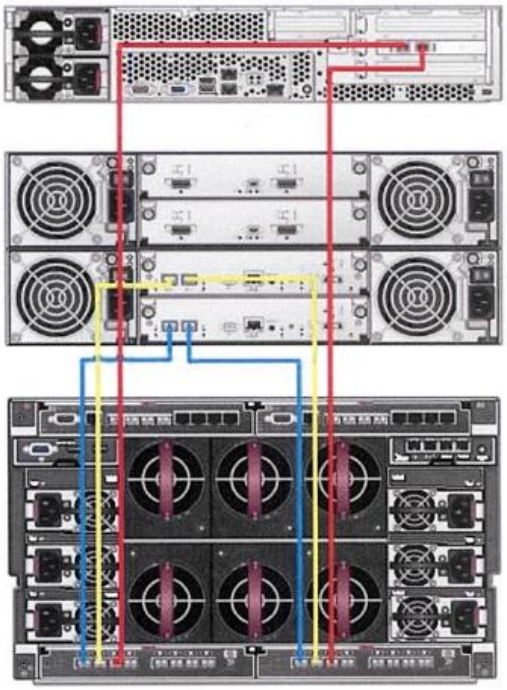


Figura 8 Conexiones SAN
Fuente: (Deporte, DTIC)

Las siguientes etapas describen paso a paso la implementación del análisis de impacto de negocio, así como el entregable correspondiente a cada apartado. En base al desarrollo de la primera etapa se pudo identificar que la DTIC se encuentra altamente vulnerable ante la materialización de un desastre, de ahí la necesidad inmediata del desarrollo de la fase de análisis que a continuación se detalla.

3.1.6.2 Fase 2: Evaluación de Impacto Operacional

Una vez identificados los activos que gestionan o que se relacionan con procesos misionales del Ministerio del Deporte, es necesario valorar el impacto que ocasionaría una suspensión al normal desenvolvimiento de los mismos.

Esta fase evalúa el grado adverso de una paralización en varios escenarios, la siguiente tabla detalla los niveles de criticidad de los activos de información del Ministerio del Deporte, la tolerancia a fallas se mide en horas, con un enfoque en los sistemas que deben funcionar todo el tiempo.

La valoración de los activos fue realizada en sesiones de trabajo con cada uno de los Coordinadores de las Gestiones Internas tomando como parámetros de calificación la siguiente tabla de valoración de impacto.

Tabla 31
Valoración Impacto

NIVEL	DETALLE
A	La operación es crítica para el negocio., la función del negocio no puede realizarse.
B	La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, función no crítica.
C	La operación no es una parte integral del negocio.

Fuente: Metodología BIA MINTIC

La siguiente matriz muestra el resultado de la aplicación de esta valoración:

Tabla 32
Valoración Operacional por niveles de criticidad

INFORMACIÓN BÁSICA			IMPACTO	
No.	**NOMBRE DEL ACTIVO**	**BREVE DESCRIPCIÓN**	**NIVEL**	**Tolerancia Fallos**
DTIC-GISU-004	OLYMPO	Sistema Contable Financiero, posee tres módulos; Gestión de Activos Fijos, Gestión de Garantías, Gestión de Vehículos, Gestión de Inventario	B	8
DTIC-GISU-005	SLA	Service Level Agreement	C	24
DTIC-GISU-007	PLANES APROBADOS E INFORMES	Planes aprobados e informes de mantenimiento preventivo y correctivo de hardware y software de usuarios finales.	C	24
DTIC-GISU-008	CONSOLA DE ANTIVIRUS SYMANTEC	Suit Antivirus	B	8
DTIC-GIP-002	ARQUITECTURA TECNOLÓGICA DE TI	Arquitectura tecnológica de TI con características de escalabilidad y flexibilidad que reducen tiempos de atención en las soluciones, procesos, y proyectos de TI	A	4
DTIC-GIP-006	REPOSITORIO E INVENTARIOS	Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados.	B	8
DTIC-GIP-011	SISTEMA POR	Aprobación y reforma de estatutos, gestión de organimos deportivos.	B	8
DTIC-GIP-012	SISTEMAS DE SUBSIDIO MÉDICOS	SISTEMAS DE SUBSIDIO MÉDICOS	C	24

CONTINÚA

DTIC-GIP-013	SEGUIMIENTO A LA SUSCRIPCIÓN Y LIQUIDACIÓN DE CONVENIOS	SEGUIMIENTO A LA SUSCRIPCIÓN Y LIQUIDACIÓN DE CONVENIOS	B	8
DTIC-GIP-015	PENSIONES VITALICIAS	PENSIONES VITALICIAS	C	24
DTIC-GIP-017	KLIPFOLIO	KLIPFOLIO	C	24
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Otorgamiento de personería jurídica a: * Clubes básicos * Clubes de deporte adaptado y/o paralímpico * Clubes especializados formativos. * Clubes especializados de alto rendimiento. * Personería jurídica a Ligas Deportivas barriales o parroquiales y cantonales. * Reconocimiento deportivo para grupos y organismos de ecuatorianos en el exterior. * Registro de Directorio para organismos deportivos	B	8
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	A	4
DTIC-GIP-024	SERVIDOR APLICATIVOS WEB DE PRUEBAS	Servidor Aplicativos Web de Pruebas	B	8
DTIC-GIP-025	SISTEMA ECUADOR EJERCÍTATE	Servidor Aplicativos Web de Producción	C	24

CONTINÚA

DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Registra todos los eventos deportivos a nivel nacional	A	4
DTIC-GIP-027	Base de Datos SQLServer y MySQL	Bases de datos de los distintos sistemas de administración interna del Ministerio del Deporte	A	4
DTIC-GII-001	PLANES DE ASEGURAMIENTO Y DISPONIBILIDAD INFRAESTRUCTURA TECNOLÓGICA	Incluye la instalación, configuración y administración de hardware, middleware, base de datos, repositorios, entre otros.	C	24
DTIC-GII-002	PLANES DE ACCIÓN Y MEJORAS EN LA INFRAESTRUCTURA, APLICACIONES Y SOPORTE DE LOS SERVICIOS TECNOLÓGICOS	Catálogos de problemas y soluciones para las diferentes aplicaciones con prevención de impacto operativo a nivel de seguridad.	C	24
DTIC-GII-006	DIAGRAMAS DE APLICACIONES Y ARQUITECTURAS DE SERVIDORES	Redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación, centralización y virtualización.	B	8
DTIC-GII-007	INVENTARIO DE PRODUCCIÓN, MANTENIMIENTO DE REDES Y TELECOMUNICACIONES	Incidentes, planes de entrenamiento en aplicativos, respaldos y restauraciones.	B	8
DTIC-GII-008	PLANES APROBADOS E INFORMES DE MANTENIMIENTO	Preventivo y correctivo de hardware y software que reposa en el centro de datos	C	24

CONTINÚA

DTIC-GII-009	PHP LIST	Envío masivo de e-mails	B	8
DTIC-GII-010	VCENTER	Herramienta de administración de recurso de VMWARE	A	4
DTIC-GII-011	MAILBOX ZIMBRA	Proporciona servicio de mensajería electrónica	A	4
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Gestión de red	A	4
DTIC-GII-013	FILE SERVER	Almacenamiento de carpetas compartidas	A	4
DTIC-GII-014	CENTRAL TELEFÓNICA	Telefonía IP	A	4
DTIC-GII-015	ANTI SPAM CORREO	Servicio que bloquea el ingreso y salida de correo no deseado	A	4
DTIC-GII-016	SERVIDOR DE CÁMARAS WEB	Circuito cerrado de video vigilancia	C	24
DTIC-GII-017	FIREWALL	Seguridad Perimetral	A	4
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Sistema de Gestión de Almacenamiento	A	4
DTIC-GII-019	[BACKUP] Sistema de Respaldo HP D2D 4210 FC	Servicio de respaldo	A	4
DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000	A	4
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Servidor Controlador Dominio HP PROLIANT DL-380 G6	A	4

CONTINÚA

DTIC-GII-022	Anti Span Correo IBM System X3550 M3	Anti Span Correo IBM System X3550 M3	B	8
DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Servidor de administración HP BL 465 GEN8	A	4
DTIC-GII-029	Enlace de Datos	Servicio de internet proporcionado por la Corporación Nacional de Telecomunicaciones, entre Planta Central y Coordinaciones Zonales,	A	4

3.1.6.3 Fase 3: Identificación de Activos Críticos

La identificación de activos críticos de información de la DTIC[8], se la realizó en función de la valoración de impacto operacional, así la siguiente tabla muestra el resultado de dicha identificación.

[8] DTIC “Dirección de Tecnologías de Información y Comunicación”

Tabla 33
Identificación de Procesos Críticos DTIC

INFORMACIÓN BÁSICA			IMPACTO	
No.	**NOMBRE DEL ACTIVO**	**BREVE DESCRIPCIÓN**	**NIVEL**	**Tolerancia Fallos (Horas)**
DTIC-GIP-006	REPOSITORIO E INVENTARIOS	Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados.	B	8
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	A	4
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	A	4
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Registra todos los eventos deportivos a nivel nacional	A	4
DTIC-GIP-027	Base de Datos SQLServer y MySQL	Bases de datos de los distintos sistemas de administración interna del Ministerio del Deporte	A	4
DTIC-GII-010	VCENTER	Herramienta de administración de recurso de VMWARE	A	4
DTIC-GII-011	MAIL BOX ZIMBRA	Proporciona servicio de mensajería electrónica	A	4
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Gestión de red	A	4
DTIC-GII-013	FILE SERVER	Almacenamiento de carpetas compartidas	A	4
DTIC-GII-014	CENTRAL TELEFÓNICA	Telefonía IP	B	8
DTIC-GII-015	ANTI SPAM CORREO	Servicio que bloquea el ingreso y salida de correo no deseado	A	4
DTIC-GII-017	FIREWALL	Seguridad Perimetral	A	4
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Sistema de Gestión de Almacenamiento	A	4
DTIC-GII-019	[BACKUS] Sistema de Respaldo HP D2D 4210 FC	Servicio de respaldo	A	4
DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000	A	4
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Servidor Controlador Dominio HP PROLIANT DL-380 G6	A	4
DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Servidor de administración HP BL 465 GEN8	A	4
DTIC-GII-024	Racks de Servidores	Rack de instalación	A	4

CONTINÚA

DTIC-GII-025	Servidores	Equipos tecnológicos de procesamiento	A	4
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Motores de bases de datos de los sistemas administrados por el Ministerio del Deporte. (SQL Server 2008 R2 / MySql 5.5.40)	A	4
DTIC-GII-029	Enlace de Datos	Servicio de internet proporcionado por la Corporación Nacional de Telecomunicaciones, entre Planta Central y Coordinaciones Zonales,	A	4
DTIC-GISU-09	Sistemas Operativos	Software para equipos Tecnológicos	A	4
DTIC-GISU-10	Equipos de Usuarios	Equipos terminales	A	4

3.1.6.4 Fase 4: Establecimientos de Tiempos de Recuperación

Toda vez que se ha identificado los activos críticos de la DTIC, es necesario determinar los tiempo de recuperación ante una alteración o falla de los servicios tecnológicos, para ello se identificó el Tiempo máximo de inactividad, de sus siglas en inglés (MTD), para lo cual se ha considerado que la mayoría de sistemas y servicios son utilizados dentro del horario de oficina, es decir de 08:00 de la mañana a 5:00 de la tarde, de ahí la valoración del tiempo que podría tolerar el Ministerio del Deporte antes de colapsar, en función del tiempo de tolerancia máximo de inactividad, esto permitirá demás priorizar la recuperación de sistemas y/o servicios.

