ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROPUESTA PARA UN ADECUADO MANEJO DE LA SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO 27002 PARA LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DEL DEPORTE, QUITO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE LA INFORMACIÓN

CÉSAR RENÉ AGUAYO CHAMORRO
cesitaraguayo@gmail.com

DIRECTOR: ING. DANNY GUAMÁN MSc.
danny.guaman@epn.edu.ec

CO-DIRECTOR: ING. FERNANDO FLORES MSc.
fernando.flores@epn.edu.ec

Quito, diciembre 2015

DECLARACIÓN

Mi persona, César René Aguayo Chamorro, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

César René Aguayo Chamorro

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por César René Aguayo Chamorro, bajo nuestra supervisión.

_____	_____
Ing. Danny Guamán	Ing. Fernando Flores
DIRECTOR DE PROYECTO	CO-DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A todas las personas que estuvieron pendientes de mí: familia, amigos y maestros.

César Aguayo

DEDICATORIA

A mi padre, mi madre y mi hermana, quienes me han dado mucho en la vida, pero sobre todo libertad y mucha paciencia.

A mis familiares más cercanos que estuvieron en todo momento en mi vida y con quienes he compartido gratos momentos además del apoyo incondicional.

A mis amigos y amigas, que curiosamente los que tienen apodos resultaron ser los mejores.

A quienes están, a quienes ya no están y a quienes quedaron en mi mente y corazón.

César Aguayo

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto de titulación tiene como objetivo realizar una propuesta para un adecuado manejo de la Seguridad de la Información en base a la norma ISO 27002, y usando como referencia a la norma 27001, para la Dirección de Gestión Tecnológica del Ministerio del Deporte, Quito.

Para ello se verificará la situación actual respecto al cumplimiento de los controles mencionados en la ISO/IEC 27002:2005.

Posteriormente se recopilará información para determinar los procesos que la Dirección de Gestión Tecnológica tiene como funciones y sus responsables. Esto permitirá identificar y relacionar dichos procesos con los activos.

Se realizará la valoración de activos en base a criterios de valoración previamente establecidos y justificados. Luego, se establecerán criterios de valoración para realizar el Análisis y Evaluación de Riesgos de la Dirección e identificar el tratamiento adecuado para los riesgos identificados.

Por medio del Enunciado de Aplicabilidad, se definirán los controles, con base a la norma ISO/IEC 27002:2005, que se requieren implementar y también aquellos que no, con su respectiva justificación.

Entonces, se establecerá la Política de Seguridad de la Información en base al Enunciado de Aplicabilidad y el Análisis y Evaluación de Riesgos previamente realizados.

Finalmente, se establecerán procedimientos de buenas prácticas en aquellos controles que lo requieran.

PRESENTACIÓN

Tanto las empresas públicas como privadas deben cumplir requerimientos mínimos en el manejo de la seguridad de su información. Estos requerimientos están estipulados en el Registro Oficial No. 88 y la Ley Orgánica de Transparencia y Acceso a la Información Pública.

La Dirección de Gestión Tecnológica del Ministerio del Deporte, como entidad pública, requiere tomar medidas que permitan favorecer la seguridad de la información. Para lograr este objetivo es necesario identificar los activos, y, tras darles una valoración, realizar el análisis y evaluación de riesgos para entender la situación actual de sus activos y responsabilidades. Tras conocer los riesgos es posible proponer una serie de políticas que pueden ser consideradas como referentes para una posterior y necesaria aplicación.

Es por ello que el presente proyecto realiza la propuesta para un adecuado manejo de la Seguridad de la Información en base a la norma ISO/IEC 27002:2005 para la Dirección de Gestión Tecnológica del Ministerio del Deporte, Quito.

En el capítulo 1 se realiza una descripción de los términos utilizados en la Seguridad de la Información y que serán utilizados a lo largo del desarrollo del proyecto. Además se mencionan metodologías para el análisis de riesgos, modelo PDCA y los lineamientos de la norma ISO/IEC 27002:2005

En el capítulo 2 se analiza el estado actual de la Dirección de Gestión Tecnológica y se establecen los lineamientos que se utilizarán para el Análisis de Riesgos. Se identifican activos, amenazas, vulnerabilidades y el impacto de ocurrencia de un evento. Posteriormente se realiza el Análisis y Evaluación de Riesgos.

En el capítulo 3 se presenta el Enunciado de Aplicabilidad y se establece la Política de Seguridad de la Dirección. Finalmente se incluyen algunos procedimientos referenciados en la Política.

En el capítulo 4 se establecen las conclusiones y recomendaciones del proyecto.

CAPÍTULO 1. MARCO TEÓRICO

1.1 ESTADO ACTUAL DE LA SEGURIDAD

Las empresas en el Ecuador tanto públicas como privadas requieren dar importancia al manejo de la seguridad de la información. Las medidas de seguridad tomadas en muchos casos no cumplen requisitos mínimos establecidos por algunos reglamentos y estándares vigentes. Además, a esto hay que añadirle el hecho de que las Tecnologías de la Información y Comunicación cada vez son parte esencial de las empresas, y aún no existe conciencia de los posibles atentados a su seguridad.

La información puede considerarse como uno de los activos[1] más importantes [**1**] que cualquier institución posee, ya que en base a ella se realizan diferentes actividades internas y externas. En tal virtud, deben tomar en consideración ciertos aspectos para garantizar confianza, orden, coordinación, credibilidad, entre otra. [**2**].

Existen vulnerabilidades presentes en todos los sistemas de la información [**1**] y en cada caso, tras un evento que comprometa a la información, la magnitud del impacto puede diferir por cada institución e incluso por cada departamento dentro de ellas. Sin embargo, aunque existan medidas que contrarresten los eventos que amenacen la seguridad de la información, no se puede determinar cuándo sucederán [**3**].

Las salvaguardas para mejorar la seguridad de la información ante eventos que puedan afectar a dicha información, serán importantes en todo momento. La manera para determinar las salvaguardas que se utilizarán, deben seguir ciertos procedimientos que permitan diferenciar qué elementos o qué procesos dentro de la organización, requieren mayor atención. [**4**] [**5**]

---

[1] Un activo es una cosa tangible o intangible que tiene valor para la organización. Ejemplos de activo son las máquinas, patentes, software, servicios, información, personas, imagen y reputación. [**6**]

Las maneras para obtener resultados cuantificables, estadísticos y referenciales que permitan entender la situación actual de la seguridad de la información de una institución variarán de acuerdo al punto de vista y decisión del analista a cargo y de la información disponible. El propósito general de determinar la situación actual será el mismo: identificar qué es lo hay, qué se dispone y qué hace falta para brindar seguridad a la información.

Por otro lado, las leyes y reglamentos vigentes en el Ecuador mencionan requerimientos que las entidades públicas deben cumplir en relación a la información y su seguridad. Existe en el Ecuador la Ley Orgánica de Transparencia y Acceso a la Información Pública [**4**], que plantea el manejo de la información en las entidades públicas. Estas entidades están comprometidas a manejar la información que adquieren con el tiempo, con medidas de seguridad que garanticen su autenticidad, que sean fiables y que sean de libre acceso para el estado ecuatoriano. No toda la información que las entidades públicas poseen puede ser expuesta, dado que existen esclarecimientos en dicha ley en que la información que está relacionada a la seguridad nacional es información clasificada, por lo tanto no puede ser expuesta al público en general.

Actualmente en el Ecuador también está vigente el Registro Oficial No. 88 [**5**] emitida por el gobierno de turno, el cual es un requisito que debe cumplirse en las instituciones públicas de la República del Ecuador. Esta resolución es una compilación de lo sugerido en la norma ISO/IEC2 27002:2005 [**6**], pero adaptada a ciertos requerimientos que se ha definido el gobierno. Abarca los 11 dominios principales de dicha norma y el propósito es establecer procedimientos de buenas prácticas para eventos en los que la información pueda verse comprometida.

Según dicho Registro, se tiene el siguiente detalle: “Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan,

[2] ISO/IEC: International Organization for Standarization / International Electrotechnical Comission

procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera", lo que indica la necesidad, importancia y obligación de las instituciones para el manejo adecuado de la seguridad de la información.

Otras referencias para comprender la importancia de tomar medidas de seguridad en la información y actividades relacionadas, está en los reportes y noticias que los mismos proveedores de seguridad recopilan anualmente. Por ejemplo, Kaspersky presentó un informe acerca de la seguridad en el 2013 [**7**], en base a información recopilada de uso y encuestas a sus usuarios. En la Figura 1.1 se muestran algunos resultados, y de ellos se puede deducir que varios de los ataques de ocurrencia interna son por mal manejo de la información de los usuarios legítimos, por la falta de capacitación adecuada a los empleados y fallos y vulnerabilidades en el software existente. Para el caso de ocurrencia de ataques de origen externo (Figura 1.2), se observa que la mayoría es debido a virus, spyware y programas maliciosos.

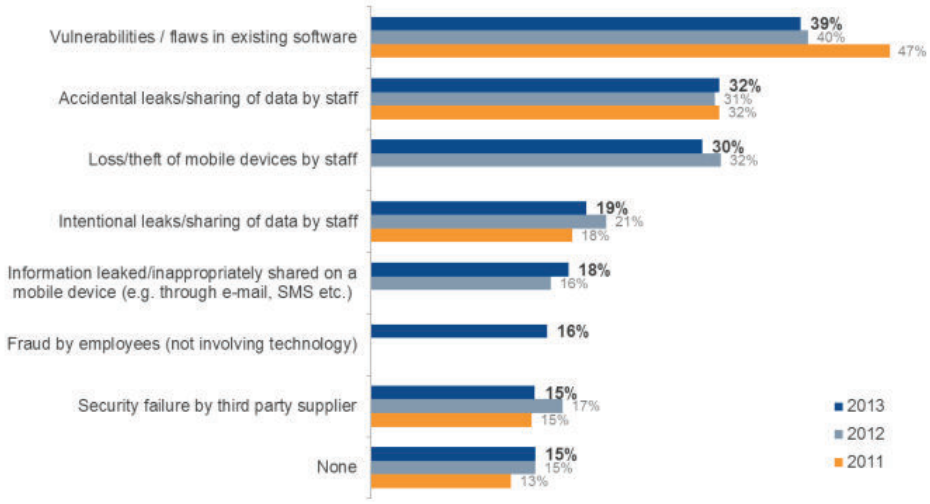

Figura 1.1. Amenazas internas de seguridad experimentadas en IT [**7**]

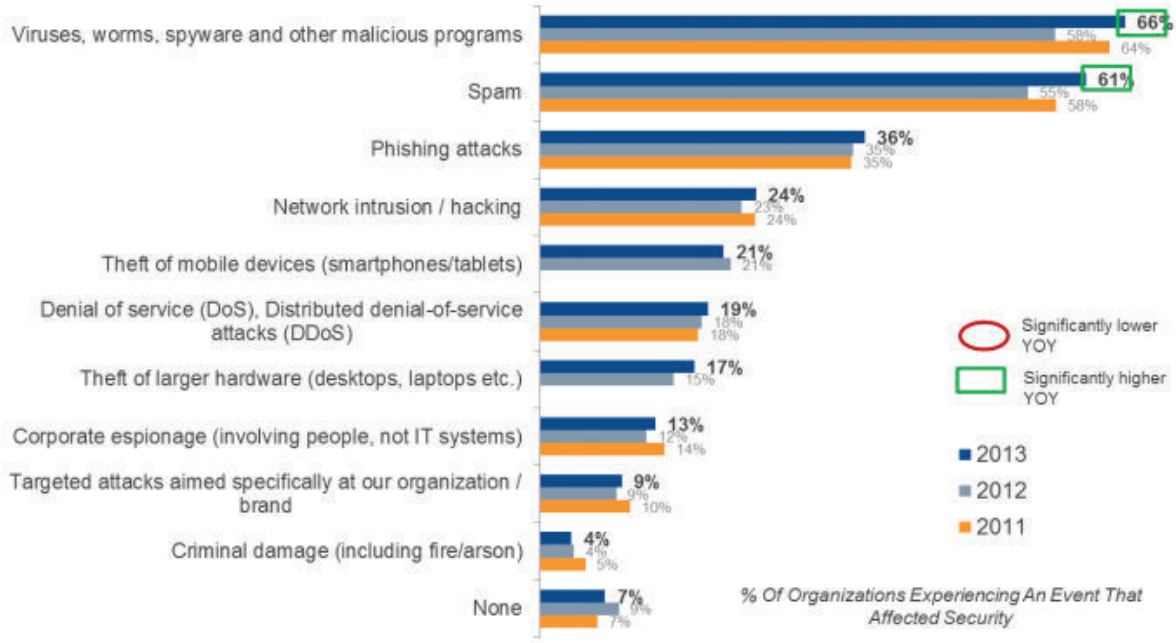

Figura 1.2. Amenazas externas de seguridad experimentadas en IT [7]

Las sugerencias que el reporte de Kaspersky presenta, son una muestra evidente de que los usuarios y más aún las instituciones, no dan la atención e importancia necesarias para prevenir o contrarrestar eventos perjudiciales para la información involucrada. Además, entre las conclusiones del informe se concuerda con el hecho de que una sola herramienta no podrá contrarrestar todos los atentados contra la seguridad de la información ya que en el manejo adecuado de la seguridad están involucrados aspectos tecnológicos, humanos, legales, éticos, etc.

Ante los antecedentes mencionados, es evidente que todas las organizaciones, entre ellas las empresas públicas, deben cumplir con requerimientos mínimos para el manejo adecuado de la información que se ajusten a las leyes, necesidades y presupuesto. Adicionalmente, se debe tener presente que la seguridad no solo depende de una herramienta tecnológica, sino de un conjunto de factores que deben ser considerados.

1.2 FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

1.2.1 INFORMACIÓN

La información es un conjunto de datos procesados que conforman un mensaje y que cambia el conocimiento del sujeto que recepta dicho mensaje.

Desde el punto de vista de la ciencia de la computación, la información es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno [**8**].

De lo anterior, se puede deducir que dentro de una empresa, la información procede de diferentes fuentes y puede encontrarse en diferentes soportes, como papel, medios digitales, e incluso puede formar parte del conocimiento de una persona. Además, otro de los aspectos importantes a considerar es el ciclo de vida de la información, ya que lo que hoy puede no ser importante para el negocio puede ser potencialmente crítica más adelante, y viceversa.

1.2.2 SEGURIDAD

La seguridad, de manera general, se refiere a un estado de ausencia de riesgo o la confianza en algo o en alguien. Para ello, se necesita evaluar, estudiar y gestionar los riesgos a los que se encuentra sometido una persona o un bien.

De acuerdo al ámbito al que esté orientado, la seguridad puede clasificarse en: seguridad física (sobre las personas), seguridad ambiental (sobre el ambiente), seguridad e higiene (en el ambiente laboral), seguridad informática (sobre la infraestructura de las TIC), seguridad de la información (sobre los activos de información de una organización), entre otros [**9**].

1.2.3 SEGURIDAD INFORMÁTICA

La seguridad informática tiene por objetivo proteger la infraestructura de las tecnologías de la información y comunicación, y la información contenida en ella; dicha infraestructura sirve de soporte tecnológico para el negocio. En la seguridad

informática se hace uso de protocolos, algoritmos y herramientas que permitan minimizar los riesgos de la infraestructura y de la información [**10**].

1.2.4 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información a diferencia de la seguridad informática, tiene un escenario de actuación más amplio que no solo involucra aspectos tecnológicos. La seguridad de la información tiene por objetivo la protección de los activos de información fundamentales para el éxito de cualquier organización. Dichos activos pueden estar soportados en distintos medios: información sobre hojas de papel (reportes, informes, planes de proyectos, etc.), información sobre discos duros locales o en la nube, información que forma parte del conocimiento de una persona pero que es sensible para la organización, etc.

La ISO/IEC 27001:2005 define a la seguridad de la información como: "la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad y no-repudio." [**11**] Por otra parte también se lo define como el conjunto de medidas preventivas y reactivas de las organizaciones para proteger y resguardar la información [**12**].

1.2.4.1 Objetivos de la Seguridad de la Información

1.2.4.1.1 Confidencialidad

Según la ISO/IEC 27001:2005 la confidencialidad es una característica de la información que asegura que ésta no se encuentra disponible o no ha sido divulgada a entidades no autorizadas. Además, se señala que por entidades se entiende a personas y procesos [**11**]. Para garantizar la confidencialidad de la información soportada por infraestructura de TICs, usualmente se usan técnicas de cifrado. Para información soportada por medios físicos, los mecanismos de control de acceso físicos (gavetas con llave, puertas con medios de autenticación biométricos, tarjetas, contraseñas, etc.) quizá sean la mejor opción.

1.2.4.1.2 Disponibilidad

Según la ISO/IEC 27001:2005 la disponibilidad es una característica de un activo que lo hace accesible y utilizable para cuando una entidad autorizada lo requiera. En el mismo estándar se menciona que por activo se entiende a la información, sistemas, computadoras y redes [**11**]. Para prevenir que la disponibilidad de un activo sea afectada se usan técnicas como respaldos y redundancia.

1.2.4.1.3 Integridad

La ISO/IEC 27001:2005 define a la integridad como una característica de la información que permite salvaguardarla de forma completa y exacta. Es decir no han existido modificaciones o cambios no autorizados [**11**]. Para prevenir que esta propiedad de la información se vea afectada se usan algoritmos criptográficos de firma digital para medios digitales, firmas (grafos manuscritos) para medios físicos. Los mecanismos de control de acceso físico también coadyuvan a garantizar la integridad de la información.

1.2.4.1.4 Autenticidad

La autenticidad prueba quién es el autor de algún documento y quién es su destinatario [**13**]. Es la capacidad de asegurar que el emisor de un mensaje es quien dice ser y no un tercero que intenta suplantarlo [**14**]. Técnicas como contraseñas, firmas, firmas digitales, tarjetas inteligentes y huellas dactilares pueden ser utilizadas para procurar brindar autenticidad.

1.2.4.1.5 No repudio

El no repudio es una característica de la información en donde los implicados en la transacción (emisor y receptor) no pueden negar el envío o recepción de un mensaje. Es decir, el no repudio tiene por objetivo proporcionar pruebas de la integridad y origen de los datos [**14**] [**15**]. Para prevenir que esta propiedad de la información se vea afectada se usan los certificados digitales y firmas.

1.2.4.2 Riesgo

Se podría definir al riesgo como la probabilidad de que un evento contra la seguridad de la información ocurra y el impacto negativo que éste causaría [**6**].

El riesgo, como unidad medible, se lo puede representar en función de la **probabilidad** de ocurrencia de un evento en el futuro y el **impacto** o las consecuencias que causaría dicho evento en caso de ocurrir.

$$R = f\,(P, I\,)$$

Dónde:

R es el riesgo de seguridad de la información.

P es la probabilidad de que un amenaza de seguridad explote vulnerabilidades en un activo de información, e;

I es el impacto que causaría una amenaza cuando se materialice.

La determinación de la probabilidad de ocurrencia depende de las condiciones actuales de la organización. Además, el historial de eventos ocurridos dentro de la organización y los reportes de seguridad locales e internacionales, son algunos insumos que pueden ser empleados para determinar la probabilidad de ocurrencia de un evento.

De la misma forma, el impacto se puede cuantificar por los daños totales o parciales sobre un bien, actividad, servicio o recuperación de estos como resultado de acciones con consecuencias negativas [**16**]. El impacto puede cuantificarse a través de escalas que se utilizarán como referencia para dar una valoración medible durante el proceso de análisis de riesgos.

Es importante mencionar la existencia de diversas alternativas que permiten establecer las tablas que contienen los valores medibles tanto de la probabilidad y el impacto. Dichas alternativas están definidas en varias metodologías que se describen en el punto 1.3.1 del presente proyecto.

1.2.4.3 Vulnerabilidad

Según la ISO/IEC 27002:2005 una vulnerabilidad es la debilidad de un activo o grupo de activos que puede ser explotada y consecuentemente materializar de una amenaza [**6**]. Las vulnerabilidades existentes dependen del tipo de activo, por ejemplo los sistemas operativos y paquetes de software pueden tener desbordamientos de buffer (buffer overflow) y condiciones de carrera (race conditions) no controladas; los servicios de red, pueden tener errores de configuración; los documentos físicos sensibles, pueden ser accedidas por personas no autorizadas, etc.

1.2.4.4 Amenaza

La ISO/IEC 27002:2005 define a la amenaza como un potencial evento que puede ocasionar un incidente no-deseado para la organización. Las amenazas están siempre presentes en una organización y pueden ser explotadas por debilidades existentes en los activos de la organización; consecuentemente, se deben tomar medidas que las contrarresten [**6**]. Se puede ver un resumen sobre la existencia de amenazas informáticas que se detectan a diario en la Figura 1.3

Figura 1.3. Estadísticas anuales de amenazas según Kaspersky [**17**]

Las amenazas se pueden clasificar según el tipo de afectación que causarían en la seguridad de la información, pudiendo ser de interrupción, interceptación, modificación o fabricación. Además, se pueden categorizar de acuerdo a la naturaleza de la amenaza, pudiendo ser accidentales o intencionales [**16**].

1.2.4.4.1 Amenazas de interrupción

Este tipo de amenaza podría evitar el acceso a la información. Para lograrlo pueden realizarse acciones como: destruir componentes físicos como el disco duro, boquear el acceso a datos denegando el acceso a una BDD, cortar o saturar los canales de comunicación, etc.

1.2.4.4.2 Amenazas de interceptación

Se presentan en un escenario en el que personas, equipos o programas no autorizados podrían acceder a un determinado recurso de la organización y captar información confidencial como datos y documentos sensibles o la identidad de personas, por mencionar algunas.

1.2.4.4.3 Amenazas de modificación

Existen en un escenario en el que ente personas, equipos o programas no autorizados no solamente podrían acceder a los activos de información, sino que además podrían hacer modificaciones sobre ellos. Por ejemplo, alterar el comportamiento de una aplicación instalada o modificar los mensajes enviados entre usuarios conectados.

1.2.4.4.4 Amenazas de fabricación

Son muy similares a las amenazas de modificación, con la diferencia de que en este caso se podría agregar información falsa en el conjunto de información veraz de la organización.

1.2.4.4.5 Amenazas accidentales

Son aquellas que podrían estar presentes de manera espontánea y se deben principalmente a factores externos. Entre las amenazas accidentales se podrían mencionar las siguientes: accidentes meteorológicos, incendios, inundaciones, fallos en equipos, fallos en redes, fallos en sistemas operativos o software, errores humanos, etc.

1.2.4.4.6 Amenazas intencionales

Son aquellas que pueden estar ahí por acción voluntaria humana. En esta categoría se incluye la introducción de software malicioso, intrusión informática, robo de documentos físicos, etc.

Es de suma importancia tener presente que tanto las amenazas accidentales como las intencionales pueden estar presentes en el exterior o en el interior de la organización.

1.2.4.5 Ataque

Un ataque lo constituyen una acción o conjunto de acciones que intentan explotar una vulnerabilidad para materializar una amenaza y causar un impacto negativo en la organización. Es decir, un ataque intenta destruir, divulgar, alterar, denegar, robar o acceder de forma no autorizada al activo de una organización.

De acuerdo al impacto causado a los activos atacados, los ataques se clasifican en: activos y pasivos [**16**] . Un ataque activo es un conjunto de acciones que alteran un activo o recurso, o que modifican la operación del sistema. Por su parte un ataque pasivo lo constituyen un conjunto de acciones que aprenden o hacen uso de un activo o recurso, pero no lo alteran.

1.2.5 ACTIVOS DE INFORMACIÓN [18]

Como ya se ha mencionado en un apartado anterior, la información procede de diferentes fuentes y puede encontrarse en diferentes soportes. En tal virtud los activos de información son aquellos elementos, tangibles o intangibles, que contienen o manipulan información y que tienen algún valor para la organización; como ejemplo se puede observar una clasificación de activos en la Figura 1.4

De una forma simplificada se puede clasificar a los activos de información en:

- Datos: Toda la data (en cualquier formato) que se recogen, generan, transmiten, gestionan y destruyen en la organización.
- Aplicaciones: Todo software que se utiliza para la gestión de la información.
- Personal: Todos aquellos individuos que tengan acceso de cualquier manera a los activos de información de la organización.
- Servicios: Función o utilidad que permite lograr un objetivo; pueden ser internos (aquellos que una parte de la organización suministra a otra) o externos (aquellos que la organización suministra a clientes y usuarios).
- Tecnología: Todos los equipos utilizados para gestionar la información.
- Instalaciones: Son los lugares donde se alojan los sistemas de información.
- Equipamiento auxiliar: Activos que dan soporte a los sistemas de información y que no son parte de los otros tipos de activo definidos (equipos de climatización, equipos de destrucción de datos, etc.)

Figura 1.4. Clasificación de Activos de Información [18]

1.3 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Según la ISO/IEC 27001:2005 un análisis de riesgos es un procedimiento sistemático que hace uso de información para identificar posibles fuentes de riesgo. El propósito de un análisis de riesgos es identificar las amenazas que pueden atentar contra los activos de información y que podrían causar un impacto negativo en la organización [**11**].

Como se mencionó en un apartado anterior, la estimación del riesgo implica la determinación de dos valores:

- La probabilidad de que una amenaza ocurra en el futuro y;
- El impacto que causaría en la organización, si una amenaza se materializa.

Una vez estimados los riesgos, se realizará una evaluación de riesgos. La evaluación de riesgos compara el riesgo estimado con un conjunto de criterios de riesgo definidor por la organización. La ISO 27005 sugiere niveles de tratamiento del riego [**20**]. Este procedimiento permite determinar cuán significativo es un riesgo para la organización y se podrá decidir qué tipo de tratamiento de riesgo se realiza:

- **Aceptar el riesgo:** También denominado “Retención”. Se acepta el riesgo con los controles existentes. Requiere monitoreo para tomar decisiones de cómo tratarlo en caso que el nivel de dicho riesgo se eleve.
- **Reducir el riesgo:** Se hace uso de controles para disminuir el riesgo a un nivel aceptable.
- **Evitar el riesgo:** Se puede retirar o modificar una actividad o conjunto de actividades con el fin de evitar tratar el riesgo.
- **Transferir el riesgo:** Un riesgo se transfiere a que sea tratado por una entidad externa. Podría implicar nuevos riesgos o modificación del riesgo inicial.

Finalmente, la organización puede adecuar las medidas de seguridad pertinentes, implementando medidas que permitan modificar el riesgo.

El análisis y evaluación de riesgos realizado puede ser válido para un momento fijo inmediatamente después de presentar los resultados. Se debería evaluar las condiciones para dar mejoras a las medidas iniciales [**19**].

1.3.1 METODOLOGÍAS PARA LA ESTIMACIÓN DEL RIESGO

La metodología para realizar la estimación de riesgo puede ser cualitativa, cuantitativa o una combinación de ellas. Entre las metodologías utilizadas para el cálculo del riesgo se encuentran en: MAGERIT [**22**], ISO/IEC 27005 [**20**], OCTAVE [**21**], NIST 800-30 [**22**], entre otros.

1.3.1.1 Metodología cualitativa

Suele ser la más utilizada para realizar el análisis de riesgo debido a que se puede realizar las estimaciones de forma dinámica e intuitiva, esto es debido a que el analista utiliza su punto de vista y experiencia para dar una valoración con base a los atributos de calificativos que están asociados a una escala. Utiliza las características de un activo para calificarlo. [**25**] [**26**]

1.3.1.2 Metodología cuantitativa

Es un proceso más complejo en el que se utilizan diferentes formas de medición y cálculo para esclarecer los datos obtenidos. Utiliza valores numéricos para la estimación de probabilidad; esta metodología permite obtener datos más precisos, sin embargo, por los amplios criterios para establecer criterios como los de pérdida o de probabilidad de ocurrencia, puede conllevar un mayor esfuerzo el desarrollar un análisis basado únicamente en valores numéricos. [**25**] [**27**] Esta metodología permite estimar haciendo uso de valores cuantificables, es decir, dar un valor numérico medible.

1.3.1.3 Metodología mixta

Este tipo de metodología combina procedimientos, sugerencias, tablas, etc., de varias referencias para establecer un método cualitativo y calificable que se puede relacionar con un valor numérico medible haciendo uso de escalas. Esta metodología permite recolectar, analizar y vincular datos cualitativos y cuantitativos en un mismo estudio o una serie de investigaciones para lograr responder a un planteamiento [**24**] [**29**].

El presente proyecto utiliza una valoración de activos cualitativa, la cual permite establecer valores fijos en las escalas de valoración para poder asignar un número de acuerdo a las características, posibilidades o costo en el análisis de un activo. Además, se ha tomado esta metodología debido a que la valoración permite ser asignada en un rango de estimación, permitiendo comparar e identificar los activos críticos para la entrega de servicios.

1.3.2 PROCESO BÁSICO PARA EL ANÁLISIS DE RIESGOS

El proceso para el Análisis de Riesgos seguirá el mismo ciclo que se muestra en la Figura 1.5, donde se empieza con un activo identificado al cual se le atribuye un valor.

A continuación se procede a determinar el nivel de afectación que un ataque podría provocar, considerando nivel de afectación y probabilidad de ocurrencia. De estos se aprecia si los controles existentes permiten disminuir la valoración que se hace sobre dichos aspectos.

Se asigna una valoración del impacto a partir del nivel de afectación de una vulnerabilidad y la valoración del activo.

Finalmente se realiza el cálculo del riesgo en base a los valores obtenidos en todo el proceso de identificación y valoración.

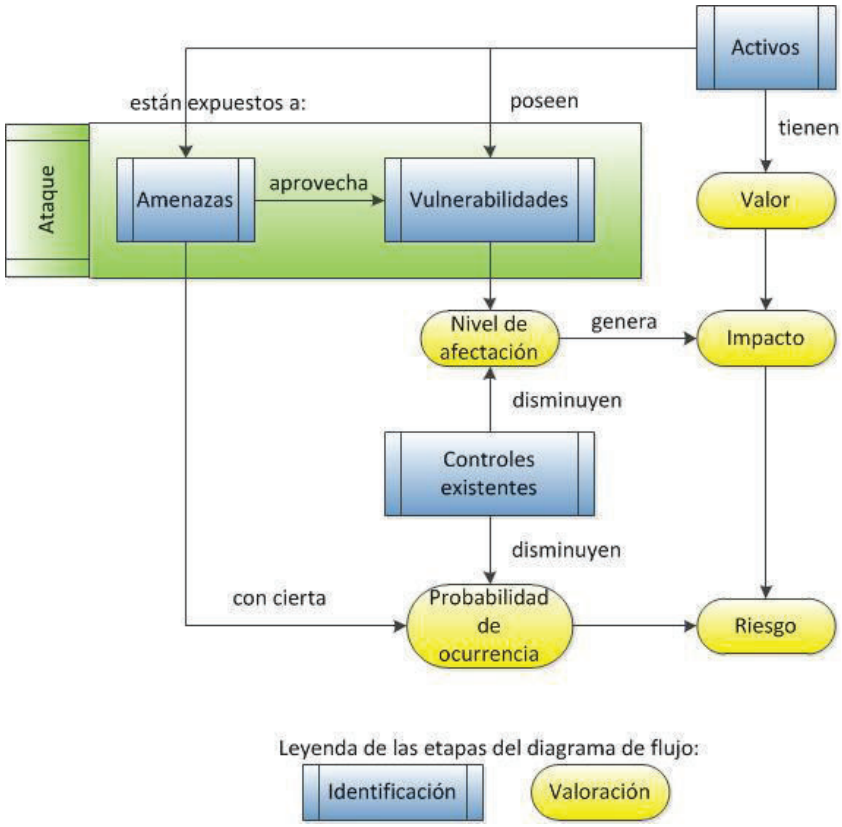

Figura 1.5. Diagrama del Análisis de Riesgos

1.4 NORMA ISO 27001:2005 [11]

La norma ISO 27001 define un conjunto de requerimientos que permiten diseñar, implementar, monitorear y mejorar un SGSI. Además, la norma es certificable y posee cuatro fases basadas en el ciclo de Deming para mejoramiento continuo.

Las fases que componen el ciclo de Deming son: Planificación, Implementación, Monitoreo y Mejoramiento. Son fases utilizadas de manera cíclica, lo que permite actuar y tomar medidas tras los eventos y evaluaciones realizadas a lo largo de un periodo de tiempo para que la empresa se encuentre preparada para contrarrestar las amenazas. El presente proyecto está enfocado únicamente en la fase de Planificación, debido al alcance del mismo.

1.4.1 TERMINOLOGÍA [11]

Los siguientes, adicionales a los definidos en las secciones anteriores, son algunos términos necesarios para comprender la norma y el presente documento:

- Evento de Seguridad de Información: Ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser de importancia para la seguridad.
- Incidente de Seguridad de la Información: Evento o eventos de seguridad de información, que son no deseados o inesperados y que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
- Sistema de Gestión de Seguridad de la Información SGSI: Esa parte del sistema gerencial general, y se basa en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- Riesgo Residual: El riesgo que queda después del tratamiento del riesgo.
- Aceptación de riesgo: Decisión de aceptar el riesgo.
- Valuación del riesgo: Proceso general de análisis de riesgo y evaluación del riesgo.
- Evaluación del riesgo: Proceso de comparar el riesgo estimado con el criterio de riesgo planteado para determinar la importancia del riesgo.
- Gestión del riesgo: Actividades coordinadas que se han definido para dirigir y controlar una organización con relación al riesgo.
- Tratamiento del riesgo: Proceso de tratamiento de la selección e implementación de las medidas definidas para modificar el riesgo.
- Enunciado de Aplicabilidad: Enunciado documentado con la descripción de los objetivos de control y los controles considerados relevantes y aplicables al SGSI de la organización.

1.4.2 MODELO PDCA

Se trata de una serie de procedimientos que permiten dar la atención a la seguridad de la información en base a un proceso que sugiere cuatro pasos, los mismos que permiten realizar mejoras continuamente.

Los pasos son: planificación, implementación, revisión, mejoramiento (en el inglés: Plan, Do, Check, Act); dichos pasos conforman el ciclo de Deming, el cual propone la mejora continua. Se puede observar el ciclo de Deming en la Figura 1.6

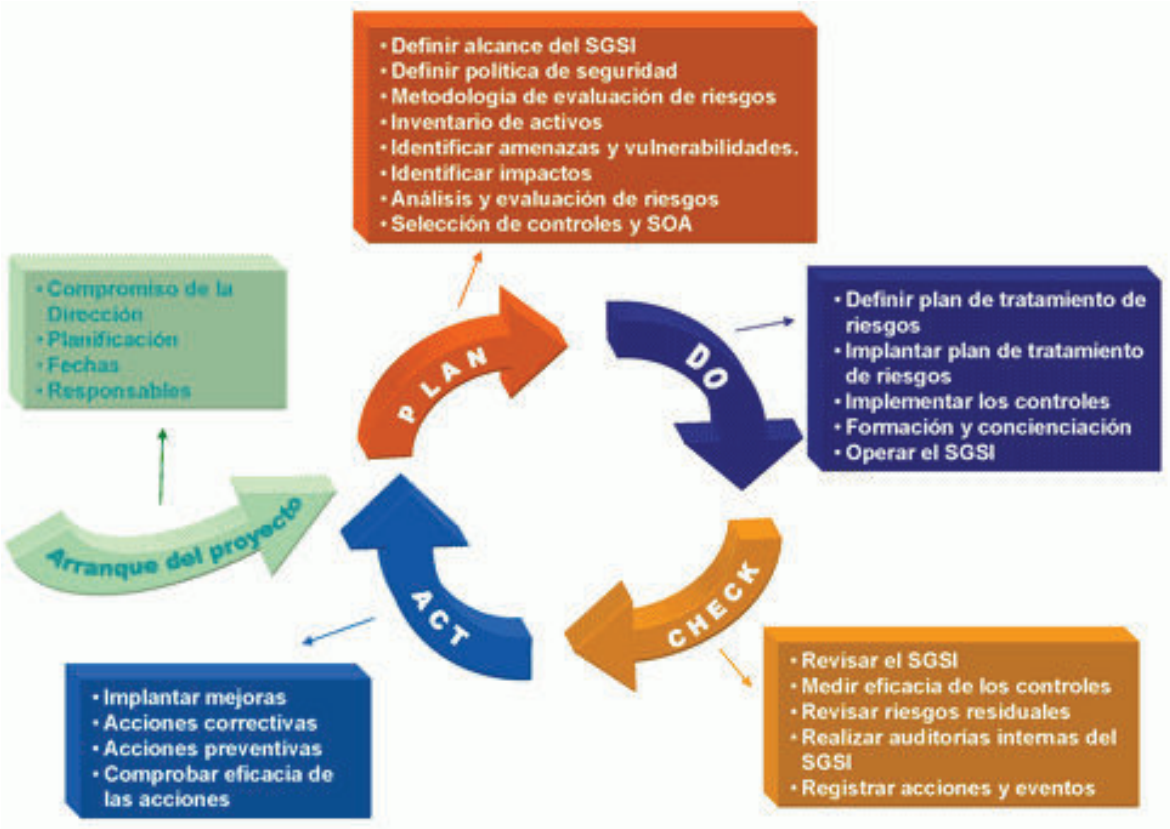

Figura 1.6. Ciclo de Deming [30]

Los detalles de las fases del SGSI bajo el modelo PDCA se describen en el punto 1.4.3 del presente documento.

El SGSI tiene en su definición una serie de procedimientos que tienen como objetivo cubrir el análisis de cada activo en la red. Cada actividad de los elementos que conforman la infraestructura de la red, ya sea físico o virtual, deberían ser registrados para detectar falencias y realizar sus correspondientes correctivos.

Los procedimientos actualizados a realizarse para contrarrestar futuros ataques similares a los ya superados, permitirán minimizar el tiempo de solución y el impacto. El análisis sobre la situación actual permitirá definir medidas a nivel de hardware, software y de nivel humano, para categorizar el ataque para poder ser resuelto.

1.4.3 FASES DE SGSI DE LA NORMA ISO 27001:2005 [11]

Existen cuatro etapas que permiten mantener la objetividad de mejoramiento continuo. Estas etapas se basan en el modelo PDCA y se detallan en las siguientes secciones.

1.4.3.1 Fase de planificación de un SGSI según la norma 27001:2005 (PLAN) [11]

Esta fase tiene como propósito diseñar el SGSI y definir los diferentes controles que serán necesarios como punto de partida para las fases siguientes.

La fase de planificación incluye las siguientes actividades que, preferiblemente, tienen que ser llevadas a cabo en orden cronológico:

i. Definir el alcance y los límites del SGSI incluyendo los detalles y justificación de cualquier exclusión.

ii. Definir una política del SGSI, que puede estar escrita en un documento y en la cual se establezca el criterio con el que se evaluará el riesgo junto con los detalles que aclaren a dicha política.
iii. Definir el enfoque de valuación del riesgo de la organización con dos objetivos claros que son: identificar una metodología de cálculo del riesgo y desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.
iv. Identificar los riesgos de los activos de información y sus posibles amenazas, las vulnerabilidades que podrían ser explotadas y materializar una amenaza y los impactos que pueden ocasionar.
v. Analizar y evaluar el riesgo con cálculos de impacto comercial sobre la organización y de la probabilidad realista de que ocurra dicha falla considerando niveles de aceptación.
vi. Identificar y evaluar las opciones para el tratamiento de los riesgos en los que se pueden realizar las acciones de: aplicar controles, aceptar los riesgos, evitar los riesgos o transferir los riesgos a otras áreas o entidades.
vii. Seleccionar objetivos de control y controles para el tratamiento de riesgos que pueden ser basados en los puntos que indica la norma ISO 27002:2005.
viii. Aprobar por medio de la gerencia sobre los riesgos residuales.
ix. La gerencia deberá autorizar la implementación y operación del SGSI.
x. Preparar un enunciado de aplicabilidad incluyendo los objetivos de control y controles actuales y los que se implementarán con sus razones para su selección, así como también aquellos objetivos y controles que no serán considerados, igualmente con las razones que justifiquen su exclusión.

Los pasos que componen la fase de planificación, se muestran en la Figura 1.7.

Figura 1.7. Actividades de la fase Planificación [30]

1.4.3.2 Fase de implementación (DO) [11]

Esta fase tiene como objetivo la implantación y operación de los controles.

La fase de implementación involucra las siguientes tareas:

i. Formular un plan de tratamiento de riesgo que permita manejar los riesgos de la seguridad de la información.
ii. Implementar el plan de tratamiento de riesgo para poder lograr los objeticos de control identificados.
iii. Implementar los controles seleccionados en la fase de Planificación para satisfacer los objetivos de control.

iv. Definir los métodos para la medida de los controles, con el objetivo de lograr el control planeado.
v. Implementar los programas de capacitación y conocimiento para el personal.
vi. Manejar las operaciones y recursos del SGSI.
vii. Implementar los procedimientos y controles para poder detectar os incidentes de seguridad.

1.4.3.3 Fase de monitoreo (CHECK) [11]

Esta fase tiene por objetivo obtener la información generada y registrarla para poder analizar y evaluar el desempeño del SGSI.

La fase Monitoreo está constituido de los siguientes pasos:

i. Ejecutar los procedimientos de monitoreo y revisión para detectar las falencias en los procedimientos y determinar los cambios correctivos que permitan solventar los problemas relacionados a la Seguridad de la Información.
ii. Realizar revisiones regulares de la efectividad del SGSI, tomando toda la información que le pueda ser útil para realizar los cambios correctivos.
iii. Revisar las evaluaciones de riesgo a intervalos planeados.
iv. Realizar auditorías internas a intervalos planeados.
v. Realizar una revisión gerencial del SGSI para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.
vi. Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
vii. Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

1.4.3.4 Fase de mejoramiento (ACT) [11]

Esta fase tiene como objetivo tomar medidas en base a los resultados obtenidos en la fase de monitoreo para poder corregir o añadir los controles que sean necesarios que permitan mejorar el desempeño del SGSI.

La fase de mejoramiento incluye los siguientes pasos:

i. Implementar las mejoras identificadas en el SGSI.
ii. Tomar acciones correctivas y preventivas acorde a los resultados y evaluaciones obtenidas en la fase de monitoreo.
iii. Comunicar los resultados y acciones a todos los involucrados para que puedan tomar las medidas necesarias o actualizar la información sobre los procedimientos que deben seguir.
iv. Verificar que las mejoras logren los objetivos señalados.

1.5 NORMA ISO 27002:2005 [6]

La norma ISO 27002:2005 define un conjunto de recomendaciones con las mejores prácticas para la gestión de la seguridad de la información de una organización. A diferencia de la norma ISO 27001, esta no es certificable. La norma posee 11 dominios de control, con sus respectivos objetivos de control, los mismos que se describen más adelante.

1.5.1 TERMINOLOGÍA [6]

Varios términos y definiciones de esta norma fueron mencionados en el punto 1.4.1 del presente proyecto, por lo que se agregarán aquellos que están indicados en la ISO 27002:2005 y que no constan en la terminología de la ISO 27001.

- Lineamiento: Una descripción que explica qué se debiera hacer y cómo, para conseguir los objetivos creados en las políticas.

- Medios de procesamiento de la información: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o el lugar físico que los alojan.
- Política: Intención y dirección general, definida y aprobada, formalmente por la gerencia.
- Tercera persona: Esa persona y organismo que es reconocido como ajeno e independiente de las partes involucradas, con relación al ítem en cuestión.

1.5.2 DOMINIOS DE LA NORMA ISO 27002:2005 [6]

La norma ISO 27002:2005 define 11 dominios de actuación, 39 objetivos de control y 133 controles que podrían ser seleccionados en la gestión de un SGSI. Aunque la implementación de todos los controles no es obligatoria, la organización debe argumentar de manera sólida la no implementación de alguna de ellas. La Tabla muestra los 11 dominios y la cantidad de objetivos de control y controles de cada dominio. La lista completa que incluye los 11 dominios, con sus respectivos objetivos de control y, de éstos últimos, los controles se encuentran en el Anexo D.