Tabla 34
Descripción de tiempos de Recuperación

INFORMACIÓN BÁSICA			IMPACTO		TIEMPOS DE RECUPERACIÓN	
No.	**NOMBRE DEL ACTIVO**	**BREVE DESCRIPCIÓN**	**NIVEL**	**Tolerancia Fallos (Horas)**	**MTD (en días)**	**Prioridad de Recuperación**
DTIC-GIP-002	ARQUITECTURA TECNOLÓGICA DE TI	Arquitectura tecnológica de TI con características de escalabilidad y flexibilidad que reducen tiempos de atención en las soluciones, procesos, y proyectos de TI.	A	4	0.2	2
DTIC-GIP-006	REPOSITORIO E INVENTARIOS	Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados.	A	4	0.6	6
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	A	4	0.2	4
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Registra todos los eventos deportivos a nivel nacional	A	4	1	5
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Bases de datos de los distintos sistemas de administración interna del Ministerio del Deporte	A	4	0.2	3
DTIC-GII-006	DIAGRAMAS DE APLICACIONES Y ARQUITECTURAS DE SERVIDORES	Redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación, centralización y virtualización.	A	4	1	6

Fuente: (Funcionarios Direccion Tecnologias de Informacion y Comunicacion)

CONTINÚA

DTIC-GII-010	VCENTER	Herramienta de administración de recurso de VMWARE	A	4	0.2	2
DTIC-GII-011	MAIL BOX ZIMBRA	Proporciona servicio de mensajería electrónica	A	4	1	4
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Gestión de red	A	4	0.2	2
DTIC-GII-013	FILE SERVER	Almacenamiento de carpetas compartidas	A	4	1	4
DTIC-GII-014	CENTRAL TELEFÓNICA	Telefonía IP	A	4	1	4
DTIC-GII-017	FIREWALL	Seguridad Perimetral	A	4	1	2
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Sistema de Gestión de Almacenamiento	A	4	0.2	1
DTIC-GII-019	[BACKUP] Sistema de Respaldo HP D2D 4210 FC	Servicio de respaldo	A	4	1	5
DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000	A	4	0.2	1
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Servidor Controlador Dominio HP PROLIANT DL-380 G6	A	4	0.2	3
DTIC-GII-022	Anti Span Correo IBM System X3550 M3	Anti Span Correo IBM System X3550 M3	A	4	1	5

CONTINÚA

DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Servidor de administración HP BL 465 GEN8	A	4	0.2	3
DTIC-GII-029	Enlace de Datos	Servicio de internet proporcionado por la Corporación Nacional de Telecomunicaciones, entre Planta Central y Coordinaciones Zonales,	A	4	1	7

3.1.6.5 Fase 5: Identificación de Recursos Críticos

Los distintos servicios ofrecidos a la ciudadanía son gestionados por actividades realizadas por los Departamentos o Direcciones del Ministerio del Deporte las mismas que son apoyadas a través del uso de sistemas y servicios proporcionados por la Dirección Tecnológica, los mismos que conforman parte de las funciones críticas de esta Cartera de Estado, la identificación de recursos informáticos y sistemas de información que apoyan la realización y gestión de estos sistemas y servicios son identificados con el fin de medir su impacto en caso de inactividad.

Tabla 35
Identificación de recursos críticos

INFORMACIÓN BÁSICA				IMPACTO		IPOS DE RECUPERAC	
CATEGORÍA	**No.**	**PROCESO CRÍTICO (SERVICIOS)**	**BREVE DESCRIPCIÓN**	NIVEL	Tolerancia Fallos (Horas)	MTD (en días)	Prioridad de Recuperación
DATA CENTER	DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	A	4	0.2	3
	DTIC-GIP-027	Base de Datos SQL Server y MySQL	Bases de datos de los distintos sistemas de administración interna del Ministerio del Deporte	A	4	0.2	3
	DTIC-GII-010	VCENTER	Herramienta de administración de recurso de VMWARE	A	4	0.2	2
	DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000 AMD Opteron 2.3 GHz / 16 Core, 32 Gb RAM. Controladora de discos interna con 512 Mb de memoria cache, dos discos duros internos SAS, 4 puertos de red 1/10 Gbps autosensing. Dos puertos fibra de 8 Gbps. 2 Switch LAN. 2 Switch SAN. 4 Fuentes de Poder. 6 ventiladores redundantes	A	4	0.2	1
	DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	2 Controladoras FC (2 Gb de memoria cache por cada controladora 4 Gb en total) 1 Caja de discos (10 discos de 500 Gb SAS) 1 Caja de discos (7 discos de 600 Gb SAS) 2 Switch SAN (8 Gbps, con 4 transceiver Fiber Chanel)	A	4	0.2	1

CONTINÚA

SEGURIDAD DE INFORMACIÓN	DTIC-GII-017	FIREWALL CHEK POINT 4600	Reglas de entrada y salida de puertos. Reglas NAT/PAT Direccionamiento IP Gestión de enlaces a Coordinaciones Zonales Gestión de reglas de navegación por Coordinación Zonal Gestión de URL Filtering	A	4	0.2	1
SISTEMAS WEB	DTIC-GIP-027	Base de Datos SQL Server y MySQL	Motores de bases de datos de los sistemas administrados por el Ministerio del Deporte. (SQL Server 2008 R2 / MySql 5.5.40)	A	4	0.6	3
	DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Registro de eventos deportivos a nivel nacional.	A	4	1	5
	DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Otorgamiento de personería jurídica a: * Clubes básicos * Clubes de deporte adaptado y/o paralímpico * Clubes especializados formativos. * Clubes especializados de alto rendimiento. * Personería jurídica a Ligas Deportivas barriales o parroquiales y cantonales. * Reconocimiento deportivo para grupos y organismos de ecuatorianos en el exterior.	A	4	1	2

CONTONÚA

COMUNICACIONES	DTIC-GII-011	MAIL BOX ZIMBRA	Proporciona servicio de mensajería electrónica	A	4	1	4
	DTIC-GII-022	Anti Span Correo IBM System X3550 M3	Anti Span Correo IBM System X3550 M3	A	4	1	3

3.2 ETAPA II: ANÁLISIS DE RIESGOS.

Para la Dirección Tecnológica es importante documentar cada una de las etapas del análisis de riesgo, esto le permitirá volver a ejecutar el análisis de riesgo cada vez que considere pertinente, con el fin de mantener actualizada su información interna.

3.2.1 Fase 1: Identificación y selección de Amenazas

Para la identificación de amenazas se planificaron múltiples sesiones de trabajo, con los funcionarios de cada una de las Gestiones Internas de la Dirección Tecnológica, estas sesiones de trabajo han permitido recopilar información relevante de las amenazas a los procesos misionales de esta Cartera de Estado, que mantienen relación con sistemas o servicios informáticos.

La materialización de una amenaza puede afectar tanto información y procesos como también sistemas informáticos, estas se pueden clasificar como deliberadas o accidentales, tomando en consideración las amenazas más comunes se identificó aquellas que tienen mayor grado de afectación en los sistema y servicios suministrados por la DTIC.

Tabla 36
Amenazas Ministerio del Deporte

No.	PROCESO CRÍTICO (SERVICIOS)	AMENAZA
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Ausencias de pistas de auditoria
		Ataques de Jacker (SQL Inyection / Denegación de servicio / suplantación de identidad)
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Fuego
		Caida del sistema por saturación de espacio de almacenamiento (91% del almacenamiento se encuentra ocupado)
		• Saturación de espacio de procesamiento, el mismo sistema alberga al Servidor de archivos, motor de base de datos y servidor de aplicaciones web, lo cual provoca que se sature los recursos de procesamiento.
		Inexistencia de puntos de restauración del sistema operativo y configuraciones de servidor.
		Inexistencia de sistemas redundantes.
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Ausencia de pistas de auditoria
		Ataques de Hacker (Sql Inyection / Denegación de servicio / suplantación de identidad.
DTIC-GIP-027	Base de Datos SQLServer y MySQL	Inexistencia de raspaldpos de bases de datos frecuentes
		Inexistencia de administrador de bases de datos (el estatuto orgánico no contenpla la figura ni las competencias de administrador de bases de datos)
		Ataque SQL Inyection / ataque de negación de servicios
		Dependencia en el uso de web service de terceros
DTIC-GII-010	VCENTER	Suplantación de Identidad
		Abuso de privilegios de acceso
		Acceso no autorizado
		Interceptación de información (escucha)
		Caida del sistema por agotamiento de recursos.

CONTNÚA

DTIC-GII-011	MAIL BOX ZIMBRA	Robo de identidad
		Ataques de Fishing
		Reputación Web (Listas Negras)
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Abuso de privilegios de acceso, por falta de política de uso de perfiles de usuario.
DTIC-GII-013	FILE SERVER	Propagación de Virus
		Perdida de información
DTIC-GII-014	CENTRAL TELEFÓNICA	Errores de configuración por mala administración
DTIC-GII-015	ANTI SPAM CORREO	Errores de configuración provocaría mala reputación web
DTIC-GII-017	FIREWALL CHECK POINT 4600	Suplantación de Identidad
		Abuso de privilegios de acceso
		Acceso no autorizado
		Interceptación de información (escucha)
		Caida del sistema por agotamiento de recursos.
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)
		Fuego (El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual)
		Incumplimiento de mantenimiento del sistema
DTIC-GII-019	[BACKUS] Sistema de Respaldo HP D2D 4210 FC	Saturación de espacio de almacenamiento.
DTIC-GII-020	CHASIS SERVIDORES BLADE HP C3000	Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)
		Fuego (El Dta Center cuenta con un sistema automático de detección de incendio, sin embargo noesxiste registros de mantenimiento del mismo dede el año 2012, se desconoce su estado actual)
		Incumplimiento de mantenimiento del sistema
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Fuego

CONTNÚA

DTIC-GII-024	Racks de Servidores	Fuego
		Desastres Naturales
		Abería de origen físico o lógicpo
		Corte de suministro eléctrico
		Condiciones inadecuadas de temperatura y humedad
		Errores de mantenimiento/ actualiuzacion de equipos (hardware)
		Caida del sistema por agotamiento de recursos.
		Suplantación de identifdad
		Abuso de privilegios de acceso
DTIC-GII-025	Servidores	Errores de los usuarios
		Errores del admnistador del sistema de seguridad
		Pérdida de equipos
		Suplantación de identidad
		Abuso de privilegios de acceso
		Acceso no autorizado
DTIC-GII-026	Switches	Pérdida de equipos
		Acceso no autorizado
		Manipulación del hardware
		Robo de equipos
DTIC-GII-027	Red LAN	Suplantación de identidad
		Abuso de privilegios de acceso
		Acceso no autorizado
		Robo de equipos
		Repudio (negación de actuaciones)
DTIC-GII-029	Elace de Datos	Caida de enlace por daño en infraestructura del proveedor
		Degradación del servicio por equipos de telecomuniciones opsoletos
		Perdida de comunicación por inexistencia de enlace redundante.
		Servicio deficiente en la velocidad de transmisión
DTIC-GISU-09	Sistemas Operativos	Multas por uso de Software pirata, no licenciado
		Incremento de niveles de inseguridad por uso de software pirata
DTIC-GISU-10	Equipos de Usuarios	Daño por falta de mantenimiento
		Robo de los equipos
		Perdida de información por falta de respaldos periodicos

3.2.2 Fase 2: Identificación de Vulnerabilidades y Salvaguardas

Con el fin de evitar la duplicidad de controles, es necesario realizar la identificación de controles existentes y valorarlos conforme lo descrito en la siguiente tabla.