Cláusulas		Objetivos de Control	Controles
1	Política de Seguridad	1	2
2	Aspectos Organizativos de la Seguridad de la Información	2	11
3	Gestión de activos	2	5
4	Seguridad Ligada a los Recursos Humanos	3	9
5	Seguridad Física y del Entorno	2	13
6	Gestión de Comunicaciones y Operaciones	10	32
7	Control de Acceso	7	25
8	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	6	16
9	Gestión de Incidentes en la Seguridad de la Información	2	5
10	Gestión de Continuidad del Negocio	1	5
11	Cumplimiento	3	10

Tabla 1.1. Dominios de la norma ISO 27002:2005

A continuación se describirán brevemente los dominios que conforman a dicha norma:

1.5.2.1 Política de Seguridad de la Información

Este dominio tiene como objetivo presentar los compromisos de la institución y sus integrantes sobre cómo llevar los procedimientos internos y el uso de recursos con el planteamiento de políticas internas.

1.5.2.2 Organización de la Seguridad de la Información

Este dominio es el que permitirá establecer un orden jerárquico de los actores involucrados en el manejo de seguridad interno y cómo estarán organizados.

1.5.2.3 Gestión de Activos

Permite esclarecer los activos más importantes y sensibles que maneja la institución. Se establecen recomendaciones que serán tomadas en cuenta para su correcta administración.

1.5.2.4 Procesos de Seguridad de Recursos Humanos

En este punto se establecerán las responsabilidades otorgadas al recurso humano o al personal de la institución. También permite establecer pasos a seguir para minimizar el riesgo de un incidente intencional o no, provocado por algún miembro de la institución.

1.5.2.5 Procesos de Seguridad Física y del Entorno

Este punto precisa tomar medidas sobre los equipos, la infraestructura y arquitectura de ser necesario, sobre las áreas donde se encuentran los activos críticos.

1.5.2.6 Procesos de Gestión de Operaciones

Abarca los procedimientos operacionales concernientes a los servicios, para que sean ejecutados adecuadamente. Estos procedimientos pueden tomarse en base a las sugerencias que las normas ISO/IEC sugieren o bien basarse en cumplir con los requerimientos legales utilizando otras metodologías.

1.5.2.7 Control de Acceso

Cubre la autenticidad y autorización de acceso a espacios físicos, equipos y administración de servicios o aplicaciones, únicamente a personas que tengan en sus responsabilidades el uso de los mencionados recursos de manera directa.

1.5.2.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Este punto tiene como objetivo detallar las medidas necesarias para asegurar la seguridad de los sistemas informáticos que manejan los usuarios de la institución.

1.5.2.9 Procesos de Gestión de Incidentes de Seguridad de la Información

Se redactará la guía que permitirá a los usuarios solventar los incidentes que involucren a los activos de la información de forma rápida y ordenada.

1.5.2.10 Gestión de la Continuidad del Negocio

Este punto abarca un conjunto de recomendaciones que se espera sean aplicadas en el caso que un incidente comprometa a algún servicio que la institución brinda a sus clientes. El propósito de las recomendaciones es reducir el impacto del incidente, minimizar e impedir que se suspenda la actividad del servicio involucrado.

1.5.2.11 Procesos de Cumplimiento

Contiene los detalles que deben cumplir con las obligaciones reglamentarias, contractuales y legales que comprometen a la institución. Se espera que al cumplir con estos requerimientos se eviten infracciones o llamadas de atención por las

entidades correspondientes de revisión y regulación, así como también de que la institución esté preparada para auditorías.

1.6 MOTIVACIÓN DEL PROYECTO

La Dirección de Gestión Tecnológica debe cumplir ciertos requerimientos en el manejo de la seguridad de la información. Estos requerimientos son los estipulados bajo ley como el Registro Oficial No. 88 [**5**] y la Ley Orgánica de Transparencia y Acceso a la Información Pública [**4**]. Además, como institución pública, debería considerar su estado actual para mejorar sus procedimientos vigentes y corregir sus falencias en el ámbito de Seguridad de la Información.

Las políticas internas debería abarcar, al menos, lo mencionado en el Registro Oficial No. 88 [**5**], debido a que en éste existe un amplio número de controles que sugiere deben ser atendidos para adecuar las medidas de Seguridad de la Información.

La Dirección de Gestión Tecnológica requiere tomar medidas que permitan favorecer la seguridad de la información. Para lograr este objetivo es necesario identificar los activos, y, tras darles una valoración, realizar el análisis y evaluación de riesgos para entender la situación actual de sus activos y responsabilidades. Tras conocer las debilidades presentes es posible proponer una serie de políticas que pueden ser consideradas como referentes para una posterior y necesaria aplicación en la Dirección.

En tal virtud, el propósito del presente proyecto de titulación es establecer las mejores prácticas en el manejo de la seguridad de información de la Dirección de Gestión Tecnológica del Ministerio del Deporte, tomando como base los once dominios definidos en la norma ISO/IEC 27002:2005.

CAPÍTULO 2. ANÁLISIS DE LA SITUACIÓN ACTUAL

En el presente capítulo inicia con una breve descripción de la Dirección de Gestión Tecnológica del Ministerio del Deporte, Quito. Dado que la mayoría de procesos de la Dirección está soportada principalmente por una infraestructura de TIC, se presenta un breve resumen de la infraestructura y servicios de red desplegados, así como también de los principales procesos llevados a cabo. Posteriormente se presenta el resultado de la evaluación de la situación actual de la seguridad de la información de la Dirección tomando como base los dominios definidos en norma ISO/IEC 27002:2005. Finalmente, se muestran los resultados del análisis y evaluación de riesgos respectivo.

2.1 VALORES DEL MINISTERIO Y DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA

2.1.1 VISIÓN DEL MINISTERIO [31]

“Es una Institución líder en el campo de la cultura física y el movimiento; reguladora del deporte, la educación física y la recreación; comprometida con el desarrollo integral del ser humano, que cuente con una administración transparente que demuestre eficiencia y eficacia en las acciones.“

2.1.2 MISIÓN DEL MINISTERIO [31]

“El Ministerio es el organismo rector de la Actividad Física y el Deporte que define las políticas, los objetivos y las estrategias del sector, como generador del buen vivir.”

2.1.3 MISIÓN DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA [31]

“Ejecutar proyectos de tecnologías de la información y comunicación estratégicos para la aplicación de políticas públicas y mejora de la gestión institucional, así como el soporte tecnológico institucional.”

2.2 INFRAESTRUCTURA Y SERVICIOS DE RED

La red del Data Center que forma parte de la Dirección tiene varios equipos que conforman su infraestructura. En la Tabla 2.1 se listan los equipos que posee y en la Figura 2.1 se observa la topología de la red.

La topología indicada en la Figura 2.1 es referencial, debido a que, a la fecha, no disponen de un diagrama con la topología interna. El resultado que se observa es en base a la asignación de los puntos de red a los usuarios (mostrados en los diagramas de distribución) y a una visita in situ a la infraestructura del Data Center de la Dirección.

Tipo	Hostname	Marca	Modelo
Switch	CORMINDEP001	HP	A5500
	ADMMINDEP-01	Cisco	Small business SG 200-08P
	ADMMINDEP-02	Cisco	Small business SG 200-08P
	ADMMINDEP-03	3COM	3CVL5F26PWRH
	ACCMINDEP001	3COM	3CVL5F26PWRH
	ACCMINDEP002	3COM	3CVL5F26PWRH
	ACCMINDEP003	3COM	3CVL5F26PWRH
	ACCMINDEP004	3COM	3CVL5F26PWRH
	ACCMINDEP005	3COM	3CVL5F26PWRH
	ACCMINDEP006	3COM	3CVL5F26PWRH
	ACCMINDEP007	3COM	3CVL5F26PWRH
	ACCMINDEP008	3COM	3CVL5F26PWRH

Tabla 2.1. Equipos de red de la Dirección

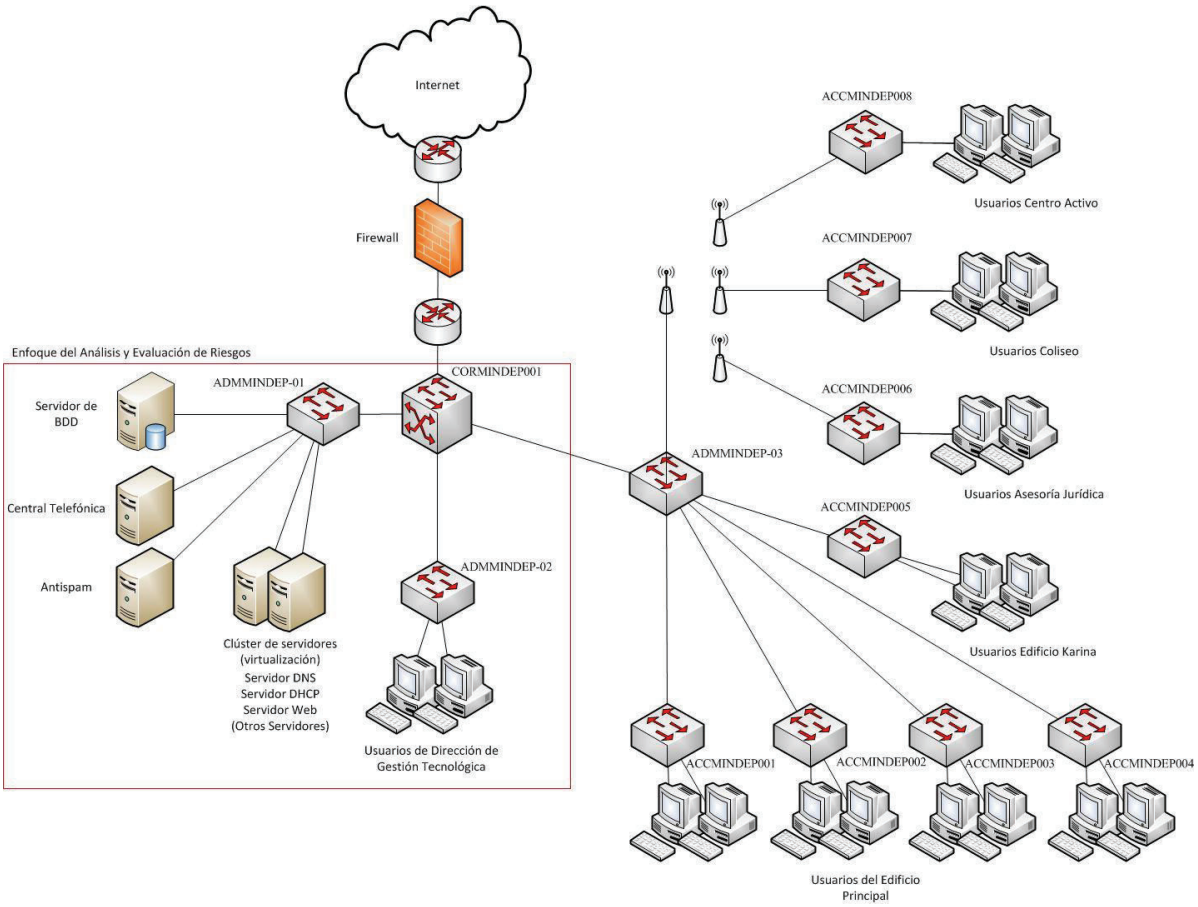

Figura 2.1. Topología de la red de la Dirección[3]

Los diagramas adicionales para comprender el estado actual de la Dirección y se pueden ver en el Anexo A.

2.2.1 EQUIPOS Y SUS CARACTERÍSTICAS TÉCNICAS

La Dirección de Gestión Tecnológica permitió el ingreso para la revisión del estado físico de los equipos, su distribución, equipamiento y medidas de seguridad. También permitieron el diálogo con el personal de dicha Dirección para entender y profundizar sobre el estado actual. La información detallada sobre los equipos no fue

[3] Lo que se encuentra dentro del rectángulo rojo en la Figura 2.1 es en lo que se enfoca el presente proyecto.

proporcionada en su totalidad por motivos de confidencialidad en la entrega de información de la institución [**30**] [**33**] y para poder estar de acuerdo sobre el procedimiento que se seguiría para la elaboración del presente proyecto, el Jefe del Área de Infraestructura sugirió nombrar de forma genérica a los equipos y servicios utilizados en el análisis que no fueron detallados en la recopilación información del estado actual por motivos de confidencialidad de la institución.

Debido a lo mencionado en el párrafo anterior, los equipos de la Dirección[4] están limitados para los fines de este proyecto según la Tabla 2.1 de Infraestructura de la Red y lo mencionado en las Tablas de Valoración de Activos en el punto 2.3.3 del presente proyecto.

2.2.2 USUARIOS

En la Dirección existen 11 usuarios, de los cuales forman parte un Director, 9 integrantes y una secretaria. La Tabla 2.2 muestra la lista de los integrantes asignados en la Dirección.

Área o Cargo	Integrantes
Jefe de Dirección	Director
Unidad de Ciencia y Tecnología	Coordinador y 1 colaborador
Desarrollo Tecnológico	Coordinador y 2 colaboradores
Infraestructura, Servicios y Soporte	Coordinador y 3 colaboradores
Secretaria	Secretaria

Tabla 2.2. Integrantes en la Dirección

El número de usuarios registrados en la infraestructura del Ministerio[5] es de 634 usuarios estimados, según el registro del área de Infraestructura, Servicios y Soporte. Dicha cantidad de usuarios es en realidad una estimación debido a que no se ha realizado una actualización por liberación de usuarios dado que es una función de Recursos Humanos el informar los empleados que ya no trabajan en la institución.

---

[4] Se referirá como “la Dirección” para indicar que se trata de la Dirección de Gestión Tecnológica
[5] Se referirá como “el Ministerio” para indicar que se trata del Ministerio del Deporte - Quito

Los clientes se consideran a todo el personal de la institución que hacen uso de los servicios que provienen de y que está a cargo la Dirección.

Para entender la relación de funciones, se puede observar un breve resumen del organigrama de la Dirección de Gestión Tecnológica se puede observar en la Figura 2.2

Figura 2.2. Organigrama de la Dirección de Gestión Tecnológica [34]

Las Áreas que conforman la Dirección tienen responsabilidades designadas para cumplir con las funciones que la Dirección está a cargo. A continuación se hace una breve mención de las actividades más destacables que está a cargo cada Área.

- ***Área de Infraestructura, Servicios y Soporte:***

Ésta Área se encarga de las actividades de administración y gestión de usuarios. Define los términos de contratación de bienes o servicios TIC. Se encarga de dar el soporte y capacitación a los clientes que hacen uso de los servicios que provienen de la Dirección.

- ***Área de Desarrollo:***

Ésta Área se encarga de los estándares para documentación del ciclo de vida de: los sistemas informáticos, gestión / entrega de servicios y seguridad de la información e infraestructura.

- ***Área de Ciencia y Tecnología:***

Ésta Área se encarga de la realización de pruebas de las aplicaciones que se esperan implementar con las validaciones correspondientes antes y durante la ejecución de las mismas. Están a cargo de los planes de capacitación tecnológica.

La elaboración de informes (de todo ámbito que corresponde a las funciones de la Dirección) y buscar soluciones relacionadas a las actividades que le compete a la Dirección son actividades que podrían ser realizadas en conjunto entre las Áreas.

Para una revisión más completa de las responsabilidades de cada Área, se puede observar en el Anexo F.

2.2.3 DEPARTAMENTOS

El Ministerio del Deporte – Quito, posee varias direcciones en su infraestructura que hacen uso de los servicios que provienen de la Dirección de Gestión Tecnológica.

Las direcciones que conforman al Ministerio y que reciben los servicios de red se pueden ver en la Tabla 2.3.

Direcciones del Ministerio del Deporte		
Edificio	Piso	Dirección
Edificio Central	Primer piso	Infraestructura deportiva
		Auditoria interna
		Recreación
		Financiero
		Tesorería
		Secretaria general
		Asuntos deportivos
		Antidoping
		Servicios institucionales
		Seguimiento y control
		Subsecretaría metodológica
		Talento humano
		Activos fijos
		Medicina deportiva
	Segundo Piso	Asesores
		Comunicación social
		Educación física
		Deportes
		Viceministro
		Deporte Adaptado
		Tecnológico
		Planificación
		Despacho
Coliseo		Conductores
		Archivo Financiero
Área de Piscina		Asuntos Legales
		Archivo de Secretaria General
		Centro activo #1
Edificio Karina	Primera Planta	Sostenibilidad y Relaciones Internacionales
		Subsecretaria Técnica de Apoyo
		Investigación Deportiva
		Capacitación
		Liquidadores Financieros
	Segunda Planta	Procesos

Tabla 2.3. Direcciones y departamentos que conforman el Ministerio del Deporte

2.2.4 SERVICIOS DE RED

La Dirección provee los servicios de red al Ministerio[6]. Estos servicios dados, se indican a continuación con una breve descripción de los mismos.

2.2.4.1 Servidor Proxy

El servidor proxy consiste en un servicio que actúa como un intermediario para receptar las peticiones de conexión de red que un cliente solicita, para que proceda a realizar una serie de tareas que permitan filtrar o establecer el tráfico para alcanzar al servidor destino. Los usuarios del Ministerio, tienen ciertas restricciones en el acceso a determinadas páginas web, por lo que se requiere autorización del acceso a determinados servicios de páginas web como videos o música.

2.2.4.2 Acceso a la Internet

Es el establecimiento de conexión con la red de redes. La forma en la que se logra esta conexión es por medio de un servidor, que establece las reglas de acceso en un dominio otorgado por un ISP (Internet Service Provider). Las medidas y condiciones en el acceso, como son velocidad de conexión y ancho de banda determinado para cada usuario, se pueden administrar en la Dirección.

2.2.4.3 Base de Datos

La base de datos es una compilación de información que está definida con diversos parámetros para clasificar datos que componen o describen a dicha información. A nivel de servidor, la base de datos se puede describir como un medio que almacena información continuamente de manera ordenada y siguiendo los parámetros con los que esté configurada, permitiendo realizar consultas, actualizaciones o correcciones en el caso que sea necesario. La información almacenada en la base de datos,

---

[6] Hay que aclarar que los usuarios, servicios y análisis de Infraestructura está orientado únicamente a la Dirección de Gestión Tecnológica del Ministerio del Deporte – Quito ubicado en la dirección: Gaspar de Villarroel E10-122 y 6 de Diciembre

proviene de las aplicaciones y administración que el Ministerio posee. Entre esta información se puede mencionar a la proveniente de los procesos de tramitación, fiscalización, registro de eventos en la red o la actualización de la información del nuevo personal, entre otros.

2.2.4.4 Servidor de Correo Electrónico

El servidor de correo provee el servicio a los usuarios para recibir y enviar correos. Cada usuario registrado en el Ministerio tiene su propia cuenta de correo. Los procedimientos de uso y condiciones para manejo de contraseñas son gestionadas por la Dirección.

2.2.4.5 Antivirus

El antivirus analiza las actividades o procesos, archivos y conexiones web, así como también la posible ejecución de programas o hilos de programas sospechosos que pueden estropear el funcionamiento de los equipos o que atenten contra la información sensible de la Dirección. En la Dirección se usa un antivirus sobre los servidores y clúster de servidores que operan en su centro de datos. También se brinda el soporte de instalación, configuración y actualización de los equipos de los usuarios.

2.2.4.6 Servidor DNS

El servidor DNS (Domain Name Server) permite asignar una dirección IP dentro de un dominio a los equipos que forman parte de la institución. Este servicio llega a todas las dependencias o demás Direcciones dentro del Ministerio, para que cada usuario disponga del servicio DNS.

2.2.4.7 Directorio Activo

El directorio activo es un servicio donde usuarios o grupos de usuarios tienen inspeccionado el inicio de sesión al acceder a la red con una serie de políticas utilizadas para administrar el acceso y permisos. Para el caso de la Dirección, se

utiliza Active Directory. Este servicio está administrado para todos los usuarios que conforman el Ministerio, por supuesto con diferentes privilegios según sea el caso.

2.2.4.8 Servidor Web

El servidor web permite dar acceso a una página propia de la institución en la cual se pueden tener interacciones de acuerdo al alcance que dicha página dispone. Este servidor permite la generación de solicitudes, preguntas y peticiones para áreas específicas del Ministerio, las cuales permiten atender a los clientes o usuarios externos. También permite el acceso a la información que está disponible para conocimiento público y la imagen de la institución para entender su propósito y forma de trabajo.

2.2.4.9 Servidor de Archivos

El servidor de archivos permite almacenar archivos digitales con información relevante y catalogada de acuerdo a parámetros que lo clasifiquen. En el Ministerio, el servidor de archivos recopila la información generada por los diferentes usuarios y está indexada de acuerdo a la Dirección que generó el archivo.

2.2.4.10 Servidor de Aplicaciones

El servidor de aplicaciones de la Dirección provee accesos a aplicaciones que sirven para la comunicación entre usuarios, validación de información, creación de archivos, entre otros.

2.2.4.11 Servicio DHCP

El servicio DHCP permite asignar una dirección dentro de un dominio de una red a un equipo o también llamado host de manera dinámica. En el Ministerio, cada usuario recibe una dirección IP propia que es administrada por la Dirección. Los usuarios de equipos de acceso inalámbrico también tienen esta posibilidad siempre que el usuario posea la contraseña de acceso a la red inalámbrica del Ministerio.

2.2.4.12 Antispam

Se trata de un servicio que limita el acceso de correo no deseado o que se cree que tiene contenido peligroso o sospechoso. En la Dirección el antispam realiza las funcionalidades para filtrar el tipo de correo recibido no-deseado y evitar que llegue a los usuarios en el Ministerio.

2.2.4.13 Clúster de Servidores

El clúster de servidores es una compilación de varios equipos que trabajan como si fueran uno solo. Para el caso de la Dirección, posee dos equipos, los cuales tienen instalados los diferentes servicios que provee al Ministerio.

2.2.4.14 Virtualización

Se trata del uso de equipos en los que existe un sistema operativo primario en el que se crea una partición virtual de disco duro en el que corre otro sistema operativo como secundario. Se utiliza para crear la redundancia virtual de algunos servicios de red que provee la Dirección al Ministerio.

2.2.4.15 Firewall

El Firewall cumple las funciones de filtrar la información que van desde y hacia la Internet con la red interna de una institución en base a políticas que definen y limitan el tipo de información emitida o recibida. La Dirección posee un firewall como mecanismo de defensa perimetral..