Tabla 37
Valoración de Riesgos

PARÁMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer control.	X	X	15
	Existen manuales, instructivos o procedimientos para el manejo de la herramienta.	X	X	15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva	X	X	30
Seguimiento al control	Están definidos los responsables de la ejecución de control y del seguimiento.	X	X	15
	La frecuencia de ejecución del control y seguimiento es adecuada.	X	X	25
			TOTAL	**100**

RANGOS DE CALIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS	
Entre 0 – 5 0	0	0
Entre 51 – 75	1	1
Entre 76 - 100	2	2

Fuente: (BCI, 2013)

Las salvaguardas o controles identificados y evaluados conforme a los parámetros proporcionados en la tabla 37, permite ubicar los controles dentro del rango correspondiente, identificando así vulnerabilidades del control y permitiendo tomar decisiones que mejoren la calificación obtenida.

Tabla 38

Salvaguardas activos críticos de la DTIC

INFORMACIÓN BÁSICA		FUENTE		VALORACIÓN DEL CONTROL						
No.	PROCESO CRÍTICO (SERVICIOS)	AMENAZA	SALVAGUARDA	C1 / 15	C2 / 15	C3 / 30	C4 / 15	C5 / 25	TOTAL	PUNTAJE
DTIC-GIP-006	REPOSITORIO E INVENTARIOS	Exceso de privilegios de acceso	NO EXISTE	0	0	0	0	0	0	0
		Acceso no autorizado por falta de restricción de acceso a servidores	Configuración de acceso por perfiles de usuario	15	0	10	10	0	35	0
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Ausencias de pistas de auditoria	NO EXISTE	0	0	0	0	0	0	0
		Ataques de Jacker (SQL Inyection / Denegación de sevicio / suplantación de identidad)	NO EXISTE	0	0	0	0	0	0	0
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Caida del sistema por saturación de espacio de almacenamiento (91% del almacenamiento se encuentra ocupado)	Borrado periódico de información	15	0	20	0	5	40	0
		Saturación de recursos de procesamiento, el mismo sistema alberga al Servidor de archivos, motor de base de datos y servidor e aplicaciones web, lo cual provoca que se sature los recursos de procesamiento	Incremento de memoria y procesamiento.	0	0	0	0	0	0	0
		Inexistencia de puntos de restauración del sistema operativo y configuraciones de servidor.	NO EXISTE	0	0	0	0	0	0	0
		Inexistencia de sistemas redundantes.	Se dispone de un servidor de pruebas el cual posee características similares de configuración, el mismo que en perdida del servidor de producción podría ser configurado, para sustituir al servidor web de producción	15	0	10	5	0	30	0
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Ausencias de pistas de auditoria	No Existe	0	0	0	0	0	0	0
		Ataques de Hacker (SQL Inyection / Denegación de servicio / suplantación de identidad)	No Existe	0	0	0	0	0	0	0
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Inexistencia de administrador de bases de datos	Actividad realizada por un asistente de tecnologías de Información	15	0	10	5	15	45	0
		Ataque SQL Inyection / ataque de negación de servicios	NO EXISTE	0	0	0	0	0	0	0
DTIC-GII-010	VCENTER	Suplantación de Identidad	Acceso restringido, sistema de administración local	5	5	30	15	5	60	1
		Abuso de privilegios de acceso	Las credenciales de acceso, son únicamente de conocimiento de los administradores del sistema.	5	0	15	15	5	40	0
		Acceso no autorizado	Acceso restringido, sistema de administración local	5	5	30	15	5	60	1
		Interceptación de información (escucha)	Firewall	15	10	30	15	25	95	2
		Caida del sistema por agotamiento de recursos.	NO EXISTE	0	0	0	0	0	0	0

CONTINÚA

DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Abuso de privilegios de acceso, por falta de política de uso de perfiles de usuario.	NO EXISTE	0	0	0	0	0	0	0
DTIC-GII-013	FILE SERVER	Propagación de Virus	Antivirus	15	5	15	15	20	70	
		Perdida de información	Inventario de permisos						0	
		No existe resplados de información	NO EXISTE	0	0	0	0	0	0	0
DTIC-GII-014	CENTRAL TELEFÓNICA	Errores de configuración por mala administración	Capacitación	15	10	20	10	20	75	
DTIC-GII-015	ANTI SPAM CORREO	Errores de configuración provocaría mala reputación web	Contratación de Servicio Vigente	15	10	25	10	25	85	
		Suplantación de Identidad		1	3	3			7	
		Abuso de privilegios de acceso	NO EXISTE	0	0	0	0	0	0	
DTIC-GII-017	FIREWALL CHEK POINT 4600	Acceso no autorizado (Invetario de credenciales de acceso es almacenado en un archivo de Excell)	Contraseña generica del archivo Excell	10	0	15	15	10	50	
		Interceptación de información (escucha)	NO EXISTE	0	0	0	0	0	0	
		Caída del sistema por agotamiento de recursos.	NO EXISTE	0	0	0	0	0	0	
		Inexistencia de Políticas de Control de Acceso a Servidores	NO EXISTE	0	0	0	0	0	0	
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Incumplimiento o terminación de vigencia de mantenimiento del sistema	NO EXISTE	0	0	0	0	0	0	0
		Daño simultaneo de dos discos duros	El Data Center de la DTIC, posee implementado un RAID 5, permitiendo la avería de un solo disco duro.	15	5	30	15	15	80	2
		Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)	NO EXISTE	0	0	0	0	0	0	0
		Fuego (El Dta Center cuenta con un sistema automático de detección de incendio, sin embargo noesxiste registros de mantenimiento del mismo dede el año 2012, se desconoce su estado actual)	NO EXISTE	0	0	0	0	0	0	0
		Incumplimiento de mantenimiento del sistema de almacenamiento	Cronograma de mantenimiento	15	10	25	15	25	90	
DTIC-GII-019	[BACKUS] Sistema de Respaldo HP D2D 4210 FC	Saturación de espacio de almacenamiento.	Terminos de referencia para la adquisisción de nuevos discos duros	0	0	0	0	0	0	0
DTIC-GII-020	CHASIS SERVIDORES BLADE HP C3000	Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)	NO EXISTE	0	0	0	0	0	0	0
		Fuego (El Dta Center cuenta con un sistema automático de detección de incendio, sin embargo noesxiste registros de mantenimiento del mismo dede el año 2012, se desconoce su estado actual)	NO EXISTE	0	0	0	0	0	0	0
		Incumplimiento de mantenimiento del sistema	1	0	0	0	0	0	0	0
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Fuego	El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual						0	0

CONTINÚA

DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Fuego	El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual	15	0	10	0	0	25	0
DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Corte de suministro eléctrico	El Data Center de la DTIC, cuenta con un UPS subdimensionado que suministra energía eléctrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de oficina.	15	5	15	15	0	50	0
		Condiciones inadecuadas de temperatura y humedad	Sistema de Climatización, presenta fallas de manera eventual	15	5	20	10	20	70	1
DTIC-GII-024	Racks de Servidores	Fuego	El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual	15	0	10	0	0	25	0
		Desastres Naturales	No Existe	0	0	0	0	0	0	0
		Avería de origen físico o lógico del servicio de energia electrica	Sistemas de alimentación initerumpida (UPS), mantenimiento de sistema de climatización	15	15	30	10	20	90	2
		Corte de suministro eléctrico	El Data Center de la DTIC, cuenta con un UPS subdimensionado que suministra energía eléctrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de oficina.	15	0	20	10	10	55	1
		Condiciones inadecuadas de temperatura y humedad	Sistema de Climatización	15	5	30	10	20	80	2
		Errores de mantenimiento/ actualización de equipos (hardware)	Contrato de soporte caducado	15	5	30	10	10	70	1
		Caída del sistema por agotamiento de recursos.	Proyección de requerimiento recursos	15	5	30	10	20	80	2
DTIC-GII-025	Servidores	Pérdida de equipos	Data Center con sistema de control de acceso (Biométrico)	15	15	25	15	20	90	2
		Suplantación de identidad	Contraseña de acceso a servidores, es de conocimiento de todos los funcionarios de la DTIC	0	0	0	0	0	0	0
		Abuso de privilegios de acceso	NO EXISTE	0	0	0	0	0	0	0
		Acceso no autorizado	NO EXISTE	0	0	0	0	0	0	0
DTIC-GII-026	Switches	Pérdida de equipos	Contrato de servicio de seguridad	15	15	20	15	25	90	2
		Acceso no autorizado	Gabinetes de pared ubicados en oficinas sin cerradura	0	0	0	0	0	0	0
		Manipulación del hardware	Uso de racks con cerradura	15	10	25	10	20	80	2
		Robo de equipos	Contrato de servicio de seguridad	15	15	20	15	25	90	2
DTIC-GII-027	Red LAN	Suplantación de identidad	NO EXISTE	0	0	0	0	0	0	0
		Abuso de privilegios de acceso	Restricción de Privilegios atraves de perfiles de usuario	10	10	25	15	20	80	2
		Acceso no autorizado	Uso de Active Directory para control de acceso.	15	15	20	15	20	85	2
		Robo de equipos	Servicio de compañía de guardias / video vigilancia	15	15	20	15	20	85	2
DTIC-GISU-009	Sistemas Operativos	Software pirata (Sin Licenciamiento)	No existe	0	0	0	0	0	0	0
		Difusión de software dañino	Uso de herramienta End Point Protection	15	15	25	15	20	90	2
DTIC-GISU-010	Equipos de Usuarios	fuego	Mantenimiento preventivo de Equipos contra incendio, señalética,	15	15	25	15	20	90	2
		corte de suministro eléctrico	Ninguna	0	0	0	0	0	0	0
		abuso de privilegios de acceso	Sesiones de usuario corresponde a perfil limitado	15	15	25	15	20	90	2
		Robo de equipos	Servicio de compañía de guardias / video vigilancia	15	15	25	15	20	90	2

CONTINÚA

3.2.3 Fase 3: Evaluación de Riesgo

Para la evaluación de riesgos es indispensable contar con los siguientes insumos:

- Catálogo de activos
- Registro de amenazas
- Catálogo de vulnerabilidades.
- Evaluación de controles

Con estos insumos es posible realizar una valoración de riesgos estimando su probabilidad de ocurrencia así como su grado de impacto en los activos y por consiguiente el grado de afectación negativa en el cumplimiento de objetivos misionales de la institución.

Tabla 39
Evaluación de riesgos

INFORMACIÓN BÁSICA		FUENTE		RIESGO		
No.	**PROCESO CRÍTICO (SERVICIOS)**	**AMENAZA**	**SALVAGUARDA**	**PROBABILIDAD (1-5)**	**IMPACTO (1-5)**	**RIESGO**
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	Ausencias de pistas de auditoria	NO EXISTE	2	4	8
		Ataques de Jacker (SQL Inyection / Denegación de sevicio / suplantación de identidad)	NO EXISTE	2	4	8
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Caida del sistema por saturación de espacio de almacenamiento (91% del almacenamiento se encuentra ocupado)	Borrado periódico de información	3	4	12
		Saturación de recursos de procesamiento, el mismo sistema alberga al Servidor de archivos, motor de base de datos y servidor e aplicaciones web, lo cual provoca que se sature los recursos de procesamiento	Incremento de memoria y procesamiento.	4	4	16
		Inexistencia de puntos de restauración del sistema operativo y configuraciones de servidor.	NO EXISTE	2	4	8
		Inexistencia de sistemas redundantes.	Se dispone de un servidor de pruebas el cual posee características similares de configuración, el mismo que en perdida del servidor de producción podría ser configurado, para sustituir al servidor web de producción	3	4	12
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Ausencias de pistas de auditoria	No Existe	2	4	8
		Ataques de Hacker (SQL Inyection / Denegación de servicio / suplantación de identidad)	No Existe	2	4	8
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Inexistencia de administrador de bases de datos	Actividad realizada por un asistente de tecnologías de Información	3	4	12
		Ataque SQL Inyection / ataque de negación de servicios	NO EXISTE	4	5	20

CONTINÚA

DTIC-GII-010	VCENTER	Suplantación de Identidad	Acceso restringido, sistema de administración local	1	2	2
		Abuso de privilegios de acceso	Las credenciales de acceso, son únicamente de conocimiento de los administradores del sistema.	2	4	8
		Acceso no autorizado	Acceso restringido, sistema de administración local	1	2	2
		Interceptación de información (escucha)	Firewall	1	2	2
		Caida del sistema por agotamiento de recursos.	NO EXISTE	3	3	9
DTIC-GII-011	MAIL BOX ZIMBRA	Robo de identidad	Caducidad de credenciales de acceso	3	4	12
		Ataques de Fishing	Herramienta Anti Spam	5	4	20
		Reputación Web (Listas Negras)	Herramienta Anti Spam	4	4	16
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Abuso de privilegios de acceso, por falta de política de uso de perfiles de usuario.	NO EXISTE	3	3	9
DTIC-GII-013	FILE SERVER	Propagación de Virus	Antivirus	3	5	15
		Perdida de información	Inventario de permisos	3	4	12
		No existe respaldos de información	NO EXISTE	3	5	15
DTIC-GII-014	CENTRAL TELEFÓNICA	Errores de configuración por mala administración	Capacitación	2	2	4
DTIC-GII-015	ANTI SPAM CORREO	Errores de configuración provocaría mala reputación web	Contratación de Servicio Vigente	2	3	6
DTIC-GII-017	FIREWALL CHEK POINT 4600	Suplantación de Identidad	Uso de perfiles de usuario	2	4	8
		Abuso de privilegios de acceso	NO EXISTE	2	4	8
		Acceso no autorizado (Invetario de credenciales de acceso es almacenado en un archivo de Excell)	Contraseña generica del archivo Excell	2	4	8
		Interceptación de información (escucha)	NO EXISTE	2	4	8
		Caída del sistema por agotamiento de recursos.	NO EXISTE	2	4	8
		Administración deficiente por inexistencia de Políticas de Control de Acceso a Servidores	NO EXISTE	3	3	9
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Incumplimiento o terminación de vigencia de mantenimiento del sistema	NO EXISTE	2	4	8
		Daño simultaneo de dos discos duros	El Data Center de la DTIC, posee implementado un RAID 5, permitiendo la avería de un solo disco duro.	3	3	9
		Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)	NO EXISTE	3	3	9
		Fuego (El Dta Center cuenta con un sistema automático de detección de incendio, sin embargo noesxiste registros de mantenimiento del mismo dede el año 2012, se desconoce su estado actual)	NO EXISTE	2	5	10
		Incumplimiento de mantenimiento del sistema de almacenamiento	Cronograma de mantenimiento	2	4	8

CONTINÚA

DTIC-GII-019	[BACKUS] Sistema de Respaldo HP D2D 4210 FC	Saturación de espacio de almacenamiento.	Terminos de referencia para la adquisisción de nuevos discos duros	3	4	12
DTIC-GII-020	CHASIS SERVIDORES BLADE HP C3000	Corte de energiía eléctrica (El Data Center de la DTIC, cuenta con un UPS que suministra energía electrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de ofcina)	NO EXISTE	3	3	9
		Fuego (El Dta Center cuenta con un sistema automático de detección de incendio, sin embargo noesxiste registros de mantenimiento del mismo dede el año 2012, se desconoce su estado actual)	NO EXISTE	2	5	10
		Incumplimiento de mantenimiento del sistema	1	2	3	6
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Fuego	El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual	2	5	10
DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Corte de suministro eléctrico	El Data Center de la DTIC, cuenta con un UPS subdimensionado que suministra energía eléctrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de oficina.	3	5	15
		Condiciones inadecuadas de temperatura y humedad	Sistema de Climatización, presenta fallas de manera eventual	3	5	15
DTIC-GII-024	Racks de Servidores	Fuego	El Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual	2	5	10
		Desastres Naturales	No Existe	3	5	15
		Avería de origen físico o lógico del servicio de energia electrica	Sistemas de alimentación initerumpida (UPS), mantenimiento de sistema de climatización	2	3	6
		Corte de suministro eléctrico	El Data Center de la DTIC, cuenta con un UPS subdimensionado que suministra energía eléctrica por 3 minutos, posteriormente se enciende la planta de energía de manera manual, solo en horario de oficina.	3	3	9
		Condiciones inadecuadas de temperatura y humedad	Sistema de Climatización	2	3	6
		Errores de mantenimiento/ actualización de equipos (hardware)	Contrato de soporte caducado	2	3	6
		Caída del sistema por agotamiento de recursos.	Proyección de requerimiento recursos	2	3	6
DTIC-GII-025	Servidores	Pérdida de equipos	Data Center con sistema de control de acceso (Biométrico)	2	5	10
		Suplantación de identidad	Contraseña de acceso a servidores, es de conocimiento de todos los funcionarios de la DTIC	3	4	12
		Abuso de privilegios de acceso	NO EXISTE	3	4	12
		Acceso no autorizado	NO EXISTE	3	4	12

CONTINÚA

DTIC-GII-026	Switches	Pérdida de equipos	Contrato de servicio de seguridad	1	3	3
		Acceso no autorizado	Gabinetes de pared ubicados en oficinas sin cerradura	2	2	4
		Manipulación del hardware	Uso de racks con cerradura			0
		Robo de equipos	Contrato de servicio de seguridad	1	2	2
DTIC-GII-027	Red LAN	Suplantación de identidad	NO EXISTE	2	3	6
		Abuso de privilegios de acceso	Restricción de Privilegios atraves de perfiles de usuario	3	4	12
		Acceso no autorizado	Uso de Active Directory para control de acceso.	2	3	6
		Robo de equipos	Servicio de compañía de guardias / video vigilancia	2	2	4
DTIC-GISU-009	Sistemas Operativos	Software pirata (Sin Licenciamiento)	No existe	5	2	10
		Difusión de software dañino	Uso de herramienta End Point Protection	3	2	6
DTIC-GISU-010	Equipos de Usuarios	fuego	Mantenimiento preventivo de Equipos contra incendio, señalética,	2	2	4
		corte de suministro eléctrico	Ninguna	2	2	4
		abuso de privilegios de acceso	Sesiones de usuario corresponde a perfil limitado	2	2	4
		Robo de equipos	Servicio de compañía de guardias / video vigilancia	2	2	4

3.2.4 Fase 4: Tratamiento de Riesgos

TABLA 40

Tratamiento de Riesgos

AMENAZA	TRATAMIENTO
DTIC-GIP-006 **REPOSITORIO E INVENTARIOS** (códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización)	**Realidad actual:** • Exceso de privilegios de acceso, las credenciales de acceso son entregadas con acceso total, sin ningún tipo de análisis de restricción. • Acceso no autorizado por falta de restricción de acceso a servidores, es imposible identificar quién hizo uso de operaciones privilegiadas y por lo tanto no se puede determinar responsabilidad
	Estrategia Propuesta: • Se debe implementar una política de control de acceso a servidores, la misma que contemple la asignación de permisos a operaciones privilegiadas • Se debe coordinar con la Dirección de Talento humano, la elaboración de Acuerdos de confidencialidad y no divulgación de información.

AMENAZA	SQL Inyection / DDoS / Suplantación de Identidad
DTIC-GIP-021 **SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS**	**Realidad actual:** • Ausencias de pistas de auditoria, el área de desarrollo hace uso del usuario Root, del motor de bases de datos, evitando así cualquier tipo de auditoria de transacciones. • Ataques de Jacker (SQL Inyection / Denegación de servicio / suplantación de identidad)
	Estrategia Propuesta: • Implementación de POOL de conexión al motor de bases de datos y migración a una nueva arquitectura de servicios. • La Gestión Interna de Infraestructura, debe ser la custodia del usuario súper administrador (Root) de los motores de bases de datos, los funcionarios que requieran acceso, deberán solicitar que se les asigne una sesión de usuario con los privilegios de acceso que requiera, para lo cual deberá existir un procedimiento formalmente definido, el mismo que permita obtener reportes de auditoria de transacciones críticas en las bases de datos.