2.3 PROCESOS A CARGO

La Dirección de Gestión Tecnológica tiene funciones y procesos asignados dentro de la institución como parte de sus responsabilidades y obligaciones. Dichos procesos están relacionados a la entrega de servicios en la intranet, manejo y administración de las TIC, y otras responsabilidades que están de acuerdo a sus actividades [**29**]. Los procesos a cargo son los siguientes:

a) **Planeación estratégica y operativa de las TIC:** relacionada con las actividades que plantean estudios y proyectos de las TIC.
b) **Dirección, control y coordinación de proyectos TIC y talento humano:** actividades relacionadas con asesorías / consultorías nacionales o internacionales.
c) **Implantación y control de políticas:** establecimiento, estudio y difusión interna de política de seguridad.
d) **Soporte Técnico y Asesoramiento en TIC:** actividades con los equipos de la institución que requieren acceso o asesoría a los servicios de la intranet.
e) **Construcción de Aplicaciones para automatización de procesos:** estudio, prueba y validación de aplicaciones que permitan automatización de procesos que se consideren necesaria su implementación.
f) **Programas de capacitación de uso de herramientas / servicios TIC:** estrategias y asignación de personal que estará a cargo para capacitación de herramientas y servicios TIC.
g) **Proyectos de interoperabilidad gubernamental:** actividades que conllevan a la comunicación y envío validados de información entre las entidades públicas.
h) **Análisis del Estado Actual, Infraestructura y Servicios:** conocimiento, estudio, resultados estadísticos y propuestas para contrarrestar falencias detectadas.
i) **Cumplimiento de disposiciones gubernamentales y que la institución requiere:** actividades que se enfocan en el cumplimiento de la ley y en las necesidades que tiene la institución que están en el ámbito de las responsabilidades de la Dirección.
j) **Medición de desempeño de procesos:** métodos de medición, valores cuantificables y datos estadísticos del desempeño de procesos.
k) **Elaboración de informes:** desarrollo detallado de: actividades relevantes a las funciones de la Dirección, propuestas, resultados de análisis, entre otros.

l) **Aseguramiento de condiciones y recursos para el funcionamiento de la Dirección:** actividades que velan por el correcto desempeño de los servicios en conjunto con los recursos que son necesarios lograrlo.

m) **Participar en contratación, pruebas y recepción de sistemas adquiridos por terceros:** integración del personal de la Dirección en actividades que requieren su criterio, punto de vista y su aprobación.

n) **Actualización y soluciones tecnológicas para las TIC de acuerdo a las necesidades que se presenten en futuro:** actividades que requieren satisfacer las necesidades, resolver problemas y actualización de las TIC.

o) **Cumplir funciones y responsabilidades designadas que concuerden con sus actividades:** cumplir las actividades que la Dirección tiene asignadas en la institución.

Los procesos mencionados son actividades asignadas a los integrantes de la Dirección de Gestión Tecnológica.

La forma en la que operan las actividades en la Dirección de forma simplificada se puede observar en la Figura 2.3

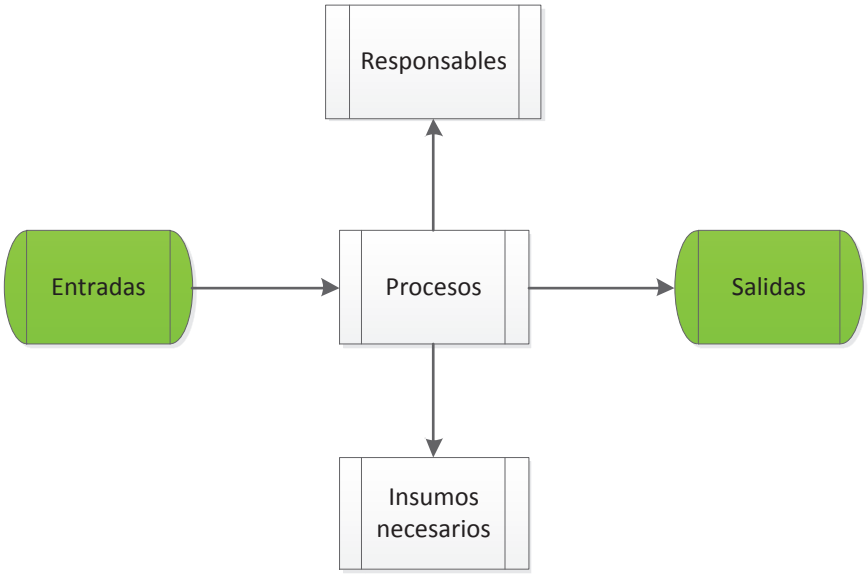

Figura 2.3. Actividades en los procesos

En las “Entradas” se encuentran los requerimientos o motivación para realizar un proceso. Tales requerimientos pueden ser: la ejecución de un incidente, objetivos de proyectos, aplicaciones o servicios requeridos, leyes vigentes que requieren ser acatadas, responsabilidades u obligaciones en el contrato de trabajo, entre otros.

Los “Procesos”, como se menciona al inicio de esta sección, son actividades o responsabilidades asignadas que en el caso de la Dirección de Gestión Tecnológica ya se las han identificado.

Los “Responsables” son individuos identificados que están comprometidos a realizar los procesos mencionados.

Los “Insumos Necesarios” son los activos necesarios para poder realizar los procesos. Comúnmente los procesos requieren más de un activo para ser ejecutados, y de igual manera un activo puede ser utilizado en más de un proceso.

Las “Salidas” son los resultados obtenidos o entregables tras la finalización de un proceso. Dichas salidas suelen ser: informes técnicos, política o reforma de la ya existente (caso especial), propuestas, entrega de servicios, entre otros.

La relación entre Responsables, Procesos e Insumos Necesarios se puede apreciar a detalle en la Figura 2.4.

2.4 POLÍTICAS DE SEGURIDAD VIGENTES

Actualmente, no existen controles que abarquen todos los dominios definidos en la norma ISO/IEC 27002:2005. La política interna vigente [**33**] está orientada a los dominios de Control de Acceso y Gestión de Comunicaciones y Operaciones que propone la norma ISO 27002:2005. El Reglamento Interno está en el Anexo E.

La política vigente con la que opera la institución orientada a la seguridad de la información, es velada por la Dirección como parte de sus funciones y responsabilidades de los procesos que está a cargo.

El Ministerio del Deporte, como entidad pública, y la Dirección de Gestión Tecnológica, como parte clave en la función de establecer las medidas de seguridad de la información, requieren establecer la política de seguridad que la ley establece. El registro oficial No. 88 describe cuáles son los aspectos que las entidades públicas deben cumplir respecto a la seguridad de la información.

2.5 ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27002:2005

El estado actual de la seguridad de la información en la dirección ha sido realizado en base a visitas in situ y entrevistas al personal pertinente de la Dirección de Gestión Tecnológica. Para determinar el estado actual de la seguridad de la información se ha realizado un análisis gap (análisis de brecha) [**35**]. El análisis gap permite identificar la distancia existente de la seguridad de la información actual de la organización respecto a las mejores prácticas definidas en la norma ISO/IEC 27002:2005; de esta manera, se puede identificar la brecha existente entre ambas y aplicar un plan de mejoramiento.

El resultado del análisis del estado actual se presenta en resumen en la **Tabla** 2.6; no obstante, el detalle de la información recopilada y análisis se presenta en el Anexo B.

En la Tabla 2.4 se presenta el responsable del control de acuerdo a la nomenclatura que se utilizará para identificarlo en la Tabla 2.6

Responsables	
Nomenclatura	Grupo al que pertenece
TIC	Área de Infraestructura
DES	Área de Desarrollo
CIE	Área de Ciencia y Tecnología
DIR	Director de la Dirección de Gestión Tecnológica
EXT	Proveedores/Soporte Externo/Otras Áreas del Ministerio
MIN	Ministro

Tabla 2.4. Nomenclatura de responsables

La distancia (brecha) entre lo que actualmente tiene la Dirección respecto a las mejores prácticas definidas en la norma ISO/IEC 27002:2005, se determinan de acuerdo a un nivel de madurez, cuyas opciones se muestran en la Tabla 2.5. Nivel de madurez

Nivel	Madurez
0	Ninguno
1	Bajo
2	Medio
3	Alto
-	No aplicable

Tabla 2.5. Nivel de madurez [31]

Los niveles de madurez definidos son:

- **Ninguno:** No existen medidas sobre el control.
- **Bajo:** Existen medidas mínimas para el cumplimiento del control
- **Medio:** Las medidas existentes son significativas para el cumplimiento del control.
- **Alto:** Se han tomado varias medidas para lograr el cumplimiento del control.
- **No aplicable:** Por las condiciones o características de las actividades en la institución no es posible o necesario analizar el cumplimiento del control.

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
5.1.1	Documento de política de seguridad de la información	TIC/DES/CIE/DIR	C	2	Reglamento interno para el uso de Servicios Tecnológicos.	Se requiere un documento emitido por la Dirección de Gestión Tecnológica abarcando los requerimientos del estatuto.
5.1.2	Revisión de la política de seguridad de la información	TIC/DES/CIE/DIR	C	1	Reglamento interno para el uso de Servicios Tecnológicos.	Falta cumplir algunos requerimientos de control que menciona el Registro No. 88 de implementación de normas ISO 27002
6.1.1	Compromiso de la Dirección con la seguridad de la información	TIC/DES/CIE/DIR	C	2	Reglamento interno para el uso de Servicios Tecnológicos.	La Dirección tiene funciones y responsabilidades que incluyen el compromiso con la Seguridad de la Información.
6.1.2	Coordinación de la seguridad de información	TIC/DES/CIE/DIR	N/C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Necesidad de establecer un Comité de Seguridad.
6.1.3	Asignación de responsabilidades de la seguridad de la información	TIC/DES/CIE/DIR	N/C	1	Reglamento interno para el uso de Servicios Tecnológicos.	Falta de cumplimiento de actividades asignadas en el Reglamento interno.
6.1.4	Proceso de autorización para los medios de procesamiento de información	TIC	C	3	Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el objetivo del control.
6.1.5	Acuerdos de confidencialidad	TIC/DES	N/C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Falla de cumplimiento de responsabilidades del personal. Uso exhaustivo de acuerdo a la segregación de funciones según CISA.
6.1.6	Contacto con autoridades	DIR/CIE	N/C	0	No existen controles definidos sobre este tema.	Falta de políticas relacionadas a este ámbito.
6.1.7	Contacto con grupos de interés especial	TIC/DES/CIE/DIR	N/C	0	No existen controles definidos sobre este tema.	En proceso de desarrollo.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (1 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
6.1.8	Revisión independiente de la seguridad de la información	TIC/DES/CIE/DIR	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deben hacer revisiones periódicas.
6.2.1	Identificación de riesgos relacionados con entidades externas	TIC/DES/CIE/DIR	N/C	1	No existen controles definidos sobre este tema.	Registro de ingreso con previa autorización para visitantes, realizado en la guardianía.
6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	TIC	C	1	Reglamento interno para el uso de Servicios Tecnológicos.	Falta de políticas relacionadas a este ámbito. Ética profesional y lineamientos de actividades como apoyo.
6.2.3	Tratamiento de la seguridad en contratos con terceras personas	TIC/EXT	N/C	1	No existen controles definidos.	Registro de ingreso con previa autorización para terceros, realizado en la guardianía.
7.1.1	Inventarios de activos	TIC/DES	C	1	Registro de activos realizado en trabajo conjunto de TIC y DES.	Adecuación de registros de activos y actualización pronta o periódica, de acuerdo a las circunstancias.
7.1.2	Propiedad de los activos	TIC/DES	C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se requiere tabular los activos existentes junto con su respectivo propietario.
7.1.3	Uso aceptable de los activos	TIC/DES	N/C	2	No existen controles definidos sobre este tema.	Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
7.2.1	Lineamientos de clasificación	DES	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Existe clasificación, sin embargo requieren ajustes para una más fácil y rápida consulta de estos.
7.2.2	Etiquetado y manejo de la información	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Existe clasificación, sin embargo requieren ajustes para una más fácil y rápida consulta de estos.
8.1.1	Roles y responsabilidades	DIR/TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Funciones y responsabilidades designadas en el Estatuto. El Estatuto requiere una revisión a fondo.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (2 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
8.1.2	Selección (Investigación de antecedentes)	MIN/DIR/TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería profundizar en los antecedentes de los postulantes, previa a la entrevista y antes de que inicien su contrato.
8.1.3	Términos y condiciones de empleo	MIN/DIR/TIC	C	2	Contrato de Trabajo	Falta de agregación de políticas internas en el contrato de trabajo. Falta de políticas que abarquen todos los requisitos del Registro Oficial No. 88
8.2.1	Gestión de responsabilidades	TIC/DES/CIE/DIR	C	1	Reglamento interno para el uso de Servicios Tecnológicos.	Falta detallar sanciones y controles relacionados con las actividades de terceros.
8.2.2	Capacitación y educación en seguridad de la información	TIC/DES/CIE/DIR	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se requiere completar políticas internas de los controles faltantes de lo mencionado en el Registro No. 88
8.2.3	Proceso disciplinario	TIC/DES/CIE/DIR	C	2	Reglamento interno para el uso de Servicios Tecnológicos.	Se requiere completar políticas internas de los controles faltantes de lo mencionado en el Registro No. 88 Falta detallar sanciones y correctivos.
8.3.1	Responsabilidades de terminación	DIR	C	2	Contrato de trabajo.	Falta de documentación que respalde el cambio o cese de actividades.
8.3.2	Devolución de activos	TIC	C	1	Contrato de trabajo.	Falta de actualización del registro de responsabilidades sobre los activos.
8.3.3	Eliminación de derechos de acceso	TIC	C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Falta de actualización inmediata de registro de actividades y/o responsabilidades.
9.1.1	Perímetro de seguridad física	TIC	C	2	Control de Acceso para el ingreso a áreas importantes.	Falta de registro de ingreso.
9.1.2	Controles de entrada físicos	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Falta de actualización inmediata de registro de actividades y/o responsabilidades.
9.1.3	Seguridad de oficinas, habitaciones y medios	MIN/DIR/TIC	C	2	Control de Acceso para el ingreso a áreas importantes.	Exceso de personal distribuido en un área limitada. Medidas de seguridad en el acceso presentes.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (3 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
9.1.4	Protección contra amenazas externas y ambientales	MIN/DIR/TIC	C	2	Control de Acceso para el ingreso a áreas importantes.	Falta de video-vigilancia, sistema anti-incendios y aire acondicionado en área de trabajo de la Dirección.
9.1.5	Trabajo en áreas seguras	MIN/DIR/TIC	C	1	Control de Acceso para el ingreso a áreas importantes.	Falta de video-vigilancia, sistema anti-incendios y aire acondicionado en área de trabajo de la Dirección.
9.1.6	Áreas de acceso público y de carga y descarga	TIC	N/C	1	No existen controles definidos sobre este tema.	Falta de registro de involucrados en entrega o deshecho de recursos. Ética profesional y lineamientos de actividades como apoyo.
9.2.1	Ubicación y protección del equipo	MIN/DIR/TIC	C	2	Video-vigilancia, Sistema Anti-incendios, Aire Acondicionado y Control de Acceso para el ingreso a áreas importantes.	Falta de medidas de vigilancia y sistema anti-incendios en área de trabajo de la Dirección.
9.2.2	Servicios públicos	MIN/DIR/TIC	C	1	UPS	EL UPS tiene un tiempo de respaldo muy bajo.
9.2.3	Seguridad en el cableado	TIC	N/C	1	No existen controles definidos sobre este tema.	Ética profesional y lineamientos de actividades como apoyo. Necesidad de monitoreo de activos.
9.2.4	Mantenimiento de equipo	TIC	N/C	1	No existen controles definidos sobre este tema.	Ética profesional y lineamientos de actividades como apoyo. Necesidad de monitoreo de activos.
9.2.5	Seguridad del equipo fuera del local	TIC	N/C	1	No existen controles definidos sobre este tema.	Ética profesional y lineamientos de actividades como apoyo. Necesidad de monitoreo de activos.
9.2.6	Reutilización o retirada segura de equipos	TIC	N/C	1	No existen controles definidos sobre este tema.	Ética profesional y lineamientos de actividades como apoyo. Necesidad de monitoreo de activos.
9.2.7	Traslado de Activos	TIC	C	2	Registro de actividades para el traslado de activos	Considerar la instalación de poner cámaras de seguridad en área de trabajo de la Dirección.
10.1.1	Procedimientos de operación documentados	TIC/DES	C	2	Documentos de procedimientos de uso de activos	Falta de organización y acceso a la documentación.
10.1.2	Gestión de cambio	DES	C	3	Ambiente de pruebas	Pruebas sobre equipos físicos. Falta virtualización.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (4 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
10.1.3	Segregación de deberes	TIC/DES/CIE/DIR	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Atención a actividades que no corresponden al Área de trabajo en casos extraordinarios.
10.1.4	Separación de los medios de desarrollo y operacionales	TIC/DES/CIE	C	3	Asignación y registro de recursos por usuario. Estatuto Orgánico de Gestión Organizacional por Procesos.	Data Center utilizado como bodega. Falta de una adecuada etiquetación física en los activos donde sea posible.
10.2.1	Provisión de servicios	TIC/DIR	C	2	Contrato de trabajo.	Falta definir garantías sobre la confidencialidad a terceros.
10.2.2	Monitorización y revisión de los servicios contratados	TIC	C	0	Herramienta de monitoreo IMC.	Disponen de herramienta de monitoreo pero no es utilizada eficientemente. Falta de certificaciones y auditorías.
10.2.3	Manejar los cambios en los servicios de terceros	DES	C	2	Ambiente de pruebas	Falta de políticas relacionadas a este ámbito. Ética profesional y lineamientos de actividades como apoyo.
10.3.1	Gestión de capacidades	TIC	C	1	Herramienta de monitoreo IMC.	Disponen de herramienta de monitoreo pero no es utilizada eficientemente. Falta de certificaciones y auditorías.
10.3.2	Aceptación del sistema	TIC/DES	C	1	Ambiente de pruebas	Falta de políticas relacionadas en este ámbito. Disponen de herramienta de monitoreo pero no es utilizada eficientemente. Falta de certificaciones y auditorías.
10.4.1	Controles contra software malicioso	TIC/DES	C	1	Antivirus, firewall, antispam en Data Center. Antivirus en cada equipo de usuario. Reglamento interno para el uso de Servicios Tecnológicos.	Falta de procedimientos de recuperación de información. Frecuente formateo en caso de ataque de software malicioso y restablecimiento de aplicaciones en equipos de clientes.
10.4.2	Controles contra códigos móviles	TIC/DIR	C	2	Reglamento interno para el uso de Servicios Tecnológicos. Antivirus en cada equipo de usuario.	Falta de verificación de cumplimiento de políticas vigentes.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (5 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
10.5.1	Copias de seguridad de la información	DES	N/C	1	No existen controles definidos sobre este tema.	Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
10.6.1	Controles de red	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Falta de análisis de reportes técnicos para respaldar guías que permitan solventar futuros problemas similares.
10.6.2	Seguridad de los servicios de red	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Falta de análisis de reportes técnicos para respaldar resultados estadísticos.
10.7.1	Gestión de los medios removibles	TIC/DIR	C	3	Reglamento interno para el uso de Servicios Tecnológicos.	Responsabilidad recae sobre el comportamiento de personal.
10.7.2	Eliminación de medios	TIC/DIR	N/C	0	No existen controles definidos en este tema.	Discos duros sin ser utilizados, almacenados en el Data Center.
10.7.3	Procedimientos de manejo de la información	TIC	N/C	1	No existen controles definidos sobre este tema.	Requieren reforzar estrategias de acceso a recursos y verificación de espacio disponible. Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
10.7.4	Seguridad de documentación del sistema	TIC/DES/CIE/DIR	N/C	1	No existen controles definidos sobre este tema.	Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
10.8.1	Procedimientos y políticas de información y software	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
10.8.2	Acuerdos de intercambio	TIC	C	2	Contrato de trabajo.	Es necesario agregar políticas que abarquen las responsabilidades y garantías sobre el manejo de la información a terceros.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (6 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
10.8.3	Soportes físicos en tránsito	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
10.8.4	Mensajes electrónicos	TIC/DES	C	3	Reglamento interno para el uso de Servicios Tecnológicos.	Falta de registro de eventos generados por mal uso.
10.8.5	Sistemas de información empresarial	EXT	-	-	-	Las actividades de contabilidad del Ministerio están asignadas a otras Áreas que no corresponden a la Dirección de Gestión Tecnológica.
10.9.1	Comercio electrónico	-	-	-	-	Página web consultiva. No se pueden hacer modificaciones desde la página web. No se realiza comercio electrónico.
10.9.2	Transacciones en línea	EXT	-	-	-	No se realizan transacciones financieras por medio de la página web. Página web consultiva. Las actividades financieras del Ministerio están asignadas a otros departamentos no correspondientes a la Dirección de Gestión Tecnológica.
10.9.3	Información públicamente disponible	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
10.10.1	Registro de auditoría	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
10.10.2	Uso del sistema de monitoreo	TIC	C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Disponen de herramienta de monitoreo pero no es utilizada eficientemente. Falta de capacitación del personal para el uso de dicha herramienta.
10.10.3	Protección de la información del registro	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (7 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
10.10.4	Registros del administrador y operador	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
10.10.5	Registro de fallas	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
10.10.6	Sincronización de relojes	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería considerar el respaldo del reloj de sincronización.
11.1.1	Política de control de acceso	TIC/DES/CIE/DIR	C	3	Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el objetivo del control.
11.2.1	Inscripción del usuario	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería revisar histórico de registros para eliminación de usuarios que ya no trabajan en la Dirección.
11.2.2	Gestión de privilegios	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
11.2.3	Gestión de la clave del usuario	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
11.2.4	Revisión de los derechos de acceso del usuario	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se recomienda realizar revisiones periódicas.
11.3.1	Uso de contraseñas	TIC	C	3	Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el objetivo del control.
11.3.2	Equipo de usuario desatendido	TIC/DES/CIE/DIR	N/C	1	No existen controles definidos sobre este tema.	Se deja a libre disposición de los usuarios el determinar el automático cierre de sesión.
11.3.3	Política de pantalla y escritorio limpio	TIC/DES/CIE/DIR	N/C	1	No existen controles definidos sobre este tema.	Se debería incentivar a los usuarios evitar dejar información expuesta sobre escritorios y monitores.
11.4.1	Política sobre el uso de servicios en red	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (8 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
11.4.2	Autenticación del usuario para conexiones externas	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el objetivo del control.
11.4.3	Identificación del equipo en red	TIC	N/C	1	No existen controles definidos sobre este tema.	Existen lineamientos orientados a las actividades que el control busca, pero aún faltan ser redactadas y aprobadas para ser puestas en vigencia.
11.4.4	Protección del puerto de diagnóstico remoto	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Debería hacerse uso de la herramienta de monitoreo sobre los puntos que se consideren críticos de la infraestructura de la red.
11.4.5	Segregación en redes	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían realizar actualizaciones y verificaciones de los registros de: servicios, usuarios y sistemas de información.
11.4.6	Control de conexión de redes	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían generar y guardar registros y actividades de los usuarios.
11.4.7	Control de encaminamiento (routing) de red	TIC	N/C	0	No existen controles definidos sobre este tema.	Se debería dar un uso más práctico a la herramienta de monitoreo IMC.
11.5.1	Procedimientos de registro en el terminal	TIC	C	2	Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el control.
11.5.2	Identificación y autenticación del usuario	TIC	C	2	Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el control.
11.5.3	Sistema de gestión de claves	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.
11.5.4	Uso de utilidades del sistema	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.
11.5.5	Sesión inactiva	TIC/DES/CIE/DIR	N/C	0	No existen controles definidos sobre este tema.	Se deja a libre disposición de los usuarios el determinar el automático cierre de sesión.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (9 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
11.5.6	Limitación de tiempo de conexión	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.
11.6.1	Restricción al acceso a la información	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.
11.6.2	Aislamiento del sistema sensible	TIC/DES	N/C	1	No existen controles definidos sobre este tema.	Se deberían separar sistemas sensibles. Es necesario un plan de migración de equipos.
11.7.1	Computación móvil y comunicaciones	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.
11.7.2	Tele-trabajo	-	-	-	-	No se realiza teletrabajo. Los accesos remotos de soporte técnico se hacen bajo la presencia y autorización de personal del Área de Infraestructura.
12.1.1	Análisis y especificación de los requerimientos de seguridad	TIC/DES/CIE	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.2.1	Validación de los datos de entrada	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.2.2	Control de procesamiento interno	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.2.3	Integridad de los mensajes	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.2.4	Validación de los datos de salida	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.3.1	Política sobre el uso de controles criptográficos	TIC/DES	N/C	1	No existen controles definidos de este tema.	Se deberían establecer textualmente las políticas sobre el uso de controles criptográficos.
12.3.2	Gestión de claves	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con el control.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (10 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
12.4.1	Control de software operacional	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían establecer guías de procedimiento para controlar la instalación de software.
12.4.2	Protección de la data de prueba del sistema	DES	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían establecer guías de procedimiento para controlar las diferentes etapas de prueba.
12.4.3	Control de acceso al código fuente del programa	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.5.1	Procedimientos de control de cambio	TIC/DES/CIE/DIR	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	TIC/DES/CIE	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.5.3	Restricciones sobre los cambios en los paquetes de software	DES/DIR	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.5.4	Filtración de información	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos. Reglamento interno para el uso de Ser. Tecno.	Se cumple con control.
12.5.5	Desarrollo externalizado de software	TIC	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se cumple con control.
12.6.1	Control de las vulnerabilidades técnicas	TIC/DES/CIE	N/C	0	No existen controles definidos sobre este tema.	Se deberían establecer evaluaciones de vulnerabilidades y test de penetración a la red.
13.1.1	Reporte de eventos en la seguridad de la información	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos. Reglamento interno para el uso de Servicios Tecnológicos.	Se cumple con el objetivo del control.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (11 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
13.1.2	Reporte de debilidades en la seguridad	TIC/DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería incentivar a los usuarios reportar cuando: sospechen sobre anomalías y comportamientos extraños de las aplicaciones, o sospechen de debilidades que podrían puedan amenazar la seguridad de la información.
13.2.1	Responsabilidades y procedimientos	TIC/DES/CIE/DIR	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Es necesario establecer una clasificación de eventos y relacionarlas entre las diferentes Áreas de la Dirección. Esto debería realizarse y actualizarse a partir de cada informe técnico generado.
13.2.2	Aprendizaje de los incidentes en la seguridad de la información	TIC/DES/CIE	N/C	1	No existen controles definidos sobre este tema.	Es necesario realizar análisis y evaluación de riesgos sobre los activos.
13.2.3	Recolección de evidencia	TIC/CIE	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería utilizar las evidencias para dar seguimiento a todo tipo de eventos, incluyendo los que conlleven acciones legales.
14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad comercial	TIC/DES/CIE	N/C	1	No existen controles definidos sobre este tema.	Se deberían tomar medidas que minimicen el impacto del cese de actividades de aplicaciones y servicios. Es necesaria la definición de responsabilidades y política para la gestión de continuidad de negocio.
14.1.2	Continuidad comercial y evaluación del riesgo	TIC	C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Es necesaria una valoración de activos previa para poder realizar análisis y evaluación de riesgos.
14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	TIC/DES/CIE	N/C	1	No existen controles definidos sobre este tema.	Se deberían redactar planes de continuidad de negocio en base a la experiencia, informes técnicos realizados y un análisis y evaluación de riesgos.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (12 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
14.1.4	Marco referencial para la planeación de la continuidad comercial	TIC/DES/CIE	N/C	1	No existen controles definidos sobre este tema.	Se deberían redactar planes de continuidad de negocio en base a la experiencia, informes técnicos realizados y un análisis y evaluación de riesgos.
14.1.5	Prueba, mantenimiento y reevaluación de planes de continuidad	TIC/DES/CIE	N/C	1	No existen controles definidos sobre este tema.	Se deberían redactar planes de continuidad de negocio en base a la experiencia, informes técnicos realizados y un análisis y evaluación de riesgos. Es necesaria la realización de pruebas periódicas para verificar su eficacia y realizar actualizaciones.
15.1.1	Identificación de legislación aplicable	CIE/DIR	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos. Registro Oficial No 88. Ley de Transparencia y el Derecho a la Información.	Se cumple con el objetivo del control.
15.1.2	Derechos de propiedad intelectual (IPR)	DES/CIE	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	La adquisición y desarrollo de software es exclusivo para uso de la institución y tiene un procedimiento legal.
15.1.3	Protección de los registros organizacionales	DES	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería definir el tiempo de almacenamiento de registros.
15.1.4	Protección de datos y privacidad de la información de carácter personal	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Los clientes requieren definir el alcance de uso de sus equipos. Se debería concientizar el manejo de información personal.
15.1.5	Prevención del mal uso de medios de procesamiento de información	TIC/DES	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían registrar las actividades del personal y generar informes sobre el mal uso de dispositivos y acceso a aplicaciones y servicios.
15.1.6	Regulación de controles criptográficos	DES	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Las pruebas criptográficas se realizan en ambiente de pruebas y requieren autorización legal para implementar.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (13 de 14)