AMENAZA	Fuego / Espacio almacenamiento
DTIC-GIP-023 SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	**Realidad actual:** • Fuego, el Data Center cuenta con un sistema automático de detección de incendio, sin embargo no existe registros de mantenimiento del mismo desde el año 2012, se desconoce su estado actual. • Caída del sistema por saturación de espacio de almacenamiento (91% del almacenamiento se encuentra ocupado) • Saturación de espacio de procesamiento, el mismo sistema alberga al Servidor de archivos, motor de base de datos y servidor de aplicaciones web. • Inexistencia de puntos de restauración del sistema operativo y configuraciones de servidor. • Inexistencia de sistemas redundantes.
	Estrategia Propuesta: • Se debe solicitor formalmente una inspección e informe del estado actual del sistema automático contra incendios, a la Dirección Administrativa, ya que de acuerdo al Estatuto Orgánico vigente le corresponde a la mencionada Dirección garantizar su correcto funcionamiento.

CONTINÚA

AMENAZA	Fuego / Espacio almacenamiento
	Estrategia Propuesta: • Se bebe definir formalmente un responsable de la Dirección tecnológica, que vele por la ejecución del control y seguimiento del sistema contra incendios, conforme a frecuencia adecuada que permita garantizar su correcto funcionamiento. • Definir una política de gestión para la información almacenada de sistemas y servicios informáticos, • Realizar una proyección de crecimiento de consumo de almacenamiento, tomando en consideración la demanda de años anteriores, • Con el fin de garantizar recursos de procesamiento, es necesario independizar los motores da bases de datos de SQLServer y MySQL, en un servidor independiente del servidor de archivos y servidor de aplicaciones web. • Solicitar a la Gestión Interna de Infraestructura la configuración de puntos de restauración del sistema operativo y configuraciones de servidor de producción de sistemas.

AMENAZA	Auditoria
DTIC-GIP-026 **SISTEMA DE ADMINISTRACIÓN DEPORTIVA**	**Realidad actual:** • Ausencias de pistas de auditoria
	Estrategia Propuesta: • Para todos los sistemas administrados internamente se deberá definir un catálogo de registros de auditoria básico para todos los aplicativos, y se deberá personalizar registros de auditoria para operaciones privilegiadas.

AMENAZA	Data Base Administrator (DBA)
DTIC-GIP-027 **Base de Datos SQL Server y MySQL**	**Realidad actual:** • Inexistencia de administrador de bases de datos • Ataque SQL Inyection / ataque de negación de servicios
	Estrategia Propuesta: • Conforme a lo descrito en el portafolio de productos y servicios, la administración de bases datos debe ser designado formalmente a la Gestión Interna de infraestructura. Las bases de datos son configuradas para mantener un correcto desempeño de acuerdo a los procedimientos definidos para su operación..

AMENAZA	
DTIC-GII-010 **VCENTER**	**Realidad actual:** • Suplantación de Identidad • Abuso de privilegios de acceso • Acceso no autorizado • Interceptación de información (escucha) • Caída del sistema por agotamiento de recursos.
	Estrategia Propuesta: • Se debe implementar una política de control de acceso a servidores, la misma que contemple la asignación de permisos a operaciones privilegiadas por medio de la asignación de nombres de usuario y contraseña individuales a cada administrador de sistemas o servicios tecnológicos. • Es necesario realzar un test de puertos abiertos y análisis que permita cerrar todos los puertos que no sean estrictamente necesarios. • Se debe realizar una proyección de crecimiento tomando en consideración los tres últimos años y coordinar con la Gestión Interna de Proyectos para iniciar con la elaboración de Términos de

	Referencia.

AMENAZA	
DTIC-GII-011 **MAIL BOX ZIMBRA**	**Realidad actual:** • Robo de identidad • Ataques de Fishing • Reputación Web (Listas Negras)
	Estrategia Propuesta: • Implementación de campañas de sensibilización a los funcionarios del Ministerio del Deporte en temas relacionados de phishing, los mismos que busquen formar buenos hábitos, tales como, no responder a enlaces en correos electrónicos no solicitados o en Facebook; no abrir adjuntos de correos electrónicos no solicitados; Proteja sus contraseñas y no las revele a nadie; no proporcione información confidencial a nadie por teléfono, entre otros. • Mantenga actualizado su navegador y aplique los parches de seguridad. • Análisis de eficacia de la herramienta

	Antiphishing, con el fin de identificar la necesidad de actualización o cambio de ser necesario.

AMENAZA	
DTIC-GII-012 **CONTROLADOR DE DOMINIO, AD, DNS, DHCP**	**Realidad actual:** • Abuso de privilegios de acceso, por falta de política de uso de perfiles de usuario.
	Estrategia Propuesta: • Es necesario la definición de una política, que contemple el procedimiento a seguir cuando un administrador de infraestructura o funcionario de la Dirección tecnológica es desvinculado de la institución, todas las contraseñas deben ser cambiadas con el fin de evitar represalias o disgustos que se materialicen en ataques a los sistemas o servicios tecnológicos.

AMENAZA	
DTIC-GII-013 **FILE SERVER**	**Realidad actual:** • Propagación de Virus • Perdida de información • No existe respaldos de información
	Estrategia Propuesta: • Es necesario definir un mecanismo de control, que verifique que el antivirus se encuentre siempre actualizado tanto en el servidor de archivos, como en los equipos terminales de todos los funcionarios, configurado de tal forma que escanee de manera automática todo dispositivo que se conecte a la PC, esto con el fin de disminuir la posibilidad de propagac

AMENAZA	
DTIC-GII-014 **CENTRAL TELEFÓNICA**	**Realidad actual:** • Errores de configuración por mala administración
	Estrategia Propuesta: • Para la designación del administrador de la central telefónica Asterisk, es necesario realizar un proceso de transferencia de conocimientos y capacitación, en temas relacionados a la configuración, restablecimiento de configuraciones, marco normativo en relación a la restricción de salida a números celulares, etc,

AMENAZA	
DTIC-GII-015 **ANTI SPAM CORREO**	**Realidad actual:** • Errores de configuración provocaría mala reputación web
	Estrategia Propuesta: • Una mala administración de la herramienta anti Spam, expone a la institución a altos niveles de riesgo de ser catalogado con mala reputación y colocado en listas negras, provocando suspensión del servicio y por ende interrupción en la comunicación por correo electrónico, por lo tanto es necesario la socialización de una cultura de prevención en temas de seguridad de la información, para lo cual se beberá elaborar charlas, conversatorios, simulacros, etc, que permitan formar a los funcionarios una cultura de prevención.

AMENAZA	SISMO, INCENDIO, APAGÓN
Componente	**Estrategia**
DTIC-GII-021 **Servidor Controlador Dominio HP PROLIANT DL-380 G6** **DTIC-GII-023** **Servidor de administración HP BL 465 4600**	**Realidad actual:** • La Dirección tecnológica no dispone de un centro de datos alterno. • Los respaldos (backup) de bases de datos son automatizados con periodicidad diaria.. • No existe backups de servidores virtuales. • El Data Center está equipado con un sistema de alimentación de energía eléctrica (UPS), que provee tres minutos. **Estrategia Propuesta:** • Es indispensable disponer de un sitio alterno, la Coordinación Zonal que albergue el Data Center alterno deberá cumplir con ciertos parámetros en sus instalaciones físicas. • El sitio alterno deberá estar equipado con servidores operativos para almacenar respaldos. • Todas las Coordinaciones Zonales poseen personal con perfil tecnológico calificado para actuar ante una emergencia y cumplir con los RTO

AMENAZA	
DTIC-GII-024 **Racks de Servidores**	**Realidad actual:** • Desastres Naturales • Corte de suministro eléctrico • Errores de mantenimiento/ actualización de equipos (hardware). • Caída del sistema por agotamiento de recursos.
	Estrategia Propuesta: • La Gestión Interna de Proyectos de la Dirección tecnológica debe iniciar con el análisis del proyecto de contratación de un sitio alterno en Cloud, identificando el tipo de servicio a contratar que mejores ventajas proporcione pudiendo ser, Aplicaciones como Servicio (SaaS), plataforma (IaaS). • Es necesario tomar en consideración el Decreto Nro. 135, sobre austeridad en Ecuador, • El suministro de energía eléctrico, es recomendación del proveedor de los equipos de infraestructura tecnológica, que se instale una acometida redundante desde el tablero principal.

AMENAZA	
	Realidad actual: • Acceso no autorizado • Manipulación del hardware • Robo de equipos • Suplantación de identidad • Abuso de privilegios de acceso • Acceso no autorizado
DTIC-GII-026 **Switches** **DTIC-GII-027** **Red LAN**	**Estrategia Propuesta:** • Se debe establecer un procedimiento formal que permita una correcta gestión de control de acceso, mediante la verificación periódica de los funcionarios que tienen acceso a través de los sistemas biométricos a áreas restringidas como el Data Center. • Con el fin de evitar manipulación inadecuada de servidores e infraestructura tecnológica es necesario la definición de un proceso de gestión de contraseñas, teniendo cuidado especial en la asignación de privilegios de acceso a servidores de administración de máquinas virtuales.

AMENAZA	
DTIC-GISU-009 **Sistemas Operativos**	**Realidad actual:** • Software pirata (Sin Licenciamiento) • Difusión de software dañino • Altos niveles de inseguridad de la Información
	Estrategia Propuesta: • Es necesario la elaboración de un análisis de factibilidad de uso de sistemas operativos Open Source, como Linux para equipos terminales, existen Direcciones Administrativas que por el tipo de información que gestionan, no podrán ser migrados a sistemas Linux, como es el caso de la Dirección Financiera que trabaja con matrices remitidas por Organismos Deportivos a nivel nacional, en formatos de Microsoft Office. • Iniciar un proceso de adquisición de sistemas operativos y paquetes office para las Direcciones Administrativas. El contrato debe contemplar el uso de actualizaciones con lo que se disminuirá el nivel de riesgo de seguridad por uso de software clandestino.

TABLA 41

Identificación de Amenazas

AMENAZA	SISMO, INCENDIO, APAGÓN
Componente	**Estrategia**
Información (Física / Digital)	**Realidad actual:** Información física: • La documentación legal emitida, como Acuerdos Ministeriales son guardados en expedientes impresos. • No existe respaldos de registros clínicos de la Dirección de Medicina del Deporte.
	Estrategia Propuesta: Información física: • Definir proceso de digitalización de documentación relevante. • Brindar las garantías adecuadas de seguridad física, cetectores de humo, extintores. • Definir políticas que permitan una correcta la conservación de documentos físicos críticos.

3.3 ETAPA III: DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Conforme a los pasos descritos por la metodología proporcionada por la Norma Internacional ISO 22301, en esta etapa se desarrolla cada uno de pasos descritos en la misma, tomando en consideración la información previamente identificada que permita formular un Plan de Continuidad de Negocio que dé solución a los riesgos identificados y que se adapte a la realidad del Ministerio del Deporte.

3.3.1 Fase 1: Contexto de la Organización

La aplicación del estándar internacional ISO 22301 se centrará en los sistemas y servicios tecnológicos del Ministerio del Deporte los mismos que son gestionados y administrados por la Dirección Tecnológica.

Entendimiento a la Organización y su Contexto

El Ministerio del Deporte fue creado con la misión de promover en la ciudadanía el uso del tiempo libre de una manera saludable mediante la práctica del deporte y la recreación, además promueve la práctica del deporte formativo y profesional para lo cual norma, regula y legaliza a toda organización deportiva como federaciones, clubes, ligas, etc, designando fondos económicos a los distintos organismos deportivos en base a una planificación anual, por lo tanto genera, administra información sensible

como Acuerdos Ministeriales, pensiones para deportivas, registros médicos de deportistas, informes de análisis anti dopaje, entre otros.

Partes Interesadas:

Los principales interesados en el levantamiento del Plan de Continuidad son:

- Ministra del Deporte
- Coordinador de “Planificación y Gestión Estratégica”
- Directora de “Tecnologías de Información y Comunicación”
- Coordinador de “Gestión Interna de Seguridad Informática”
- Coordinador de “Gestión Interna de Infraestructura tecnológica”

Entendimiento de las Necesidades de la Continuidad.

El Ministerio del Deporte al ser el ente rector del deporte ecuatoriano maneja información legal, financiera, administrativa y de control, de alto grado de sensibilidad, como es el caso de respaldos, acuerdos y resoluciones ministeriales de todas las instituciones deportivas a nivel nacional, así como también sistemas informáticos de gestión de todos los eventos deportivos ejecutados anualmente, los mismos que almacenan información sensible sobre subsidios, pensiones, antidopaje y detalles de gastos de los presupuestos asignados anualmente a cada entidad deportiva del Ecuador, todo esto enmarcado en el cumplimiento a los parámetros exigidos en el

Marco Regulatorio de Gobierno Electrónico, como el Decreto Ejecutivo 1384 de Interoperabilidad, el Acuerdo 166, basado en la Norma ISO 27002, Normas 410 de Control Interno de la Contraloría General del Estado, entre otras.

En el caso de existir manipulación o adulteración de ésta información, el impacto o daño al normal desenvolvimiento de ésta Cartera de Estado sería catastrófico, además de pérdida de imagen y reputación ante la ciudadanía debido a la interrupción de la prestación de sus servicios, con altos niveles de probabilidad de pérdida de información y datos o duplicidad de los mismos, afectando no solo a esta Cartera de Estado, sino a la representatividad, credibilidad y reputación de todas las entidades del servicio público en general.

Alcance del Plan de Continuidad de Negocio

La presente propuesta de titulación, elabora un prototipo como plan de continuidad para la Dirección Tecnológica de planta central del Ministerio del Deporte ubicado en la ciudad de Quito.

La propuesta contempla:

- Identificación de activos de información
- Identificación de activos críticos
- Identificación y análisis de peligros de los servicios críticos de la institución
- Identificación de amenazas potenciales a los servicios críticos

- Estimación de riesgos
- Tratamiento de riesgos
- Estrategias para recuperación de servicios críticos.
- Prioridad de recuperación de servicios.
- Responsabilidades para ejecución del Plan de Continuidad.

La propuesta no contempla los siguientes aspectos:

- Implementación del Plan de Continuidad de la Dirección de Tecnologías de Información y Comunicación, ya que los recursos económicos que involucre su implementación serán detallados y solicitados en el Plan Operativo Anual de Tecnologías de Información (POATIC), como parte del Plan Estratégico de Tecnologías de Información y Comunicación (PETI) del siguiente año fiscal, los mismos que pueden ser aprobados en su totalidad o parcialmente, conforme lo disponga la máxima autoridad (Ministro/a).
- Plan de emergencia para evacuación de edificios.
- Plan de reanudación de infraestructura tecnológica que no forme parte de los servicios críticos.
- Plan de recuperación de coordinaciones zonales del Ministerio del Deporte.

Los activos criticos de la DTIC que se ven envueltos son los siguientes:

Tabla 42

Servicios y aplicaciones Críticas de la DTIC

INFORMACIÓN BÁSICA			IMPACTO	
No.	**NOMBRE DEL**	**BREVE DESCRIPCIÓN**	**NIVEL**	**Tolerancia**
DTIC-GIP-021	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	SODE SISTEMA DE REGISTRO DE ORGANISMOS DEPORTIVOS	A	4
DTIC-GIP-023	SERVIDOR APLICATIVOS WEB DE PRODUCCIÓN	Servidor Aplicativos Web de Producción	A	4
DTIC-GIP-026	SISTEMA DE ADMINISTRACIÓN DEPORTIVA	Registra todos los eventos deportivos a nivel nacional	A	4
DTIC-GIP-027	Base de Datos SQLServer y MySQL	Bases de datos de los distintos sistemas de administración interna del Ministerio del Deporte	A	4
DTIC-GII-010	VCENTER	Herramienta de administración de recurso de VMWARE	A	4
DTIC-GII-011	MAIL BOX ZIMBRA	Proporciona servicio de mensajería electrónica	A	4
DTIC-GII-012	CONTROLADOR DE DOMINIO, AD, DNS, DHCP	Gestión de red	A	4
DTIC-GII-013	FILE SERVER	Almacenamiento de carpetas compartidas	A	4
DTIC-GII-014	CENTRAL TELEFÓNICA	Telefonía IP	B	8
DTIC-GII-015	ANTI SPAM CORREO	Servicio que bloquea el ingreso y salida de correo no deseado	A	4
DTIC-GII-017	FIREWALL	Seguridad Perimetral	A	4
DTIC-GII-018	SISTEMA DE ALMACENAMIENTO CENTRALIZADO (P2000)	Sistema de Gestión de Almacenamiento	A	4
DTIC-GII-019	[BACKUS] Sistema de Respaldo HP D2D 4210 FC	Servicio de respaldo	A	4
DTIC-GII-020	Chasis Servidores Blade HP C3000	Chasis Servidores Blade HP C3000	A	4
DTIC-GII-021	Servidor Controlador Dominio HP PROLIANT DL-380 G6	Servidor Controlador Dominio HP PROLIANT DL-380 G6	A	4
DTIC-GII-023	Servidor de administración HP BL 465 GEN8	Servidor de administración HP BL 465 GEN8	A	4
DTIC-GII-024	Racks de Servidores	Rack de instalación	A	4
DTIC-GII-025	Servidores	Equipos tecnológicos de procesamiento	A	4
DTIC-GIP-027	Base de Datos SQL Server y MySQL	Motores de bases de datos de los sistemas administrados por el Ministerio del Deporte. (SQL Server 2008 R2 / MySql 5.5.40)	A	4
DTIC-GII-029	Enlace de Datos	Servicio de internet proporcionado por la Corporación Nacional de Telecomunicaciones, entre Planta Central y Coordinaciones Zonales,	A	4
DTIC-GISU-09	Sistemas Operativos	Software para equipos Tecnológicos	A	4
DTIC-GISU-10	Equipos de Usuarios	Equipos terminales	A	4

Definición de Requerimientos y estrategia.

El objetivo primordial de la continuidad de actividades y asistencia de servicios tecnológicos es mantener operativos sus sistemas y aplicaciones a pesar de la materialización de un riesgo o evento inesperado; para lograr este objetivo es necesario que la reanudación de actividades y disponibilidad de servicios se lo realice lo antes posible, para ello es imprescindible el disponer de un Plan de Continuidad, el mismo que contempla procedimientos clave que de como resultado una alta disponibilidad de servicios tanto a funcionarios y público en general.

3.3.2 Fase 2: Liderazgo

El éxito de la aplicación del Plan de Continuidad depende en gran manera del grado de compromiso de la máxima autoridad (ministro/a) y el grupo jerárquico superior del Ministerio del Deporte, ya que son ellos quienes dispondrán la puesta en marcha de la presente política, además se deberá nombrar una comisión que velará por el cumplimiento de las actividades descritas en la política de continuidad, logrando así obligar a las demás partes interesadas a formar parte del proceso, de esta manera se conseguirá el compromiso de todos los funcionarios.

El liderar del Plan de Continuidad del Negocio conforme a la descripción de sus deberes y atribuciones descritas en el Esrtatuto Organicode Gestion Organizacional por Procesos será el Oficial de Seguridad de la Informacion, miembro de la Coordinación de Planificación y Gestión Estratégica, quien tendrá la responsabilidad

de formar comisiones que realicen el respectivo seguimiento al cumplimiento de metas planteadas.

Política de Continuidad del Negocio

Introducción

La política de Continuidad de Negocio tiene por objeto garantizar la continuidad de actividades de los procesos previamente identificados como críticos de la DTIC ante la presencia de un evento inesperado o la materialización de un riesgo que afecte la continuación de las operaciones en la prestación de sus servicios o aplicaciones.

Alcance

La presente política de Continuidad de Negocio, es de obligado cumplimiento para la DTIC de planta central del Ministerio del Deporte de la ciudad de Quito.

Política

La Política de Continuidad se sustenta en principios y compromisos, tales como:

- Es prioridad la protección y seguridad de las personas, tanto en situación normal como en escenario de crisis derivada de un desastre.
- Se deberá designar un grupo de funcionarios para la conformación de la Comisión de Continuidad quienes deberán participar activamente en el monitoreo evaluación y mejora del Plan de Continuidad de Negocio.

- Adoptar medidas razonables para la provisión permanente de recursos financieros, humanos y materiales que permitan garantizar la continuidad operativa de los procedimientos y actividades, en función de la criticidad de los mismos
- Definición de criterios de seguridad y fiabilidad que aseguren la continuidad de servicios claves proporcionados por terceros.
- Coordinar y ejecutar jornadas de capacitación, concienciación y formación a los funcionarios del Ministerio del Deporte en temas relacionados a responsabilidades y procedimientos para la continuidad de negocio.
- Tomar en consideración las mejores prácticas recomendadas por la norma ISO 22301, en la política de Continuidad.

Vigencia de Política

La vigencia de la política de continuidad será de un año a partir de su fecha de aprobación o hasta que exista algún cambio en la comisión de continuidad.

Incumplimiento de Política

Las partes comprendidas en la presente política están sujetas al estricto cumplimiento de la misma, en caso de incumplimiento el Ministerio del Deporte tiene la facultad de emitir sanciones acorde al nivel de impacto que produzca el incumplimiento, para lo cual tomará en consideración aspectos operacionales y legales.

Roles y Responsabilidades del equipo de recuperación TI

La Dirección de Talento Humano será la responsable de determinar un proceso de selección para elegir al personal idóneo para conformar la Comisión de Continuidad, quienes deben cumplir con siguientes obligaciones:

Tabla 43
Roles y responsabilidades Comisión de Continuidad.