REQUISITO ISO 27001	CONTROL	ENCARGADO	C/(N/C)	MADUREZ	CONTROLES	Observaciones
15.2.1	Cumplimiento con las políticas y estándares de seguridad	TIC/DES/CIE/DIR	C	3	Estatuto Orgánico de Gestión Organizacional por Procesos. Reglamento interno para el uso de Servicios Tecnológicos.	Se debería capacitar al personal y verificar el cumplimiento para el uso correcto de herramientas (software o hardware) para prevenir incidentes de seguridad.
15.2.2	Chequeo de cumplimiento técnico	TIC	C	2	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se deberían registrar las actividades del personal y generar informes sobre el mal uso de dispositivos y acceso a aplicaciones y servicios.
15.3.1	Controles de auditoría de sistemas de información	TIC/DES/CIE/DIR	N/C	0	No existen controles definidos.	Se debería considerar tener visión de cumplimiento de requerimientos de seguridad en el marco legal, y también para obtener certificaciones.
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	DES	C	1	Estatuto Orgánico de Gestión Organizacional por Procesos.	Se debería hacer uso del ambiente de pruebas, resguardo de respaldos y registros de actividades en la red, para aplicarlos en uso de auditorías.

Tabla 2.6. Resumen del análisis gap del estado actual de la seguridad de la información (14 de 14)

Según el resumen gap se observa que se han considerado con mayor énfasis dos dominios de la ISO/IEC 27002:2005 (dominios 11 y 12). Además, existen controles que no han sido aún considerados en la Dirección para cumplir los requerimientos de ley sobre la Seguridad de la Información. Finalmente, algunos controles que sí han sido considerados en la Dirección requieren ciertos ajustes para ser eficientes o adecuados.

2.6 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para la valoración de activos y para el análisis y evaluación de riesgos se considerarán determinados parámetros y criterios. El análisis de riesgos se realizará tomando como referencia la norma ISO/IEC 27005:2008 y las sugerencias de clasificación de amenazas mencionado en MAGERIT.

2.6.1 CRITERIOS Y SUS VALORACIONES

Para poder lograr una medición cuantificable sobre las evaluaciones es necesario dar valores a los parámetros utilizados en el proceso. Los valores dados definen diferentes niveles de criticidad.

Cada nivel tendrá atributos que lo califiquen junto con un valor numérico para poder realizar un cálculo matemático medible. El cálculo que se realice se utilizará para diferenciar niveles en la valoración de activos y determinar una estimación de riesgo en el análisis y evaluación.

2.6.1.1 Criterios de Valoración de Activos

Los incidentes de seguridad suelen comprometer la confidencialidad, integridad y disponibilidad de un activo. Debido a ello, se han considerado darles a dichas características de los activos una escala de valoración que permita identificar cuáles son los que se considerarán críticos.

Los valores utilizados para la medición de los parámetros de Confidencialidad, Integridad y Disponibilidad de los activos, se encuentran en la escala mostrada en la **¡Error! No se encuentra el origen de la referencia.** [22] [2] [3]

Criterios de valoración de activos				
Valoración		Parámetros		
		[C] Confidencialidad	[I] Integridad	[D] Disponibilidad
1	bajo	La divulgación del activo podría afectar de forma insignificante la entrega de servicios.	La modificación del activo podría afectar de forma insignificante la entrega de servicios.	La no disponibilidad del activo podría afectar de forma insignificante la entrega de servicios.

Tabla 2.7. Criterios de Valoración de Activos (1 de 2)

Criterios de valoración de activos				
Valoración		Parámetros		
		[C] Confidencialidad	[I] Integridad	[D] Disponibilidad
2	moderado	La divulgación del activo podría afectar parcialmente la entrega de servicios.	La modificación del activo podría afectar parcialmente la entrega de servicios.	La no disponibilidad del activo podría afectar parcialmente la entrega de servicios.
3	alto	La divulgación del activo podría afectar significativamente la entrega de servicios.	La modificación del activo podría afectar significativamente la entrega de servicios.	La no disponibilidad del activo podría afectar significativamente la entrega de servicios.
4	muy alto	La divulgación del activo podría afectar gravemente la entrega de servicios.	La modificación del activo podría afectar gravemente la entrega de servicios.	La no disponibilidad del activo podría afectar gravemente la entrega de servicios.
5	crítico	La divulgación del activo podría afectar totalmente la entrega de servicios.	La modificación del activo podría afectar totalmente la entrega de servicios.	La no disponibilidad del activo podría afectar totalmente la entrega de servicios.

Tabla 2.7. Criterios de Valoración de Activos (2 de 2)

La escala mostrada tiene un incremento de criticidad con el aumento del valor dado, es decir, mientras mayor sea el valor otorgado al parámetro (5 es el valor máximo), mayor será la criticidad.

Debido a que, de manera general, no existen respaldos para los activos (salvo en excepciones puntuales), se definirá un valor en el costo del activo según la Tabla 2.8 [**22**]

[Costo] Costo del Activo		
Valoración		Descripción
1	bajo	El costo del activo o su reposición es despreciable y no representa una pérdida económica para el Data Center.
2	moderado	El costo del activo o su reposición es bajo y representa una pérdida económica mínima para el Data Center.
3	alto	El costo del activo o su reposición es significativo y representa una pérdida económica considerable para el Data Center.
4	muy alto	El costo del activo o su reposición es elevado y representa una pérdida económica grave para el Data Center.
5	crítico	El costo del activo o su reposición es demasiado alto y representa una pérdida económica fatal para el Data Center.

Tabla 2.8. Costo de Activos

El resultado de la valoración será realizado bajo la operación matemática:

$$[NI] = [C] + [I] + [D] + [Costo] \qquad [22] [37]$$

En donde:

NI *es el nivel de Importancia*

C *es la confidencialidad*

I *es la Integridad*

D *es la disponibilidad*

Costo *es el costo del activo*

El resultado obtenido será NI, el cual representa el nivel de importancia y permitirá diferenciar los activos más relevantes. Este valor será clasificado de acuerdo al rango en el que se encuentre según la Tabla 2.9.

[NI] Nivel de Importancia		
Valoración		**Descripción**
4 a 5	no importante	El activo es insignificante para la entrega de servicios, en base a los criterios de costo del activo y la confidencialidad, disponibilidad e integración.
6 a 8	poco importante	El activo es de poca importancia para la entrega de servicios, en base a los criterios de costo del activo y la confidencialidad, disponibilidad e integración.
9 a 11	Importante	El activo es significativo para la entrega de servicios, en base a los criterios de costo del activo y la confidencialidad, disponibilidad e integración.
12 a 15	muy importante	El activo es muy significativo para la entrega de servicios, en base a los criterios de costo del activo y la confidencialidad, disponibilidad e integración.
16 a 20	Crítico	El activo es vital para la entrega de servicios, en base a los criterios de costo del activo y la confidencialidad, disponibilidad e integración.

Tabla 2.9. Nivel de Importancia

2.6.1.2 Criterios de Probabilidad de Ocurrencia

Los criterios de probabilidad de ocurrencia de una amenaza tienen un valor cuantificable del 1 al 4, siendo 4 el valor más alto y de mayor criticidad.

La Tabla 2.10 muestra los valores que serán tomados en un rango porcentual para la probabilidad de ocurrencia [**22**] [**2**] [**3**].

[Prob] Probabilidad de ocurrencia		
Valoración		**Descripción**
1 (0 a 25%)	muy improbable	Amenazas con muy baja probabilidad de explotar vulnerabilidades
2 (26 a 50%)	moderadamente probable	Amenazas con poca frecuencia de probabilidad de explotar vulnerabilidades
3 (51 a 75%)	altamente probable	Amenazas con alta probabilidad de explotar vulnerabilidades
4 (76 a 100%)	muy probable	Amenazas que muchas veces explotan vulnerabilidades

Tabla 2.10. Probabilidad de ocurrencia

La probabilidad de ocurrencia es una apreciación de que la amenaza suceda, aun considerando los controles existentes.

2.6.1.3 Criterios de Valoración del Impacto

El impacto analizado sobre un activo está directamente relacionado con los criterios de valoración del activo: confidencialidad, integridad y disponibilidad; debido a ello los resultados que se obtengan en la valoración de activos, incluido el nivel de importancia, serán puntos clave en la decisión de valoración del impacto.

Por el modus operandi de la institución y particularmente de las actividades de la Dirección, se ha considerado tomar dos puntos de vista sobre el impacto: orientado al número posible de clientes afectados y, orientado al tiempo en recuperar un servicio.

Dichos criterios se los ha considerado, debido a que son los puntos de vista más significativos durante el tratamiento de ataques o eventos fortuitos y suelen ser requeridos en los informes técnicos para tener una idea de lo perjudicial que sería si sucediera de nuevo, lo cual ayuda determinar la prioridad en el tratamiento de eventos similares en el futuro.

Podrían considerarse más puntos de vista, dependiendo de las condiciones que se requieren analizar, lo cual conlleva a más categorías del impacto con sus respectivas escalas; del mismo modo se puede centralizar la medida del impacto en una sola categoría simplificando de esa manera el análisis de riesgo.

En cualquier caso mencionado anteriormente, el impacto siempre estará relacionado directamente con los criterios de confidencialidad, integridad y disponibilidad del activo analizada frente a una amenaza.

Las 2 categorías seleccionadas para el análisis de impacto son:

1. Impacto de clientes afectados: en caso de ocurrencia de un ataque, cuál sería la posible cantidad de usuarios que estarían afectados. La escala a esta valoración se observa en la Tabla 2.11 [**22**] [**2**] [**3**]

2. Impacto de recuperación del servicio: en caso de ocurrencia, cuánto tiempo estimado se demoraría en resolver el evento. La escala a esta valoración se observa en la Tabla 2.11 [**22**] [**2**] [**3**]

[$I_{Clientes}$] Impacto de clientes afectados		
Valoración		**Descripción**
1	insignificante	Si una amenaza sucede, muy pocos clientes dejarían de recibir servicio. Menor a 10 clientes.
2	pequeño	Si una amenaza sucede, pocos clientes dejarían de recibir servicio. Entre 11 a 25 clientes.
3	moderado	Si una amenaza sucede, una cantidad moderada de clientes dejarían de recibir servicio. Entre 26 a 40 clientes.
4	grave	Si una amenaza sucede, una cantidad significativa de clientes dejarían de recibir servicio. Entre 41 a 60 clientes.
5	catastrófico	Si una amenaza sucede, una gran cantidad de clientes dejarían de recibir servicio. Mayor a 60 clientes.

Tabla 2.11. Criterios de valoración del impacto de clientes afectados

[I_{Recup}] Impacto de recuperación de servicios		
Valoración		**Descripción**
1	insignificante	Tiempo de recuperación inmediato. El cliente no percibe pérdida del servicio.
2	pequeño	Tiempo de recuperación casi inmediato. El cliente percibe apenas la pérdida del servicio.
3	moderado	Tiempo de recuperación considerable. El cliente percibe pérdida del servicio.
4	grave	Tiempo de recuperación amplio. El cliente percibe considerable pérdida del servicio con posible reclamo.
5	catastrófico	Tiempo de recuperación extenso. El cliente percibe pérdida del servicio y exige que se reponga.

Tabla 2.12. Criterios de valoración del impacto de recuperación de servicios

2.6.1.4 Criterios de Evaluación del Riesgo

El riesgo, como medida cuantificable, será el resultado del producto de la probabilidad de ocurrencia de la amenaza por los dos impactos mencionados en la Tabla 2.8 y Tabla 2.9 [**22**] [**2**] [**3**]

$$[Riesgo] = [Prob] * [I_{Clientes}] * [I_{Recup}] \qquad [3]\ [22]$$

El valor obtenido del riesgo será una medida que se comparará con la Tabla 2.13 dentro de los intervalos identificados en dicha tabla.

[Riesgo]		
Valoración		**Descripción**
1 a 10	Bajo	Riesgo bajo en consideración al número de clientes que serían afectados y el tiempo que tomaría a la Dirección reactivar los servicios. La pérdida de servicio para los clientes sería imperceptible.
11 a 27	moderado	Riesgo moderado en consideración al número de clientes que serían afectados y el tiempo que tomaría a la Dirección reactivar los servicios. La pérdida de servicio para los clientes sería leve.
28 a 60	Alto	Riesgo alto en consideración al número de clientes que serían afectados y el tiempo que tomaría a la Dirección reactivar los servicios. La pérdida de servicio para los clientes sería notoria.
61 a 80	muy alto	Riesgo muy alto en consideración al número de clientes que serían afectados y el tiempo que tomaría a la Dirección reactivar los servicios. La pérdida de servicio para los clientes sería elevada.
81 a 125	Crítico	Riesgo crítico en consideración al número de clientes que serían afectados y el tiempo que tomaría a la Dirección reactivar los servicios. La pérdida de servicio para los clientes sería crítica.

Tabla 2.13. Criterios de evaluación del riesgo

2.6.1.5 Criterios para el Tratamiento del Riesgo

Tras la evaluación realizada sobre las amenazas seleccionadas y los resultados obtenidos en el cálculo del riesgo, se escogerán dos opciones: retención del riesgo o reducción del riesgo.

No se ha seleccionado la opción de *evitar el riesgo*, debido a que se busca que los servicios que provee la Dirección de Gestión Tecnológica en la institución deberían garantizarse estar operativos al menos en horario de oficina. Tampoco se ha escogido la *transferencia del riesgo* dado que sería utilizada en casos extremos como se menciona a continuación de los criterios para el tratamiento del riesgo en la Tabla 2.14.

Esta selección está directamente relacionada con los resultados de valoración del riesgo obtenidos en la Tabla 2.13, y la decisión de qué acción tomar para su tratamiento, según la Tabla 2.14 [**22**] [**2**] [**3**]

Valoración del Riesgo	Tratamiento del Riesgo
Bajo	Aceptación del Riesgo
moderado	
Alto	Reducción del Riesgo
muy alto	
Crítico	

Tabla 2.14. Criterios para el tratamiento del riesgo

- Aceptación del riesgo: No es requerida la implementación de controles adicionales y el riesgo se puede retener (se asume que los controles existentes son suficientes para que se contrarreste tal amenaza y requiere monitoreo para verificar que no explote otras vulnerabilidades) o aceptar (el riesgo es insignificante y los controles podrán contrarrestarlo).
- Reducción del riesgo: Se aplicarán los controles relacionados con: corrección, prevención, minimización de impacto, disuasión, eliminación, monitoreo, recuperación y toma de conciencia. En caso que existan riesgos que conlleven a costos demasiado elevados, se optará por la transferencia del riesgo.

Esto es utilizado como equivalencia/referencia y se realizará “evitar el riesgo” o “transferir el riesgo” cuando se considere pertinente.

2.6.2 VALORACIÓN DE ACTIVOS

La valoración de activos se realizará con el uso de los valores mencionados en la **¡Error! No se encuentra el origen de la referencia.** y Tabla 2.8 con lo cual, el esultado obtenido, se comparará finalmente con la categorización de la Tabla 2.9

Los valores evaluados según la **¡Error! No se encuentra el origen de la eferencia.**, son los parámetros de: confidencialidad, integridad y disponibilidad del activo y se define su valoración para cuando un incidente podría afectar en la entrega de servicios.