ROL	RESPONSABILIDADES	DESTREZAS REQUERIDAS
OFICIAL DE SEGURIDAD DE LA INFORMACION **Coordinador de Recuperación de TI** **(CREI)**	• Mantener comunicación permanente con el Comite de Seguridad. • Administrar equipos de infraestructura, enlaces de datos, servicios de terceros. • Verificación de cumplimiento de tiempos • Administrar recursos para brindar continuidad de sistemas y servicios. • Administración de recursos. • Coordinar tareas del equipo de recuperación.	• Dirección • Trabajo en equipo • Comunicación efectiva • Gestión de personal

ROL	**RESPONSABILIDADES**	**DESTREZAS**
Coordinador Gesrtion Interna de Infraestructura (Redes y BD) **(CRBD)**	• Accionar y vigilar la ejecución del Plan de continuidad de infraestructura tecnológica. • Validar la reanudación de servicios de red luego de una interrupción. • Ejecutar procedimientos de diagnóstico de redes de un incidente. • Realizar cambios o actualizaciones al Plan de Continuidad, cuando las circunstancias lo ameriten. • Coordinar la restauración de respaldos de bases de datos, información cuando la situación lo amerite. • Definir políticas para el uso adecuado de respaldos de información y bases de datos.	• Liderazgo • Manejo de stress ante situaciones de apremio. • Conocimientos solidos de redes. • Conocimiento de administración de equipos tecnológicos de Centro de Datos.

Tabla 44
Roles y Responsabilidades

ROL	RESPONSABILIDADES	DESTREZAS REQUERIDAS
Seguridad de la DTIC Coordinador de Infraestructura	• Administración de infraestructura tecnológica. • Definir y aplicar políticas de restricción de acceso físico • Validar la disponibilidad del sitio alterno y diagnosticar el estado de la infraestructura tecnológica.	• Manejo de stress ante escenarios de apremio
Director de DTIC Coordinador de Personal Operativo (CPO)	• Coordinar las responsabilidades de los funcionarios de la DTIC, • Definir políticas de comunicación y actualización de medios de contacto • Definir tareas y responsabilidades a cumplir cada funcionario de la DTIC .	• Capacidad de trabajo bajo presión. • Manejo de personal
Coordinador de Aplicacione	• Apoyar a los usuarios de sistemas administrados por el MD. • Apoyar en la puesta en marcha del sitio alterno.	• Manejo de stress ante situaciones de presión

Toda vez que se han definido los roles y responsabilidades, es necesario listar las responsabilidades de la comisión como equipo.

Tabla 45
Responsabilidades de la Comisión de Continuidad

RESPONSABILIDADES	
Comisión de Continuidad de Negocio	• Velar por la gestión de la continuidad. • Implantar un mecanismo de valoración continua de amenazas. • Implantar mecanismos de mejora continua que permita mantener un plan de continuidad actualizado. • Definir controles que den cumplimiento a los tiempos determinados garantizando una recuperación inmediata de sistemas y servicios. • Verificar que el Plan de Continuidad sea correctamente socializado. • Capacitar constantemente a los funcionarios del Ministerio sobre la importancia de una conducta preventiva en y temas de seguridad.

3.3.3 Fase 3: Planificación.

En esta fase es importante definir de manera clara los objetivos que plantea alcanzar el Plan de Continuidad.

Objetivos

El Plan de Continuidad de Tecnologías de Información del Ministerio del Deporte busca alcanzar los siguientes objetivos.

- Mantener el nivel operativo de los servicios y aplicaciones críticos de la DTIC.
- Disminuir la probabilidad de pérdida y divulgación de información sensible de la DTIC.
- Garantizar la protección de activos críticos de la DTIC
- Diseñar un Plan de acción ante un desastre.
- Garantizar la buena imagen de la DTIC.

Factores Críticos de Éxito

Los componentes claves de triunfo son identificados en función de los objetivos planteados, así tenemos la siguiente tabla que presenta cada uno de ellos.

Tabla 46
Factores de éxito.

OBJETIVOS	FACTORES CRÍTICOS DE ÉXITO
Mantener el nivel operativo de los servicios y aplicaciones críticos de la DTIC.	Implementar un Data Center alterno que almacene la información, bases datos, códigos fuentes y respaldos de bases de datos de los activos críticos de la DTIC.
Disminuir la probabilidad de pérdida y divulgación de información sensible de la DTIC.	Implementar acuerdos de confidencialidad en los contratos de trabajo, con los funcionarios que administran, gestionan, o tienen acceso a información sensible.
Garantizar la protección de activos críticos de la DTIC	Elaborar y socializar políticas de respaldo de servicios y aplicaciones críticos de la DTIC.
Diseñar un Plan de acción ante un desastre.	Elaboración de documento para selección de Comisión de Continuidad con sus respectivas atribuciones y responsabilidades.
Garantizar la buena imagen de la DTIC.	Crear políticas que garanticen niveles adecuados de confidencialidad, integridad y disponibilidad

3.3.4 Fase 4: Soporte

Recursos

El Director/a tecnológico deberá contemplar en su próximo Plan Operativo Anual los recursos económicos necesarios que le permitan ejecutar su Plan de Continuidad, el ministro/a del Deporte deberá disponer la asignación de los recursos económicos solicitados por la DTIC

Competencia

A continuación, se detalla las características más importantes de los integrantes del grupo que bebe liderar el Plan de Continuidad.

Tabla 47
Requerimientos Equipo Plan de Continuidad.

ROL	REQUISITOS MÍNIMOS
Coordinador de Continuidad de Negocio	• Experiencia mínima dos años en la DTIC. • Tener conocimientos de Continuidad de Negocio.
Coordinador alterno de Continuidad de Negocio	• Experiencia mínima dos años en la DTIC. • Tener conocimientos de Continuidad de Negocio.
Equipo de Gestión de Riesgos	• Poseer conocimiento de la norma ISO 27000. • Pertenecer mínimo un año al Ministerio del Deporte
Equipo de Recuperación	• Experiencia mínima un año • Conocimientos específicos relacionados a sus
Equipo de Apoyo	• Experiencia laboral en la DTIC mínima de un año. • Conocimiento de las operaciones

Toma de conciencia y comunicación

Los miembros de la Comisión de Continuidad deben tener total conocimiento de la Política de Continuidad, con el fin de tener claro cual es su función dentro del equipo de trabajo, cumplir y hacer cumplir las directrices proporcionadas en este documento, así como también socializar a todos los funcionarios de la DTIC los procedimientos a través de charlas, capacitaciones, simulacros, material informativo la importancia de la oportuna y acertada participación de cada uno de los funcionarios de la DTIC en la puesta en macha de Plan de Continuidad, acciones que permitan restablecer los servicios y aplicaciones informáticas en el menor tiempo posible.

3.3.5 Fase 5: Operación.

La fase de operación se basa en el proceso de ejecución del BIA[9], el mismo que encuentra detallado fase por fase en el apartado 3.1.6.

Estrategia de Continuidad del Negocio

Para la elección de la estrategia de continuidad del negocio se han tomado en consideración los aspectos ambientales, tecnológicos, humanos y servicios suministrados por terceros, todos con un enfoque hacia la mitigación de los riesgos identificados en los activos críticos de la DTIC.

Escenarios de recuperación

[9] BIA “Análisis de Impacto del Negocio“

La elección del tipo de recuperación dependerá en gran manera de la magnitud del impacto del incidente que se requiere enfrentar, así los posibles escenarios son:

i. HOT SITE (Sitio Caliente)

Este escenario proporciona condiciones eléctricas, ambientales, mobiliarios y activos tecnológicos de red equipos de procesamiento en caso de un desastre, es decir se dispone de una réplica del ambiente de operación. Por ejemplo, si el Data Center del Ministerio del Deporte deja de funcionar, se podría mover todas sus operaciones de procesamiento de datos al sitio alterno. (Rouse, 2017)

ii. WARM SITE (Sitio Cálido)

Consiste en la instalación anticipada de equipos informáticos y ancho de banda acorde a la necesidad para que en caso de materialización de una amenaza o desastre se deba proceder únicamente a la configuración de del software para poder restablecer los sistemas del negocio.

iii. COLD SITE (Sitio Frio)

Un cold site consiste en un servicio de recuperación que provee un espacio físico, instalaciones eléctricas, y aire acondicionado pero no proporciona equipos informáticos, es decir el cliente instala todo el equipo necesario que le permita continuar sus operaciones. Un cold site es más económico, pero demanda más tiempo ponerlo en funcionamiento. (SANDRA, 2016)

iv. MOBILE SITE (Sitio Movil)

> Este tipo de escenario cuenta con equipos móviles de telecomunicaciones necesarias para implementar un sitio alterno de operación ante la notificación de la materialización de un desastre o interrupción prolongada. (Marcelo, 2013)

La siguiente tabla muestra un resumen de los escenarios de recuperación mencionados para facilitar la toma de decisiones.

Tabla 48
Escenarios de Recuperación

SITIO	COSTO	HARDWARE	TELECOMUNICACIONES	TIEMPO
Cold Site	Bajo	No	Ninguno	45 días
Warm Site	Medio	Parcial	Parcial	10 días
Hot Site	Alto	Completo	Parcial	15 días
Mobile Site	Alto	Variable	Variable	8 días
Mirror Site	Muy Alto	Completo	Completo	30 días

Conforme lo descrito en la tabla anterior, se ha tomado en consideración los costos y tiempo estimado de implementación.

Estrategias de Continuidad de Negocio

- **Acuerdo reciproco con "Centro de Entrenamiento para el Alto Rendimiento" (CEAR EP)**. La Coordinación Zonal 6 del Ministerio del Deporte perteneciente a la Provincia del Azuay, cumple con los requisitos necesarios de ubicación física, instalaciones eléctricas, aire acondicionado e interconexión de datos mediante enlace dedicado proporcionado por CNT hacia planta central, además del personal técnico capacitado para actuar ante la materialización de una amenaza o desastre.

- **Almacenamiento en la nube.** Esta solución es la más comúnmente utilizada por la mayoría de Instituciones públicas ya que los datos son almacenados en la nube, el proveedor para toda institución dependiente de la función ejecutiva es CNT, el mismo que posee distintos centros de almacenamiento de datos garantizando así la disponibilidad de los mismos en cualquier momento.

- **Servicios en la nube.** Entre los varios tipos de servicios que ofrece CNT se encuentran:
    - **SAS (Sofware as a Serevice)** este tipo de servicio permite al usuario acceder a través de un navegador a aplicaciones e información del usuario que están almacenados en la nube.

- **PASS (Platform as a Service).** Este servicio proporciona Fuentes para el desarrollo de aplicaciones web.
- **IASS (Infraestructure as a Service).** Este servicios suministra hardware a medida, es decir la institución estipula requerimientos en recursos de servidor, networking, memoria, ciclos de CPU y espacio de almacenamiento.

3.3.6 Selección de Estrategia de Continuidad del Negocio

Una vez analizadas las estrategias en conjunto con los coordinadores de la Gestión Interna de Infraestructura tecnológica, Soporte a Usuarios, Proyectos y Directora de TIC, se llega a la conclusión de que de acuerdo a las características propias del Ministerio del Deporte, las mejores opciones son:

- Implementación de un centro de datos alterno mediante un acuerdo reciproco con la Coordinación Zonal 6 Azuay.
- Almacenamiento en la nube.

Estas estrategias fueron elegidas tomando en consideración los factores económicos en coste de implementación, el recurso humano y mano de obra calificada, conectividad de red existente e infraestructura propia del Ministerio del Deporte.

3.3.6.1 Implementación de un Centro de Datos Alterno.

El desarrollo de esta estrategia se la realiza en función del escenario de acuerdo reciproco con el CEAR[10] de la provincia del Azuay.

i. Definición de términos y condiciones entre el Ministerio del Deporte y la Empresa Pública CEAR EP.
ii. Análisis de términos y condiciones
iii. Firma de acuerdo.
iv. Respaldar información crítica del Centro de Datos diariamente fuera del horario de oficina.

3.3.6.2 Almacenamiento en la Nube

i. Elaboración de términos de referencia con especificaciones técnicas de las capacidades de almacenamiento requeridas y tipo de servicio a contratar.
ii. Postulación de proyecto de contratación de servicio Cloud en el sistema de aprobación de contrataciones tecnológicas (CTI) del MINTEL[11].
iii. Contratación de servicio
iv. Respaldar información de sistemas y servicios críticos de forma diaria.

[10] CEAR “Centro de Entrenamiento para el Alto Rendimiento”
[11] MINTEL “Ministerio de Telecomunicaciones y Sociedad de la Información”

CAPÍTULO IV: CONCLUSIONES RECOMENDACIONES

4.1 Conclusiones.

Una vez finalizado el análisis y diseño de la propuesta del Plan de Continuidad de Negocios para la Dirección de Tecnología de Información y Comunicación del Ministerio del Deporte se puede llegar a las siguientes conclusiones:

- En base a la encuesta de cumplimiento a la norma NTE INEN ISO/IEC 27002, se pudo evidenciar de manera clara la inexistencia de un correcto y adecuado manejo de sistemas y servicios informáticos, produciendo un alto grado de vulnerabilidad al no existir ningún plan de continuidad del negocio que permita garantizar la confidencialidad, integridad y disponibilidad de sistema y servicios ante la presencia o materialización de una amenaza.
- Tanto las fases de identificación de amenazas, vulnerabilidades, tratamiento de riesgos, estuvieron enfocadas hacia los sistemas y servicios informáticos críticos los cuales son aquellos vinculados directamente con la ejecución de procesos misionales del Ministerio del Deporte, los mismos que interactúan con servicios ofrecidos a la ciudadanía, como es el caso de los sistemas administrados internamente, los cambios propuestos buscan disminuir la probabilidad de ocurrencia o disminución del impacto que provocaría en el

momento del materialización de una amenaza, mediante la optimización de recursos

- El análisis de impacto de negocio permitió identificar el nivel de impacto y tolerancia a fallos de los sistemas y servicios informáticos suministrados por la Dirección de Tecnologías de Información y Comunicación (DTIC), encontrando que todos los sistemas y servicios son gestionados desde el Data Center de administrado y gestionado por la Gestión Interna de Infraestructura, mediante la asignación de recursos de procesamiento, memoria RAM, espacio de almacenamiento, ante la presencia o materialización de una amenaza que paralice el normal funcionamiento del Data Center sería catastrófico, por lo tanto se realizó un plan de tratamiento de riesgos que disminuya el grado de impacto a un nivel aceptable.
- Para el desarrollo de cada una de las etapas del proyecto, fue necesaria el apoyo de la Coordinación de Planificación y Gestión Estratégica y la Dirección de Tecnologías de Información y Comunicación, así como de técnicos y analistas especialistas en el conocimiento del funcionamiento del negocio para garantizar el éxito del proyecto. La presente propuesta permitirá no sólo cumplir con lo dispuesto por los Organismos de control, sino que también provee un valor agregado que brinda la pauta inicial para futuros proyectos que fortalezcan la gestión de la continuidad en el Ministerio del Deporte.
- Se recomienda la contratación de servicios Cloud Computing, tales como los ofrecidos por la Corporación Nacional de Telecomunicaciones con VMWare,

para el respaldo de información crítica ya que al no contar con un Data Center externo existe un alto grado de vulnerabilidad de pérdida de información, además de la definición de políticas de respaldo y verificación de bases de datos de los sistemas web administrados internamente por la DTIC, los mismos que en un ambiente de pruebas deberá cumplir con todos los parámetros requeridos para su ejecución en producción.

- Mantener un plan de mantenimiento continuo a los procesos para su actualización por medio de revisiones periódicas de procesos, planes y procedimientos del Plan de Continuidad del Negocio.
- Se recomienda solicitar a la Dirección de Procesos el levantamiento del manual de procesos de la Dirección de Tecnologías de Información y Comunicación que permita un mejor gobierno de IT ya que la asignación de responsabilidades e interrelación entre las gestiones internas de la DTIC no están claramente definidas.
- Se debe implementar un proceso formal para la asignación de privilegios de acceso a servidores ya que hoy en día el acceso a servidores lo realizan todos los funcionarios de la DTIC, con un mismo usuario y contraseña genérica, lo cual impide la identificación de acciones de manera individual por medio de registros de auditoría, con lo que no se puede determinar responsabilidades por abuso de privilegios.

4.2 Recomendaciones

- Se recomienda designar formalmente a la Gestión Interna de Infraestructura el dar seguimiento al mantenimiento eléctrico y sistema automático contra incendios del Data Center, los mismos que no han recibido mantenimiento desde el año 2010, es necesario además la sustitución del Acuerdo 2023 de políticas de uso de servicios y sistemas informáticos, hay que sus conceptos son desactualizados y obsoletos, de esta manera seguir el proceso regular para la aprobación de políticas actualizadas mediante Acuerdo Ministerial, para posterior proceder a su socialización y aplicación, las mismas que faculten ade manera formal a la Dirección de Tecnologías de Información y Comunicación (DTIC) una correcta administración de su Data Center, sistemas y servicios.
- Una correcta gestión documental en la identificación de procesos críticos, es de vital importancia ya que permiten una mejor comprensión de la gestión de los mismos, la inexistencia de los mencionados documentados, implico la designación de más tiempo de entrevistas y visitas para realizar el análisis produciendo retraso al desarrollo del BCP.
- El incumplimiento a la aplicación de políticas detalladas en el Esquema Gubernamental de Seguridad de la Información (EGSI), basado en la INEN ISO/IEC 27002 genera una gran debilidad e impacto en la protección de información, por lo que se recomienda definir un plan de trabajo que permita dar

cumplimiento de manera eficaz, eficiente y efectiva a las los mencionados lineamientos.

- Coordinar con la Dirección de Talento Humano la definición de un proceso formal para la suscripción de acuerdos de confidencialidad y proceso disciplinario a aplicar en caso de incumplimiento al acuerdo.

BIBLIOGRAFÍA

(INEN), I. E. (2009). NTE INEN-ISO/IEC 27002:2009. Quito: INEN.

22301, I. (2011). *Business Continuity Management System.* Suiza: ISO.

BCI, B. C. (2013). *Good Practice Guidelines 2013.* Reino Unido: Edición Global.

Ciberseguridad, I. I. (2012). *Plan Director De Seguridad.* Madrid.

COLOMBIA, M. M. (2015). *Guía Para Realizar El Análisis De Impacto De Negocio Bia* Bogota: MINTIC.

Delgado, R. C. (2012). *Interoperabilidad Gubernamental. Quito, Ecuador.*

Deporte, M. D. (2015). *Ley Del Deporte, Educacion Fisica Y Recreacion.* Quito, Ecuador: Asamblea Nacional.

Deporte, M. D. (2016). *Estatuto Orgánico De Gestión Organizacional Por Procesos.* Quito, Ecuador.

Desarrollo, S. N. (2014). *Plan Nacional De Desarrollo.* Quito, Ecuador.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Estado, C. G. (2010). *Normas de Control Interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos.* Quito, Ecuador.

INEN, I. E. (2011). *NTE INEN-ISO/IEC 27001.* Ecuador.

INEN, I. E. (2011). *NTE INEN-ISO/IEC 27001.* Ecuador: Instituo De Altos Estudios Nacionales.

INEN, I. E. (2012). *ISO 22301.* Quito, Ecuador: INEN.

INEN, I. E. (2012). *NTE INEN ISO/IEC 27005.* Quito, Ecuador: INEN.

INSTITUTE, T. B. (2010). *Guía de Buenas Prácticas 2010.* Lee Glendon: Edición Global.

INTECO. (2013). *Implementación De Un Sgsi En La Empresa.*

ISACA, I. S. (2012). *COBIT 5 Procesos Catalizadores.* Illinois: ISACA.

ISO. (2011). *ISO 27035.* ISO.

ISO_31000. (2009). *Administracion del Riesgo.*

JOHN, S. (2012). *The Route Map to Business Continuity Management: Meeting the Requirements of ISO 22301.* Reino Unido: ISBN: 978-0-580-74341-2.

Marcelo, Á. (2013). Diseño e implementación de un DRP para Departamento de Ingenierías de la Empresa Continental Tire. *Universidad De Cuenca*.

Nacional, A. (2010). *Ley Del Sistema Nacional de Registro de Datos Públicos.* Quito, Ecuador.

Nacional, B. (2010). *Ley del Sistema Nacional de Registro de Datos Públicos.* Quito, Ecuador.

Nacional, C. (2002). *Ley de Comercio Electrónico, Firmas .* Quito, Ecuador.

Nacional, C. (2004). *Ley Organica de Transparencia y Acceso a la Información.* Quito, Ecuador.

Normalización, I. I. (2012). *INEN-ISO/IEC 9001:2012.* Quito.

Ortega, J. (2015). *Plan Estratégico De Tecnologías De Información Y Comunicación PETI.* Quito, Ecuador.

Publica, S. N. (2013). *Esquema Gubernamental De Seguridad De La Información.* Ecuador.

Públicas, M. D. (2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de. *Catálogo de Elementos*.

Públicas, M. D. (2014). *Methodology for Information Systems Risk Analysis and Management.* Madrid.

Rouse, M. (05 de noviembre de 2017). *Techtarget*. Obtenido de http://searchcio.techtarget.com/definition/hot-site-and-cold-site

Sandra, N. (2016). Plan de contiuidad de negocio para el departamento de TI de empresas. Caso de aplicación empresarial. *Escuela Politécnica Nacional*.

Secretaría Nacional de la Administración Pública SNAP. (2013). *Esqema Gubernamental de Seguridad de la Información.* Quito, Ecuador.

Secretaria Nacional de la Administración Pública, S. D. (2013). *Plan Nacional De Gobierno Electrónico.* Quito, Ecuador.

Standardization, I. O. (2004). *Information security incident management .* ISO.

Standardization, I. O. (2004). *Management of information and communications technology security.* ISO.