Los valores evaluados según la Tabla 2.8, serán sobre el costo del activo el cual está relacionado al costo económico que implicaría al recuperarlo o reponerlo tras un incidente y lograr reanudar la entrega de servicios.

2.6.2.1 Clasificación de Activos

Los activos han sido clasificados en categorías [**22**] para poder identificar de mejor manera cuáles serán los riesgos a ser analizados en el análisis y evaluación de riesgos. Estas categorías son:

- **Activos de Documentación:** Elementos que poseen contenido textual que puede estar escrita o almacenada digitalmente como: procedimientos, contratos, manuales, etc.
- **Activos de Software:** Aplicaciones y software que provee el data center para facilitar y / o permitir las actividades de los usuarios.
- **Activos de Red:** Elementos que forman parte de la infraestructura de red de la institución en cuestión que permiten la comunicación entre usuarios y el acceso a los servicios provenientes del data center.
- **Activos de Sistema Eléctrico:** Elementos que forman parte de la circuitería que permite el acceso al servicio eléctrico, incluidos aquellos elementos que lo salvaguardan.
- **Activos de Soporte Mecánico:** Elementos que forman parte del sistema que permite el control de climatización.
- **Activos de Vigilancia:** Elementos utilizados para el sistema de video vigilancia, incluidos los sensores que permitan la activación de grabación.
- **Activos de Anti-incendios:** Elementos que permiten las medidas que contrarresten un posible incendio, incluidos los sensores involucrados.
- **Activos de Control de Acceso:** Elementos utilizados como alternativa de control que permiten la verificación de identidad y permisión de acceso.

2.6.3 IDENTIFICACIÓN DE ACTIVOS

Para la identificación de los activos, y su posterior clasificación dentro de una de las categorías definidas en la sección anterior, se utilizó el enfoque de “arriba hacia abajo”, el cual consiste en identificar y analizar los procesos y de éstos, finalmente identificar los activos con los que están involucrados. La Figura 2.4 muestra el resultado de dicha tarea.

2.6.3.1 Proceso de Valoración de un Activo

En esta sección se presentan tres ejemplos de muestra que resumen el proceso llevado a cabo para la valoración de cada uno de los activos de la Dirección. Los ejemplos de muestra han sido seleccionados de tal forma que se pueda demostrar la diferencia de criticidad que existe entre cada activo.

Los resultados completos del proceso de valoración de cada activo han sido recopilados desde la Tabla 2.15 hasta la Tabla 2.22.

2.6.3.1.1 Ejemplo de Muestra 1

El activo denominado *Sistema operativo de los servidores*, de la categoría de activos *Software* tiene las siguientes características:

- Aloja los procesos en ejecución de cada uno de los servicios que se brindarán en la Dirección.
- Almacena archivos de configuración de los servicios de la dirección.
- Es necesario que inicie sin contrariedades para la ejecución de aplicaciones y procesos que son necesarios para la entrega de servicios.

Por lo antes mencionado a este activo le corresponde el siguiente procedimiento de valoración:

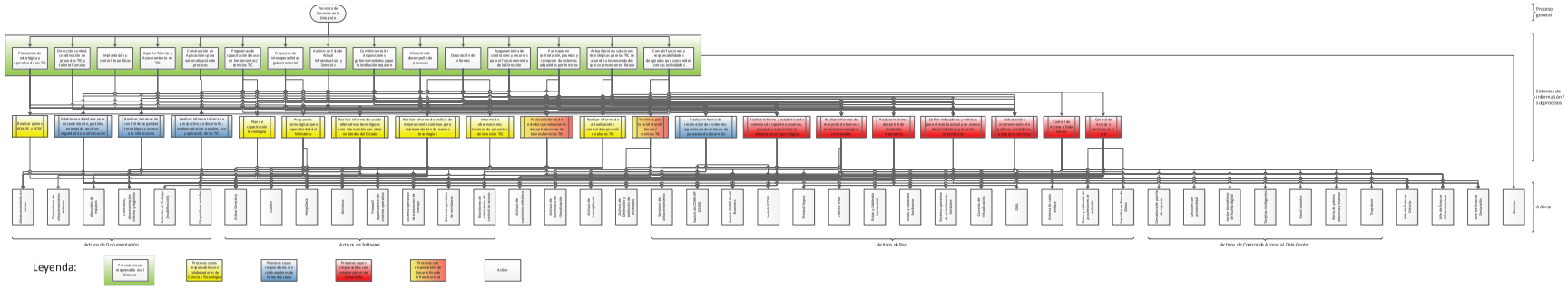

Figura 2.4. Relación de Procesos y Activos

Parámetro a evaluar: Valor Confidencialidad [C]

- Dado que aloja los servicios a entregar en la red interna de la Dirección y toda la información asociada para su funcionamiento, parámetros de configuración (direcciones IP, puertos, procesos, usuarios, etc.), paquetes de software (versiones, parámetros de configuración, códigos de programa, etc.), etc., y también almacena información de credenciales de acceso al sistema y otra información sensible.
- Se podrían tomar medidas para contrarrestar su divulgación como el cambio de contraseñas de acceso de manera periódica.

Por las características presentadas, este activo tiene un **nivel de valoración crítico en torno a confidencialidad** que corresponde al valor de 5.

Parámetro a evaluar: Valor Integridad [I]

- Si se modificara la información, contenida en este activo (parámetros de configuración, permisos, etc.) sería perjudicial ya que sobre éste se soportan los servicios de red provistos por la Dirección, siendo una de sus tareas primordiales.

Por las condiciones analizadas, ocasionarían resultados significativos para la entrega de servicios, se le categoriza como un **activo crítico respecto a integridad** (5).

Parámetro a evaluar: Valor Disponibilidad [D]

- La no disponibilidad del activo podría afectar la entrega de servicios si ocurriera un incidente que requiere recuperación de servicios inmediata.
- Se verían afectados muchos o probablemente todos los servicios de red.

- Las pruebas y análisis que harían uso de este activo no podrían ser desplazadas a nuevos dispositivos de reemplazo por la falta de redundancia del mismo.
- Habría una pérdida considerable en el tiempo de restablecimiento de servicios si se dependiera de este activo únicamente.

Por lo antes mencionado, este activo se categoriza con un **valor crítico para disponibilidad** (5).

Parámetro a evaluar: Costo del Activo [C]

- El reemplazo o restitución de este activo es bajo y representa una inversión económica mínima a la institución.

Por esta justificación, se le categoriza con un valor moderado (2).

Tras obtener los valores en el análisis, se procede a realizar la suma de todos ellos, según la fórmula definida en el punto 2.6.1.1 de NI:

NI = 5 + 5 + 5 + 2

NI = 17

Según este valor de NI, se puede comparar con los parámetros definidos en la Tabla 2.9, con lo que se concluye que el **Nivel de Importancia del activo es "crítico"** para la entrega de servicios.

2.6.3.1.2 Ejemplo de Muestra 2

Para el activo denominado *Switch de Core HP A5500*, de la categoría de activos *Red*, tiene las siguientes características:

- Es el equipo por el que pasa la mayor cantidad de tráfico en la red.

- Es el equipo central de la institución que comunica a todos los puntos de red.
- Es el equipo al que se conectan los servicios de la Dirección para abastecer a la institución.

Por lo antes mencionado a este activo le corresponde el siguiente procedimiento de valoración:

Parámetro a evaluar: Valor Confidencialidad [C]

- Este activo requiere que se configuración en sus puertos para definir los tráficos que acceden o salen hacia la intranet.
- Si se divulgara la información podría afectar al acceso a servicios de proveedores externos y a la comunicación con otras entidades.
- Además representa un riesgo si llegara a conocimiento de terceros que intenten penetrar a la intranet.
- Se podrían tomar medidas para contrarrestar su divulgación como el cambio de contraseñas de acceso de manera periódica.

Por las características presentadas, este activo tiene un **nivel de valoración crítico en torno a confidencialidad** y se le categoriza con un valor de 5.

Parámetro a evaluar: Valor Integridad [I]

- Si se modificara la información contenida en este activo sería perjudicial en el caso de comunicarse con otras entidades, acceder a servicios externos, y comunicación interna entre los hosts.
- Las actividades internas requerirían compromiso firmado en los procesos, lo cual implicaría papeleo.

Por las condiciones analizadas, ocasionarían resultados significativos para la entrega de servicios, se le categoriza como un **activo valorado como muy alto respecto a integridad** (4).

Parámetro a evaluar: Valor Disponibilidad [D]

- La no disponibilidad del activo podría afectar la entrega de servicios si ocurriera un incidente que requiere recuperación de servicios inmediata.
- Toda la comunicación en la intranet podría verse afectada parcial o totalmente.
- Habría una pérdida considerable en el tiempo de restablecimiento de servicios si se dependiera de este activo únicamente.

Por los pros y contras analizados, se le categoriza como un activo crítico respecto a disponibilidad (5).

Parámetro a evaluar: Costo del Activo [C]

- Existe un respaldo que podría ser intercambiado si fallara el original, sin embargo, es de alto costo.
- El reemplazo o restitución de este activo es alto y representa una inversión económica excesiva a la institución.

Por esta justificación, se le categoriza el parámetro “costo” como crítico con un valor de 5.

Tras obtener los valores en el análisis, se procede a realizar la suma de todos ellos, según la fórmula en el punto 2.3.1 de NI:

NI = 5 + 4 + 5 + 5

NI = 19

Según este valor de NI, se puede comparar con la Tabla 2.6, con lo que se define que el Nivel de Importancia del activo es “crítico” para la entrega de servicios.

2.6.3.1.3 Ejemplo de Muestra 3

Para el activo denominado *Lector biométrico de huella digital*, de la categoría de activos *Control de Acceso*, tiene las siguientes características:

- Es el medio utilizado para acceder al Data Center.
- Es administrado por el Jefe del Área de Infraestructura y registra el acceso al área del Data Center.
- La huella digital de acceso que valida el ingreso es del Jefe del Área de Infraestructura o a uno de sus colaboradores en caso que sea necesario, con previa autorización del mismo Jefe.

Por lo antes mencionado a este activo le corresponde el siguiente procedimiento de valoración:

Parámetro a evaluar: Valor Confidencialidad [C]

- Este activo requiere registro previo por parte del Jefe del Área de Infraestructura.
- El registro está permitido únicamente el acceso al Jefe de Infraestructura y al personal de su Área con validación previa y temporizada, es decir, con un tiempo límite definido.
- En caso que personales externos o terceros requieran acceder, requerirán de la presencia del Jefe del Área de Infraestructura, o en su defecto una validación previa con un colaborador de su Área.
- Si se divulgara la información no afectaría directamente la entrega de servicios dado que existen medidas de control de acceso y es muy limitada y requerirían del Jefe de Infraestructura in situ.

Por las condiciones mencionadas, este activo le corresponde una valoración en torno a confidencialidad de moderado, correspondiente al valor 2.

Parámetro a evaluar: Valor Integridad [I]

- Si se modificara la información contenida en este activo sería únicamente bajo manipulación del Jefe de Infraestructura.
- La manera más directa de afectar a este activo sería por negligencia o acciones intencionales del Jefe de Infraestructura.
- Es necesaria la presencia del Jefe de Infraestructura y de los códigos de acceso que utilice para modificar la información de registro.

Por las condiciones mencionadas, este activo le corresponde una valoración en torno a integridad de “alto”, correspondiente al valor 3.

Parámetro a evaluar: Valor Disponibilidad [D]

- La no disponibilidad del activo podría afectar la demora en el acceso al Data Center.
- Sería un inconveniente si no respondieran las medidas adicionales de acceso y la configuración realizada por el Jefe de Infraestructura.
- Sería un inconveniente en caso de eventos aleatorios como en caso de incendios, sin embargo, existen medidas adicionales para contrarrestar incendios.
- En caso de trabajos programados, se realizarían con una demora el acceso a personal que requiera ingresar al Data Center, sin embargo, sería una solución que debe buscar el Jefe de Infraestructura.

Por las condiciones mencionadas, este activo le corresponde una valoración en torno a disponibilidad de “alto”, correspondiente al valor 3.

Parámetro a evaluar: Costo del Activo [C]

- El reemplazo o restitución de este activo es bajo y representa una inversión económica mínima a la institución.
- Existen alternativas adicionales para acceder al Data Center.

Por esta justificación, se le categoriza el parámetro “costo” como moderado, con un valor de 2; tras obtener los valores en el análisis, se procede a realizar la suma de todos ellos, según la fórmula en el punto 2.3.1 de NI:

NI = 2 + 3 + 3 + 2

NI = 10

Según este valor de NI, se puede comparar con la Tabla 2.6, con lo que se define que el Nivel de Importancia del activo es “importante” para la entrega de servicios.

2.6.3.2 Valoración de Activos por Categorías

Los activos han sido agrupados en categorías, debido a que se algunos activos se encuentran estrechamente relacionados más con unos que son otros y de esa forma permite identificar del grupo cuáles sobresalen en la búsqueda de los activos críticos o que requieren mayor atención.

Los activos mostrados en el punto 2.6.3 han sido agrupados en categorías para realizar la valoración de cada uno. Con los ejemplos dados en el punto 2.6.3.1 del presente proyecto, a continuación se muestran los resultados obtenidos al valorar a cada activo en las siguientes Tablas:

Valoración de Activos de Documentación del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Almacenamiento en cintas	3	5	4	2	14
Dispositivos de almacenamiento externo	4	3	2	2	11
Manuales de equipos	1	1	2	1	5
Contratos, documentación interna, registros	1	1	1	2	5
Estación de trabajo (Área de Infraestructura / TI / Administración del Data Center / Help Desk)	2	2	3	2	9
Laptops, Agendas electrónicas (Área de Infraestructura - Administración del Data Center / TI)	3	3	2	2	10

Tabla 2.15. Valoración de Activos de Documentación de la Dirección

Valoración de Activos de Software del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Active Directory	3	3	4	2	12
Correo	4	3	2	3	12
Help desk	2	3	3	4	12
Antivirus	2	2	3	3	10
Firewall dependiente del sistema operativo	3	3	4	2	12
Sistema operativo de estaciones de trabajo	2	2	2	2	8
Sistema operativo de los servidores	5	5	5	2	17
Monitoreo del subsistema control de acceso	2	3	4	2	11

Tabla 2.16. Valoración de Activos de Software

Valoración de Activos de Red del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Servidor Almacenamiento (almacenamiento en disco)	4	5	5	3	17
Switch de Core HP A5500	5	4	5	5	19
Switch Cisco Mall Business SG 200-08P (x2)*	4	4	4	5	17
Switch 3COM 3CVL5F26PWRH (x9)**	4	4	5	5	18
Firewall Kypus	4	4	4	4	16
Central IPBX	3	4	4	4	15
Rutas y Cableado Horizontal	1	1	4	4	10
Rutas y Cableado Backbone	1	1	4	4	10
Sistema Operativo de Virtualización - Vmware	3	3	3	2	11
Router de Frontera	5	5	4	4	18
Consola de virtualización (Vmware)	4	4	4	3	15
DNS	4	3	4	2	13
Antena de Radio Enlace	3	3	3	2	11
Rutas y Cableado de Proveedores de Entrada	3	2	4	3	12
Servidor de BDD	3	5	4	3	15

Tabla 2.17. Valoración de Activos de Red de la Dirección

Valoración de Activos de Soporte Mecánico del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Enfriador de agua	3	4	3	3	13
Bomba centrífuga	1	2	3	2	8
Tanque de expansión	1	2	2	2	7
Filtro separador de aire	1	1	2	1	5
Unidad de Mantenimiento de Aire (UMA)	3	2	4	3	12
Válvula reguladora de flujo	1	3	2	1	7

Tabla 2.18. Valoración de Activos de Soporte Mecánico de la Dirección

Valoración de Activos de Sistema Eléctrico del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Transformador trifásico	1	4	4	3	12
Tablero de distribución principal	2	3	5	5	15
Módulo para Chiller	1	2	3	2	8
Tablero eléctrico para Servicios Generales	3	3	2	3	11
Transformador 220/127v para Servicios Generales	2	2	3	3	10
Tableros eléctricos para UPS IN – OUT	3	2	2	2	9
UPS 200 KVA	2	1	3	3	9
Baterías para UPS	1	2	3	2	8
Módulo para PDU	1	2	4	2	9
Tablero eléctrico para PDU	3	3	4	2	12
PDU	2	3	4	2	11

Tabla 2.19. Valoración de Activos de Sistema Eléctrico de la Dirección

Valoración de Activos de Vigilancia del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Cámara Interior	1	2	3	2	8
Grabador de Vídeo en la Red	4	2	4	3	13

Tabla 2.20. Valoración de Activos de Vigilancia de la Dirección

Valoración de Activos de Sistema Anti-Incendios del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Detectores y sensores	2	3	3	2	10
Panel de Incendio	4	3	5	3	15
Panel de Control de Extinción de Incendios	4	3	5	4	16
Tanque de gas Pentaflouretano Ecaro 25	3	5	5	4	17
Sirenas y Luces Estroboscópicas Blancas	1	1	2	1	5
Extintores manuales	1	1	2	1	5
Botones Manuales de Incendio	2	2	3	1	8

Tabla 2.21. Valoración de Activos de Sistema Anti-Incendios de la Dirección

Valoración de Activos de Control de Acceso del Data Center					
Activos	Parámetros				NI
	[C] Valor Confidencialidad	[I] Valor Integridad	[D] Valor Disponibilidad	[Costo] del Activo	
Cerradura de puerta de ingreso	2	1	1	1	5
Lectores de Proximidad	2	2	2	2	8
Lector biométrico de huella digital	2	3	3	1	9
Tarjetas inteligentes	2	3	1	1	7
Panel Maestro	4	5	4	3	16
Barra de pánico eléctrica y manual	1	2	1	1	5
Trap-door	2	2	2	2	8

Tabla 2.22. Valoración de Activos de Control de Acceso de la Dirección

La Figura 2.5 muestra un resumen sobre los resultados obtenidos del NI (nivel de importancia) de los activos a lo largo de las Tabla 2.15 a la Tabla 2.22

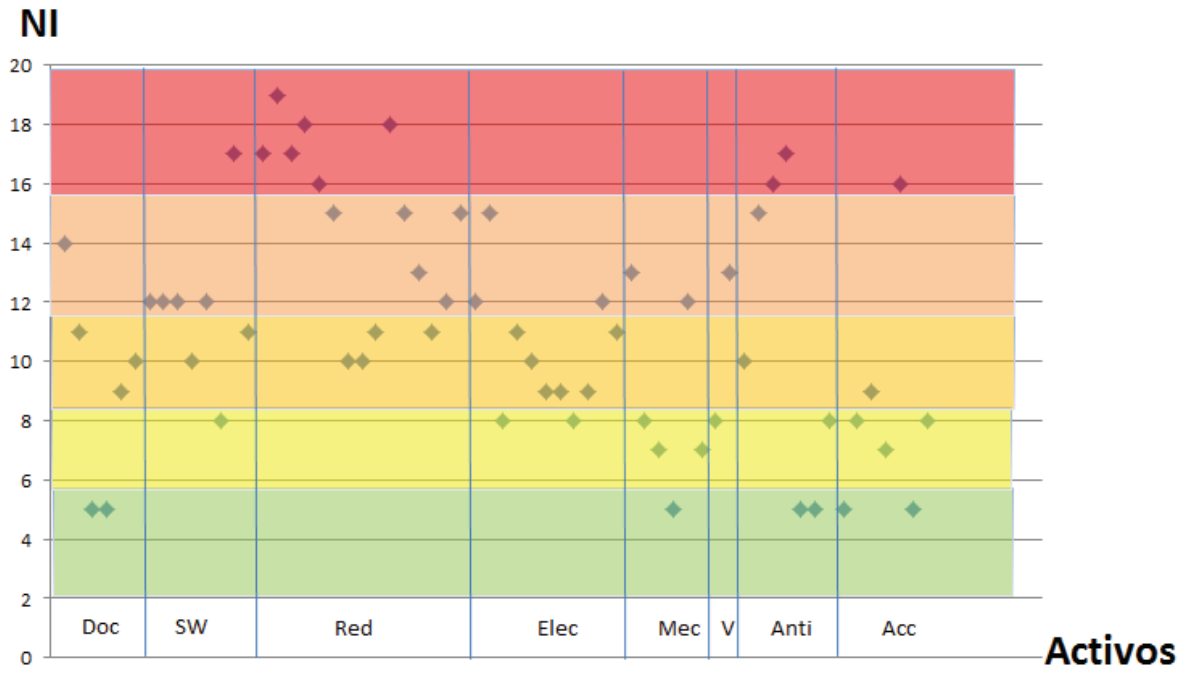

Figura 2.5. Relación de Densidad de NI respecto a los Activos

Las franjas horizontales de colores son de acuerdo a lo definido en la Tabla 2.9 sobre los rangos desde “no importante” (color verde) hasta “crítico” (color rojo). El resultado de esta figura, muestra que los activos críticos que requieren atención son más notables en los activos de red, un par en los activos del sistema anti-incendios y uno en los activos de control de acceso.

En el eje horizontal están identificados la categoría de los activos de acuerdo a lo definido en la clasificación de activos: Activos de Documentación (Doc), Activos de Software (SW), Activos de Red (Red), Activos del Sistema Eléctrico (Elec), Activos del Sistema Mecánico (Mec), Activos del Sistema de Video Vigilancia (V), Activos de Sistema Anti-incendios (Anti) y Activos de Control de Acceso (Acc).

También se puede apreciar los activos que son más y menos importantes para la entrega de servicios.

2.6.4 IDENTIFICACIÓN DE AMENAZAS

Para la identificación de amenazas se utilizó como base MAGERIT versión 3 que aporta varios métodos de clasificación de amenazas. Se ha hecho una recopilación de las posibles amenazas y se las ha clasificado en función al activo que podría afectar.

El resultado de la recopilación de amenazas y su relación con el tipo de activo (definido en la Clasificación de Activos en el punto 2.6.2.1) que requiere analizarse se observa en la **¡Error! No se encuentra el origen de la referencia.**

Dicha Tabla está creada en base a las sugerencias de tipo de amenazas de MAGERIT y los ejemplos de amenazas típicas que menciona la ISO/IEC 27005.

Es necesario recalcar que existirán criterios del analista en los que una amenaza, por su naturaleza, no requerirá ser analizada en ciertos activos.

Identificación de Amenazas			Para el Análisis de Riesgos							
			Tipo de Activo							
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Documentación	Software	Red	Soporte Eléctrico	Soporte Mecánico	Vigilancia	Anti-Incendios	Control de Acceso
Daño Físico	Agua	Daño por agua ocasionado por personal interno de forma accidental			X	X	X	X	X	X
		Daño por agua ocasionado por personal externo de forma accidental			X	X	X	X	X	X
		Daño por agua ocasionado por personal interno de forma intencionada			X	X	X	X	X	X
		Daño por agua ocasionado por personal externo de forma intencionada			X	X	X	X	X	X
		Fugas de agua ocasionadas por corrosión					X			
	Fuego - Explosión	Fuego ocasionado por personal interno de forma accidental	X			X	X			
		Fuego ocasionado por personal externo de forma accidental	X			X	X			
		Fuego ocasionado por personal interno de forma intencionada	X			X	X			
		Fuego ocasionado por personal externo de forma intencionada	X			X	X			
	Destrucción de equipo	Destrucción de respaldos / equipamiento por personal interno de forma accidental	X				X	X	X	X

Tabla 2.23. Identificación de Amenazas orientada al tipo de activo (1 de 5)

Identificación de Amenazas			Para el Análisis de Riesgos							
			Tipo de Activo							
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Documentación	Software	Red	Soporte Eléctrico	Soporte Mecánico	Vigilancia	Anti-Incendios	Control de Acceso
Daño Físico	Destrucción de equipo	Destrucción de respaldos / equipamiento por personal externo de forma accidental	X				X	X	X	X
		Destrucción de respaldos / equipamiento por personal interno de forma intencionada	X				X	X	X	X
		Destrucción de respaldos / equipamiento por personal externo de forma intencionada	X				X	X	X	X
	Sobrecarga Eléctrica / Cortocircuito	Cortocircuito en las baterías del panel ocasionado por personal interno de forma accidental								X
		Cortocircuito en las baterías del panel ocasionado por personal externo de forma accidental								X
		Cortocircuito en las baterías del panel ocasionado por personal interno de forma intencional								X
		Cortocircuito en las baterías del panel ocasionado por personal externo de forma intencional								X
	Polvo - Suciedad	Suciedad o polvo por falta de limpieza			X	X	X	X		X
Desastres Naturales	Fenómeno sísmico	Debilitamiento o colapso de las instalaciones	X		X	X		X	X	X
	Fenómeno volcánico	Ceniza en los mecanismos					X			
	Fenómeno meteorológico	Descarga eléctrica sobre equipamiento					X			
Pérdida de Servicios Esenciales	Fallo del sistema de climatización	Agotamiento del suministro de agua fría			X		X	X		
	Interrupción de alimentación eléctrica	Pérdida de la alimentación eléctrica	X		X		X	X	X	X
	Fallo en los servicios de comunicaciones	Corte del cableado de backbone						X	X	X
	Interrupción de suministros	Agotamiento de capacidad en disco para almacenaje						X		
		Daño del disco de almacenamiento						X		
		Finalización de licencia en software del servidor						X		
Compromiso de la Información	Ingeniería social	Acceso a la información confidencial / operativa de usuario, equipos o la institución	X	X	X	X	X	X	X	X

Tabla 2.23. Identificación de Amenazas orientada al tipo de activo (2 de 5)

Identificación de Amenazas			Para el Análisis de Riesgos							
			Tipo de Activo							
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Documentación	Software	Red	Soporte Eléctrico	Soporte Mecánico	Vigilancia	Anti-Incendios	Control de Acceso
Compromiso de la Información	Recuperación de medios descartados	Utilización de medios para ingreso no autorizado a la información	X		X					
	Divulgación de la información	Divulgación de la configuración o información por parte de personal interno de forma accidental		X	X		X			
		Divulgación de la configuración o información por parte de personal interno de forma intencional		X	X		X			
		Revelación por indiscreción del funcionamiento de equipos, sistemas o servicios a personas externas				X		X	X	X
	Escucha no autorizada	Intercepción no autorizada por parte de personal interno de forma intencional		X						
		Intercepción no autorizada por parte de personal externo de forma intencional		X						
	Robo de Información	Robo de configuración por parte de personal interno de forma intencional	X	X	X					
		Robo de configuración por parte de personal externo de forma intencional	X	X	X					
		Copia de archivos o configuraciones del servidor						X		
	Espionaje	Acceso no autorizado por parte de personal	X	X				X		
		Sniffer oculto por parte de personal interno			X					
		Sniffer oculto por parte de personal externo			X					
	Vulnerabilidades de configuración	Puertos habilitados			X					
	Intercepción de señal de red inalámbrica	Intercepción de señal de red inalámbrica por parte de personal interno de forma intencional			X					
		Intercepción de señal de red inalámbrica por parte de personal externo de forma intencional			X					
	Degradación de los soportes de almacenamiento de la información	Degradación de la documentación por el paso del tiempo	X							
Fallas Técnicas	Fallo del equipo	Avería física del equipo	X		X	X	X	X	X	X
	Mal funcionamiento de equipos	Respuesta inadecuada del funcionamiento del equipo				X	X	X	X	X
	Errores de mantenimiento	Mala realización de mantenimiento del equipo por impericia del personal			X	X	X	X	X	X

Tabla 2.23. Identificación de Amenazas orientada al tipo de activo (3 de 5)

Identificación de Amenazas			Para el Análisis de Riesgos							
			Tipo de Activo							
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Documentación	Software	Red	Soporte Eléctrico	Soporte Mecánico	Vigilancia	Anti-Incendios	Control de Acceso
Fallas Técnicas	Errores de mantenimiento	Mala realización de actualización de software por impericia del personal		X				X		
	Saturación del sistema de información	Saturación de red de video vigilancia						X		
		Caída del sistema por agotamiento de recursos		X	X					
		Denegación de servicio ocasionado por personal interno de forma intencional		X	X					
		Denegación de servicio ocasionado por personal externo de forma intencional		X	X					
Acciones no Autorizadas	Procesamiento ilegal de datos	Manipulación de los registros de actividad o contenido de forma deliberada por personal interno	X	X	X					
		Manipulación de los registros de actividad o contenido de forma deliberada por personal externo	X	X	X					
		Eliminación de información por parte de personal interno de forma intencional	X	X	X			X		
		Eliminación de información por parte de personal externo de forma intencional	X	X	X			X		
	Uso no autorizado de equipos	Activación intencional de los equipos por personal interno				X	X			
		Activación intencional de los equipos por personal externo				X	X			
	Uso de software falsificado o copiado	Uso de cracks para falsificar licencias de software propietario			X					
	Difusión de Software dañino	Utilización de código erróneo o malicioso		X						
	Manipulación de Software	Mala configuración del servicio de forma deliberada		X	X					
		Modificación por parte de personal interno de forma deliberada		X	X			X		
		Modificación por parte de personal externo de forma deliberada		X	X			X		
	Manipulación de los equipos	Desconexión intencional por personal interno			X	X	X	X	X	X
		Desconexión intencional por personal externo			X	X	X	X	X	X
		Modificación intencional en el funcionamiento por parte de personal interno				X	X		X	
		Modificación intencional en el funcionamiento por parte de personal externo				X	X		X	

Tabla 2.23. Identificación de Amenazas orientada al tipo de activo (4 de 5)

Identificación de Amenazas			Para el Análisis de Riesgos							
			Tipo de Activo							
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Documentación	Software	Red	Soporte Eléctrico	Soporte Mecánico	Vigilancia	Anti-Incendios	Control de Acceso
Compromiso de Funciones	Error de uso	Desconexión accidental por parte de personal interno			X	X	X	X	X	X
		Desconexión accidental por parte de personal externo			X	X	X	X	X	X
		Mal manejo del equipo / servicio por impericia del personal interno		X		X	X	X	X	X
		Mal manejo del equipo / servicio por impericia del personal externo			X	X	X	X	X	X
		Mala configuración del equipo / servicio por impericia de los administradores		X				X	X	
		Error de monitoreo por impericia del personal interno		X						
		Activación accidental de los equipos / sistemas por parte de personal interno					X			
		Activación accidental de los equipos / sistemas por parte de personal externo					X			
		Borrado accidental de la información por parte de personal interno						X		
		Borrado accidental de la información por parte de personal externo						X		
	Indisponibilidad del personal	Ausencia accidental o intencional del puesto de trabajo	X	X	X	X	X	X	X	X
	Suplantación de identidad	Ingreso de personal interno no autorizado	X	X	X	X	X	X	X	X
		Ingreso de personal externo no autorizado	X	X	X	X	X	X	X	X
		Acceso a la información del servidor por parte de personal no autorizado						X		
	Abuso de Derechos	Abuso de privilegios de acceso	X	X	X	X	X	X	X	X
	Ocupación enemiga	Pérdida de control sobre el manejo del servicio / equipo que está en ejecución	X	X	X	X	X	X	X	X
	Deficiencia en la organización	Ingreso de personal no calificado o nocivo				X	X	X	X	X
	Extorsión	Presión sobre personal interno para realizar daños sobre el servicio / equipo que está en ejecución	X	X	X	X	X	X	X	X

Tabla 2.23. Identificación de Amenazas orientada al tipo de activo (5 de 5)

[20] [22]

2.6.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS

En base a la Tabla 2. y todos los activos valorados en las Tabla 2.15 hasta la Tabla 2.22, en la presente sección se realiza el Análisis y Evaluación de Riesgos de cada activo.

Tomando los ejemplos del punto 2.6.3.1 como punto de partida, se procede a mostrar el procedimiento llevado a cabo para el análisis, valoración y evaluación de riesgos considerando una amenaza específica según la Tabla 2..

2.6.5.1 Ejemplo 1 de Análisis y Evaluación de Riesgos para una Amenaza Específica

El activo analizado pertenece a la categoría Software, y se denomina Sistema Operativo de los Servidores.

Identificación de la Amenaza:

- **Tipo de Amenaza:** Acciones no autorizadas.
- **Nombre de la Amenaza:** Procesamiento ilegal de datos.
- **Descripción de la Amenaza:** Eliminación de la configuración.
- **Involucrado:** ocasionado por personal externo de forma deliberada.

Controles existentes: En base a la información obtenida en el Anexo B se conoce que existe control de acceso a la ubicación física de los servidores. Los servidores se encuentran en el Data Center por lo que su acceso es bajo autorización previa y con presencia del Jefe de Área de Infraestructura. Existe un ambiente de pruebas en el que se hacen los cambios en una simulación utilizando la configuración actual con la que operan los servidores. El acceso lógico es administrado por el Jefe del Área de Infraestructura.

Vulnerabilidad: Posible fallo total o parcial del ambiente de pruebas, justamente cuando se requiera recuperar la configuración del servidor.

Nivel de Importancia: Por las características analizadas del activo, se tiene que es un activo cuyo nivel de importancia es “crítico” en la entrega de servicios en el caso que fallara. Esto será considerado para en la categorización de los impactos.

Impacto sobre clientes afectados [$I_{Clientes}$]: Los clientes no podrían acceder a servicios o aplicaciones que provienen del servidor. Las actividades de los clientes podrían verse detenidas parcial o totalmente hasta la reanudación del servidor. Una gran cantidad de clientes se vería afectada y notarían la falta de acceso a los servicios.

Por las posibles afectaciones mencionadas y según la Tabla 2.11, se categoriza a este impacto como *catastrófico* y se le asigna con el valor 5.

Impacto de recuperación de servicios [I_{Recup}]: Si se perdieran las salvaguardias del ambiente de pruebas y el guardado de una configuración de respaldo, el tiempo que requeriría reponerlas sería notorio, lo que podría afectar las actividades de la institución; además que se necesitaría la reinstalación del sistema operativo en el servidor. El cese de actividades que requieren acceso o uso del servidor, dependerá del tiempo que demore reinstalar o configurar nuevamente las características de dicho servidor.

Por las posibilidades mencionadas y según la Tabla 2.12, se categoriza a este impacto como *catastrófico* con el valor 5.

Probabilidad de ocurrencia [Prob]: Existe un ambiente de pruebas actualizado y una configuración que salvaguarda cada vez que se requieran hacer cambios en la configuración del software de servidores. Existen restricciones de acceso tanto físico (acceso restringido a la institución, control de acceso al data center, presencia necesaria del Jefe del Área de Infraestructura ante actividades de terceros sobre los servidores o en la configuración de su sistema operativo) como lógico (firewall, administración de cuentas de acceso remotas a cargo del Jefe de Infraestructura, antispam, antivirus) a los servidores.

Por las condiciones mencionadas de control de acceso y salvaguardias existentes, es más probable que se intente hacer la eliminación de la configuración por parte de terceros por medio de acceso lógico. Además, las amenazas que suelen ser constantes que provienen de la Internet (todo software malicioso) se pueden considerar como parte del intento que podría eliminar la configuración del sistema operativo de servidores.

Por las condiciones, salvaguardias y probabilidades expuestas y según la Tabla 2.10 se considera que es un evento de *moderadamente probable* y se asigna el valor de 2.

Para determinar el valor del riesgo, se procede con la fórmula de su cálculo en el punto 2.6.1.4

Riesgo = 5 * 5 * 2

Riesgo = 50

Según este valor de Riesgo, se puede comparar con la Tabla 2.13, con lo que se define que el riesgo está en el rango de “alto” en impacto y recuperación de servicios si esta amenaza ocurriese.

Dado que el riesgo está en el rango “alto”, el tratamiento de esta amenaza será de “Reducción” según la Tabla 2.14

Así concluye el procedimiento de análisis para una amenaza específica.

2.6.5.2 Ejemplo 2 de Análisis y Evaluación de Riesgos para una Amenaza Específica

El activo analizado pertenece a la categoría Red, y se denomina Switch de Core HP A5500.

Identificación de la Amenaza:

- **Tipo de Amenaza:** Compromiso de funciones.

- **Nombre de la Amenaza:** Deficiencia en la organización.
- **Descripción de la Amenaza:** Ingreso de personal no calificado o nocivo.
- **Involucrado:** personal interno o externo a la institución.

Controles existentes: En base a la información obtenida en el Anexo B se conoce que existe control de acceso a la ubicación física del Switch de Core. El switch se encuentra en el Data Center por lo que su acceso es bajo autorización previa y con presencia del Jefe de Área de Infraestructura. El Jefe del Área de Infraestructura es el responsable de autorizar el ingreso al data center. Existe un switch idéntico y con la misma configuración que posee el switch activo en caso que se requiera reemplazarlo. Existe guardianía en la institución por lo que se registra el acceso a todo el personal ajeno a la institución; se puede restringir el acceso en caso que se lo requiera pertinente.

Vulnerabilidad: Ingreso forzado de personal no calificado o nocivo en la ubicación del switch de core y provocar daños sobre dicho switch.

Nivel de Importancia: Por las características analizadas del activo, se tiene que es un activo cuyo nivel de importancia es “crítico” en la entrega de servicios en el caso que fallara. Esto será considerado para en la categorización de los impactos.

Impacto sobre clientes afectados [$I_{Clientes}$]: Los clientes no podrían acceder a servicios o aplicaciones a través de la intranet. Servicios, equipos y clientes podrían estar incomunicados. Las actividades de los clientes podrían verse detenidas parcial o totalmente hasta la reanudación o cambio del switch del servidor. Una gran cantidad de clientes se vería afectada y notarían la falta de acceso a los servicios.

Por las posibles afectaciones mencionadas y según la Tabla 2.11, se categoriza a este impacto como *catastrófico* y se le asigna con el valor 5.

Impacto de recuperación de servicios [I_{Recup}]: A pesar que existe un equipo que salvaguarda al switch de core para reemplazarlo, en el caso que una persona no calificada o nociva ingresara al data center, donde se ubican ambos equipos switch, y los dañara, el daño sería notorio para los clientes. La reanudación de la

comunicación entre equipos dependería el tiempo que se demore en realizar el reemplazo de switch o en el peor de los casos hasta obtener un nuevo switch en caso que ambos hayan sido afectados.

Por las posibles afectaciones mencionadas y según la Tabla 2.12, se categoriza a este impacto como *catastrófico* con el valor 5.

Probabilidad de ocurrencia [Prob]: La verificación de antecedentes del nuevo personal contratado es muy retrasado, por lo que los resultados podrían estar listos luego que el personal se encuentra trabajando. El mantenimiento de proveedores requiere permisos de acceso al Data Center, tanto de manera física como lógica. El soporte por parte de terceros, cuando lo requiere, requiere permisos de acceso autorizados por el Jefe del Área de Infraestructura. A pesar que se requieren privilegios de acceso, no se puede acertar las intenciones de todo el personal que ingrese en el Data Center, lugar donde se encuentra el switch.

Por las condiciones mencionadas de control de acceso y la necesidad de terceros, cuando se los requiere, para hacer mantenimiento o cambios en la Dirección; los permisos y privilegios que está a cargo el Jefe del Área de Infraestructura, se puede considerar que hay involucrados, externos a la institución, que requerirán privilegios en la ubicación y acceso lógico del switch.

Por las condiciones, salvaguardias y probabilidades expuestas y según la Tabla 2.10 se considera que es un evento de *moderadamente probable* y se asigna el valor de 2.

Para determinar el valor del riesgo, se procede con la fórmula de su cálculo en el punto 2.6.1.4

Riesgo = 5 * 5 * 4

Riesgo = 50

Según este valor de Riesgo, se puede comparar con la Tabla 2.13, con lo que se define que el riesgo está en el rango de “crítico” en impacto y recuperación de servicios si esta amenaza ocurriese.

Dado que el riesgo está en el rango “crítico”, el tratamiento de esta amenaza será de “Reducción” según la Tabla 2.14, por lo que también se puede llegar al traslado del riesgo en caso que se requiera necesario, según lo mencionado en 2.6.1.5

Así concluye el procedimiento de análisis para una amenaza específica.

2.6.5.3 Ejemplo 3 de Análisis y Evaluación de Riesgos para una Amenaza Específica

El activo analizado pertenece a la categoría *Control de Acceso*, y se denomina *Lector Biométrico de Huella Digital*.

Identificación de la Amenaza:

- **Tipo de Amenaza:** Compromiso de funciones.
- **Nombre de la Amenaza:** Extorsión.
- **Descripción de la Amenaza:** Presión sobre personal para realizar daños sobre el sistema de control de acceso.
- **Involucrado:** ocasionado por personal interno o externo bajo presión de alguien más.

Controles existentes: En base a la información obtenida en el Anexo B se conoce que existe control de acceso a la ubicación del Data Center. Existe guardianía en la institución que permite o no el ingreso a visitantes.

Vulnerabilidad: Posible fallo total o parcial del ambiente de pruebas, justamente cuando se requiera recuperar la configuración del servidor.

Nivel de Importancia: Por las características analizadas del activo, se tiene que es un activo cuyo nivel de importancia es “importante” en la entrega de servicios en el caso que fallara. Esto será considerado para en la categorización de los impactos.

Impacto sobre clientes afectados [$I_{Clientes}$]: Los clientes no podrían acceder a servicios o aplicaciones que provienen del servidor. Las actividades de los clientes podrían verse detenidas parcial o totalmente hasta la reanudación del servidor. Una gran cantidad de clientes se vería afectada y notarían la falta de acceso a los servicios.

Por las posibilidades mencionadas y según la Tabla 2.11, se categoriza a este impacto como *catastrófico* y se le asigna con el valor 3.

Impacto de recuperación de servicios [I_{Recup}]: Si se perdieran las salvaguardias del ambiente de pruebas y el guardado de una configuración de respaldo, el tiempo que requeriría reponerlas sería notorio, lo que podría afectar las actividades de la institución; además que se necesitaría la reinstalación del sistema operativo en el servidor. El cese de actividades que requieren acceso o uso del servidor, dependerá del tiempo que demore reinstalar o configurar nuevamente las características de dicho servidor.

Por las posibilidades mencionadas y según la Tabla 2.12, se categoriza a este impacto como *catastrófico* con el valor 5.

Probabilidad de ocurrencia [Prob]: Existe un ambiente de pruebas actualizado y una configuración que salvaguarda cada vez que se requieran hacer cambios en la configuración del software de servidores. Existen restricciones de acceso tanto físico (acceso restringido a la institución, control de acceso al data center, presencia necesaria del Jefe del Área de Infraestructura ante actividades de terceros sobre los servidores o en la configuración de su sistema operativo) como lógico (firewall, administración de cuentas de acceso remotas a cargo del Jefe de Infraestructura, antispam, antivirus) a los servidores.

Por las condiciones mencionadas de control de acceso y salvaguardias existentes, es más probable que se intente hacer la eliminación de la configuración por parte de terceros por medio de acceso lógico. Además, las amenazas que suelen ser constantes que provienen de la Internet (todo software malicioso) se pueden

considerar como parte del intento que podría eliminar la configuración del sistema operativo de servidores.

Por las condiciones, salvaguardias y probabilidades expuestas y según la Tabla 2.10 se considera que es un evento de *moderadamente probable* y se asigna el valor de 2.

Para determinar el valor del riesgo, se procede con la fórmula de su cálculo en el punto 2.6.1.4

Riesgo = 3 * 5 * 1

Riesgo = 15

Según este valor de Riesgo, se puede comparar con la Tabla 2.13, con lo que se define que el riesgo está en el rango de “alto” en impacto y recuperación de servicios si esta amenaza ocurriese.

Dado que el riesgo está en el rango “alto”, el tratamiento de esta amenaza será de “Reducción” según la Tabla 2.14

Así concluye el procedimiento de análisis para una amenaza específica.

En la **¡Error! No se encuentra el origen de la referencia.** a la Tabla 2.26, se bservan los resultados del análisis y evaluación de riesgos de los tres ejemplos de muestra definidos en sección 2.6.3.1. Esta actividad se hace de acuerdo a la Tabla 2.23 en la que se definen las amenazas que serán analizadas de acuerdo a la clasificación otorgada al activo.

La compilación de todo el análisis y evaluación de riesgos para el resto de activos, se puede observar en el Anexo C.

Sistema Operativo de Servidores									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Compromiso de la Información	Ingeniería social	Acceso a la información	Existen políticas sobre la restricción de acceso a personal interno y externo. Se requiere al personal no declarar información personal del uso de servicios y sus credenciales a terceros, dentro y fuera de la institución.	Negligencia del personal en revelar o entregar información	Pérdida de la confidencialidad e integridad de la información gestionada por el sistema operativo	4	4	3	48
	Divulgación de la información	Divulgación de la configuración por parte de personal interno de forma accidental	Existen políticas que mencionan sobre el manejo de la información dentro de la institución y sobre las sanciones en caso que lo requiera.	Posible impericia del personal al dejar información personal confidencial escrita en sus puestos de trabajo.	Pérdida de confidencialidad de la información gestionada por el sistema operativo	5	2	2	20
		Divulgación de la configuración por parte de personal interno de forma deliberada				4	4	1	16
	Robo de Información	Robo por parte de personal interno de forma deliberada	Existen políticas en el control de acceso al personal interno y externo; Asignación de privilegios para configuración y acceso; Se realiza comprobación de identidad y de pase de acceso otorgado a personal externo en Recepción del Ministerio.	No se hace un exhaustivo chequeo de pertenencias en la entrada y salida en la Recepción y al ingreso de la Dirección.	Pérdida de confidencialidad y disponibilidad de la información gestionada por el sistema operativo	5	5	1	25
		Robo por parte de personal externo de forma deliberada				5	3	2	30
	Espionaje	Acceso no autorizado por parte de personal	Se restringe el acceso a personal no autorizado.	Falta de verificación de credenciales y pases de acceso.	Problemas de confidencialidad, integridad y disponibilidad de la información gestionada por el sistema operativo	5	5	3	75
Fallas Técnicas	Errores de mantenimiento	Mala realización de actualización de software por impericia del personal	Existen responsabilidades al personal para el manejo y configuración de servicios; Ambiente de pruebas	Errores fortuitos durante la manipulación y configuración del servicio Antivirus.	Pérdida parcial o total de la información gestionada por el sistema operativo	5	5	2	50

Tabla 2.24. Análisis y Evaluación de Riesgos de Sistema Operativo de servidores (1 de 3)

Sistema Operativo de Servidores									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Fallas Técnicas	Saturación del sistema de información	Caída del sistema por agotamiento de recursos	Existen responsabilidades al personal para la gestión de incidentes; se tiene una herramienta de monitoreo	No se realiza un monitoreo adecuado del servicio de la red; Insuficiente uso de la herramienta de monitoreo; Algunos eventos son atendidos sólo cuando los usuarios reportan el incidente.	Pérdida parcial o total de la información gestionada por el sistema operativo	4	5	2	40
		Denegación de servicio ocasionado por personal interno de forma deliberada				4	3	1	12
		Denegación de servicio ocasionado por personal externo de forma deliberada				5	5	3	75
Acciones no Autorizadas	Procesamiento ilegal de datos	Manipulación de los registros de actividad (logs) de forma deliberada por parte de personal interno	Se realizan respaldos de registros semanales	Pérdida o daño irreparable en el ambiente de pruebas; Pérdida parcial o total de los registros	Problemas de confidencialidad, integridad y disponibilidad de la información gestionada por el sistema operativo	3	3	2	18
		Manipulación de los registros de actividad (logs) de forma deliberada por parte de personal externo				5	3	2	30
		Eliminación de la configuración por personal interno de forma deliberada	Existe un ambiente de pruebas y copia de configuración del sistema activo	Pérdida o daño irreparable en el ambiente de pruebas	Problemas de disponibilidad, confidencialidad e integridad de la información gestionada por el sistema operativo	4	3	2	24
		Eliminación de la configuración por personal externo de forma deliberada				5	5	2	50
	Manipulación de Software	Mala configuración del servicio de forma deliberada	Se realizan pruebas previas antes de poner en producción la actualización de servicios; Privilegios de acceso	Fallo de configuración y puesta en producción imprudencial.	Problemas de confidencialidad, integridad y disponibilidad de la información gestionada por el sistema operativo	4	5	2	40
		Modificación por parte de personal interno de forma deliberada		Fallo en registro de actividades y en ejecución de control de acceso lógico.	Problemas de disponibilidad de la información gestionada por el sistema operativo	4	5	2	40
		Modificación por parte de personal externo de forma deliberada				4	5	2	40

Tabla 2.24. Análisis y Evaluación de Riesgos de Sistema Operativo de servidores (2 de 3)

Sistema Operativo de Servidores									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Compromiso de Funciones	Error de uso	Mala administración por impericia del personal interno (administrador)	Se realizan pruebas previas antes de poner en producción la actualización de servicios; Privilegios de acceso	Fallo de configuración y puesta en producción imprudencial.	Pérdida parcial o total de la información gestionada por el sistema operativo	5	3	2	30
		Mala configuración por impericia del personal interno (administrador)		Fallo en registro de actividades y en ejecución de control de acceso lógico; Insuficiente uso de la herramienta de monitoreo	Problemas de confidencialidad, integridad y disponibilidad de la información gestionada por el sistema operativo	4	5	2	40
		Error de monitoreo por impericia del personal interno			Pérdida parcial o total de la información gestionada por el sistema operativo	4	3	1	12
	Indisponibilidad del personal	Ausencia accidental o intencional del puesto de trabajo	Se dispone de un grupo de trabajo en el que al menos uno de los integrantes estará disponible.	Falta de disponibilidad de personal en situaciones muy particulares.	Tiempos altos para la solución de incidencias	4	2	1	8
	Suplantación de identidad	Ingreso de personal interno no autorizado al sistema operativo de los servidores	Existen políticas para el acceso a personal tanto interno como externo; Asignación de privilegios	Falta de control en el caso de pérdida de credenciales portables.	Pérdida parcial o total de la información gestionada por el sistema operativo	2	5	2	20
		Ingreso de personal externo no autorizado al sistema operativo de los servidores				4	2	1	8
	Abuso de Derechos	Abuso de privilegios de acceso	Existen privilegios de acceso y existen políticas de manejo de documentación	Negligencia del personal en revelar o entregar información; acciones malintencionadas del personal	Problemas de confidencialidad, integridad y disponibilidad de la información gestionada por el sistema operativo	4	5	2	40
	Ocupación enemiga	Pérdida de control sobre el manejo del servicio de sistema operativo de los servidores	Se tiene personal de guardianía en la institución	Falla en el cumplimiento de verificación de credenciales y permisos de acceso	Pérdida parcial o total de la información gestionada por el sistema operativo	2	2	3	12
	Extorsión	Presión sobre personal interno para realizar daños sobre el sistema operativo	Entre las políticas internas se menciona sobre la ética profesional y el reporte de incidentes.	Amenaza física o verbal sobre el personal.	Pérdida parcial o total de la información gestionada por el sistema operativo	4	4	1	16

Tabla 2.24. Análisis y Evaluación de Riesgos de Sistema Operativo de servidores (3 de 3)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Daño Físico	Agua	Daño por agua ocasionado por personal interno de forma accidental	Control de acceso biométrico al Data Center; revisión semestral de sistema de aire acondicionado por el proveedor	Incumplimiento en el mantenimiento programado	Daño del switch de core. Reemplazo manual por el de respaldo	2	4	2	16
		Daño por agua ocasionado por personal interno de forma deliberada		Falta de políticas de comportamiento de personal en el Data Center		2	4	2	16
		Daño por agua ocasionado por personal externo de forma accidental		Intento forzado de acceso al Data Center a personal no autorizado		2	4	1	8
		Daño por agua ocasionado por personal externo de forma deliberada				2	4	1	8
	Destrucción de equipo	Destrucción de equipo por personal interno de forma accidental	Existen contratos y garantías sobre los equipos, que incluyen soporte y mantenimiento del proveedor	Error de actividades del personal a cargo del mantenimiento	Daño del switch de core. Reemplazo manual por el de respaldo	2	4	2	16
		Destrucción de equipo por personal interno de forma deliberada		Falta de registros de actividades del personal		2	4	2	16
		Destrucción de equipo por personal externo de forma accidental		Intento forzado de acceso al Data Center a personal no autorizado		2	4	1	8
		Destrucción de equipo por personal externo de forma deliberada				2	4	1	8
	Polvo / Suciedad	Suciedad o polvo por insuficiente limpieza en el cuarto de cómputo	Se hace limpieza de polvo y del entorno frecuentemente	Insuficiente mantenimiento y limpieza sobre los equipos	Inhibición de un switch de core. Soporte técnico y reemplazo manual por el de respaldo	2	4	2	16
Desastres Naturales	Fenómenos sísmicos	Debilitamiento o colapso de las instalaciones del Data Center	El Data Center no tiene certificación del edificio para soportar terremotos.	El edificio de la institución está construido con estándares mínimos	Daño del switch de core. Pérdida de los servicios de red del Data Center	2	5	2	20

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (1 de 6)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Pérdida de Servicios Esenciales	Fallo del sistema de climatización	Agotamiento del suministro de agua fría	Existen políticas de comportamiento sobre ser pertinente en el revelar información de la institución dentro y fuera de ésta	Negligencia del personal en revelar o entregar información	Caída del switch de core. Pérdida de los servicios de red del Data Center	2	4	3	24
	Interrupción de alimentación eléctrica	Pérdida de la alimentación eléctrica en el Data Center	Se tiene un soporte de UPS para tiempo de respaldo mínimo. Existen protecciones eléctricas de entrada	Falta de políticas y respaldos fiables sobre corte de energía eléctrica		2	5	2	20
	Interrupción de suministros	Falla de actividad del switch	Existe un respaldo de cambio manual	Falta de políticas respecto a mantenimientos		2	5	2	20
Compromiso de la Información	Ingeniería social	Acceso a la información	Existen políticas de comportamiento sobre ser pertinente en el revelar información de la institución dentro y fuera de ésta	Negligencia del personal en revelar o entregar información	Pérdida de la confidencialidad e integridad del sistema de red	5	2	4	40
	Divulgación de la Información	Divulgación de información por parte de personal interno de forma accidental	Existen políticas de comportamiento sobre ser pertinente en el revelar información de la institución dentro y fuera de ésta	Negligencia del personal en revelar o entregar información	Pérdida de la confidencialidad e integridad del sistema de red	5	3	4	60
		Divulgación de información por parte de personal interno de forma deliberada				5	3	3	45
	Recuperación de medios descartados	Utilización de medios para ingreso no autorizado a la información	No se tiene políticas de control	Falta de políticas de desecho de información obsoleta	Pérdida de integridad y confidencialidad de la información de red del Data Center.	5	2	2	20
	Vulnerabilidades de la configuración	Puertos habilitados	No existe una adecuada distribución de puertos habilitados en la red del Data Center	Falta de políticas sobre seguridades en la red del Data Center	Tráfico malicioso podría ingresar y comprometer los servicios de información; Acceso a información confidencial	4	5	2	40

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (2 de 6)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Compromiso de la Información	Robo de Información	Robo de la configuración por parte de personal interno de forma deliberada	Existen controles para el ingreso de dispositivos electrónicos como teléfonos inteligentes, flash memory, entre otros	Falla en el cumplimiento de políticas de ingreso de dispositivos electrónicos; envío de correos a personal no autorizado	Pérdida de la confidencialidad en los servicios ofrecidos en el Data Center	5	3	2	30
		Robo de la configuración por parte de personal externo de forma deliberada	Existen controles para el ingreso de dispositivos electrónicos como teléfonos inteligentes, flash memory, entre otros; Existen controles de ingreso en la guardianía de la institución	Verificación de dispositivos a personal externo mínimo o parcial; envío de correos a personal no autorizado		5	3	1	15
	Intercepción de señal de red inalámbrica	Intercepción de señal de red inalámbrica por parte de personal interno de forma deliberada	Existen medidas de seguridad dados por el proveedor de las antenas	Falta de políticas de seguridad de red inalámbrica	Pérdida de la confidencialidad en los servicios ofrecidos en el Data Center	5	4	1	20
		Intercepción de señal de red inalámbrica por parte de personal externo de forma deliberada	Existen medidas de seguridad dados por el proveedor de las antenas	Falla en la eliminación de equipos registrados temporalmente		5	4	1	20
	Espionaje	Acceso a la información por personal no autorizado	Existen privilegios de acceso y existen políticas de manejo de documentación	Falta de cumplimiento de políticas de control de acceso	Pérdida de la confidencialidad en los servicios ofrecidos en el Data Center	5	3	2	30
		Sniffer oculto por parte de personal interno	Existe un reglamento que menciona el compromiso del personal sobre la manipulación de la información	Negligencia del personal en revelar o entregar información; acciones malintencionadas del personal		5	4	2	40
		Sniffer oculto por parte de personal externo	Existen medidas de seguridad con encriptación en la comunicación de la intranet	Falta de verificación de facilidad de captura de señal inalámbrica		5	4	1	20
Fallas Técnicas	Fallo del equipo	Avería física del equipo	Mantenimiento y soporte de proveedores y uso de garantías	Desperfecto durante su uso	Caída de un switch de core; Reemplazo manual del respaldo	2	4	3	24

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (3 de 6)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Fallas Técnicas	Mal funcionamiento de equipos	Respuesta inadecuada en el funcionamiento normal del Switch de Core Nexus 7000	Mantenimiento y soporte de proveedores y uso de garantías	Insuficiente mantenimiento	Caída de un switch de core; Reemplazo manual del respaldo	2	4	4	32
	Errores de mantenimiento	Mala realización del mantenimiento del equipo por impericia del personal	Existen medidas de prueba de SW previa a su modificación	Pérdida o daño irreparable en el ambiente de pruebas	Caída de un switch de core; Reemplazo manual del respaldo	2	4	4	32
		Mala realización de actualización de software por impericia del personal	Existen medidas de downgrade y de pruebas de SW previa a su instalación	Pérdida o daño irreparable en el ambiente de pruebas	Problemas de confidencialidad, integridad y disponibilidad servicios que provienen del Data Center	4	5	3	60
	Saturación del sistema de información	Caída del sistema por agotamiento de recursos	Se tiene de una herramienta de monitoreo	No es utilizada la herramienta de monitoreo de manera adecuada y eficaz	Caída del switch de core. Pérdida de los servicios de red del Data Center	2	5	3	30
		Denegación de servicio de Switch de Core Nexus 7000 de forma deliberada				2	5	3	30
Acciones no Autorizadas	Procesamiento ilegal de datos	Manipulación de los registros de actividad (logs) de forma deliberada por parte de personal interno	Se realizan respaldos de registros semanales	Pérdida o daño irreparable en el ambiente de pruebas	Problemas de confidencialidad e integridad en los servicios ofrecidos en el Data Center	4	3	3	36
		Manipulación de los registros de actividad (logs) de forma deliberada por parte de personal externo				4	3	1	12
		Eliminación de la configuración por parte de personal interno de forma deliberada	Existe un ambiente de pruebas y copia de configuración del sistema activo	Pérdida o daño irreparable en el ambiente de pruebas	Pérdida de los servicios de red del Data Center	3	5	4	60
		Eliminación de la configuración por parte de personal externo de forma deliberada				3	5	2	30
	Uso de software falsificado o copiado	Utilización de cracks para falsificar licencias de software propietario	Existe un reglamento con el compromiso del personal en manipular de la información	Intento forzado del personal de instalar SW sin autorización	Violación de propiedad intelectual. Afectación de los servicios de red del Data Center	4	5	3	60

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (4 de 6)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Acciones no Autorizadas	Manipulación de Software	Mala configuración de forma deliberada	Existen privilegios de acceso y existen políticas de manejo de documentación	Negligencia del personal en revelar o entregar información; acciones malintencionadas del personal	Problemas de integridad y disponibilidad en los servicios ofrecidos en el Data Center	2	5	2	20
		Modificación de configuración por parte de personal interno de forma deliberada	Asignación de responsabilidades respecto a la modificación de configuración; reglamento vigente sobre el compromiso del personal; respaldos de configuración	Negligencia del personal en revelar o entregar información; acciones malintencionadas del personal	Problemas de confidencialidad, integridad y disponibilidad en los servicios ofrecidos en el Data Center	3	5	4	60
		Modificación de configuración por parte de personal externo de forma deliberada	Contratos con compromiso de actividades para terceros; respaldos guardados de configuración activa	Incumplimiento en el contrato de personal externo		3	5	2	30
	Manipulación de los equipos	Desconexión por personal interno	Existen privilegios de acceso; reglamento de compromiso de uso de servicios	Acciones malintencionadas del personal	Caída de un switch de core; Reemplazo manual del respaldo	2	4	2	16
		Desconexión por personal externo	Contratos con compromiso de actividades para terceros; respaldos guardados de configuración	Incumplimiento en el contrato de personal externo		2	4	1	8
Compromiso de Funciones	Error de uso	Desconexión accidental por personal interno	Contratos con compromiso de actividades para terceros; respaldos guardados de configuración; capacitación previa a su uso	Negligencia en procesos de mantenimiento	Caída de un switch de core; Reemplazo manual del respaldo	2	4	4	32
		Desconexión accidental por personal externo		Incumplimiento de contrato		2	4	3	24
		Mal manejo por impericia del personal interno	Existe un reglamento que menciona el compromiso del personal sobre la manipulación de la información; compromiso de actividades en contrato de trabajo	Falta de procesos para el buen uso de activos	Caída de un switch de core; Reemplazo manual del respaldo	2	4	4	32

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (5 de 6)

Switch de Core HP A5500									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Compromiso de Funciones	Error de uso	Mal manejo por impericia del personal externo	Contratos con compromiso de actividades para terceros; respaldos guardados de configuración	Falta de procesos para el buen uso de activos	Caída de un switch de core; Reemplazo manual del respaldo	2	4	2	16
	Indisponibilidad del personal	Ausencia accidental o intencional del puesto de trabajo	Existen funciones designadas y responsabilidades sobre la presencia de personal para soporte	Casos particulares de falta de soporte o presencia de personal	Tiempos altos para la solución de incidencias	2	4	4	32
	Suplantación de identidad	Ingreso de personal interno no autorizado	Existe control de acceso de personal y privilegios de acceso a los equipos y servicios	Intento forzado de acceder a sesiones de usuario	Caída del switch de core. Pérdida de los servicios de red del Data Center	5	5	3	75
		Ingreso de personal externo no autorizado				4	5	2	40
	Abuso de derechos	Ingreso de personal interno no autorizado	Existen privilegios de acceso y existen políticas de manejo de documentación	Negligencia del personal en revelar o entregar información; acciones malintencionadas del personal	Caída del switch de core. Pérdida de los servicios de red del Data Center	5	5	3	75
	Ocupación enemiga	Pérdida de control sobre el manejo del switch de core	Se tiene personal de guardianía en la institución	Falta de procedimientos de seguridad en caso de invasión	Daño del switch de core. Pérdida de los servicios de red del Data Center	4	5	1	20
	Deficiencia en la organización	Ingreso de personal no calificado o nocivo	Se tiene personal de guardianía en la institución; existe un proceso de evaluación y calificación para el personal nuevo	Falta de procesos de verificación de antecedentes en la contratación de personal; Falta de capacitación	Daño del switch de core. Pérdida de los servicios de red del Data Center	5	5	4	100
	Extorsión	Presión sobre personal interno para realizar daños sobre los activos	Existen políticas sobre el reporte de incidentes	Amenaza física o verbal sobre el personal.	Daño del switch de core. Pérdida de los servicios de red del Data Center	4	5	1	20

Tabla 2.25. Análisis y Evaluación de Riesgos de Switch de CORE HPA5500 (6 de 6)

Lector biométrico de huella digital									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Daño Físico	Agua	Daño por agua ocasionado por personal interno de forma accidental	Ambiente cerrado, privilegios de acceso al ambiente de trabajo	Negligencia de comportamiento en actividades laborales	Daño del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	1	4	2	8
		Daño por agua ocasionado por personal interno de forma deliberada				1	4	2	8
		Daño por agua ocasionado por personal externo de forma accidental		Incumplimiento del contrato		1	4	1	4
		Daño por agua ocasionado por personal externo de forma deliberada				1	4	1	4
	Destrucción de equipo	Destrucción del lector por personal interno de forma accidental	Configuración de acceso por parte del Jefe de Infraestructura; soporte técnico por proveedor	Falta de políticas sobre el uso del lector	Daño del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	1	4	2	8
		Destrucción del lector por personal interno de forma deliberada		Registros descontinuados de actividades del personal en el *Data Center*		1	4	2	8
		Destrucción del lector por personal externo de forma accidental		Falta de control de ingreso de personal no autorizado al *Data Center*		1	4	1	4
		Destrucción del lector por personal externo de forma deliberada				1	4	1	4
	Polvo / Suciedad	Suciedad o polvo en los lectores	Mantenimiento de limpieza periódico en ambiente de trabajo	Insuficiente mantenimiento del lector	Mal funcionamiento del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	1	2	1	2
Desastres Naturales	Fenómenos sísmicos	Debilitamiento o colapso de las instalaciones del *Data Center*	El Data Center no tiene certificación para soportar terremotos.	El edificio de la institución está construido con estándares mínimos	Incapacidad para acceder al cuarto de cómputo y pérdida de seguridad de dicha área	1	5	2	10

Tabla 2.26. Análisis y Evaluación de Riesgos de Lector biométrico de huella digital (1 de 3)

Lector biométrico de huella digital									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Pérdida de Servicios Esenciales	Fallo en los servicios de comunicaciones	Corte de cableado de señalización y energía	No se tiene controles	Falta de políticas de mantenimiento	Falla de comunicación con un lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	2	5	2	20
Compromiso de la Información	Ingeniería social	Acceso a la información del funcionamiento del lector	Existen políticas de comportamiento sobre ser pertinente en el revelar información de la institución dentro y fuera de ésta	Negligencia del personal en revelar o entregar información	Pérdida de la confidencialidad e integridad del control de acceso al cuarto de cómputo	3	2	3	18
	Divulgación de la Información	Revelación por indiscreción del funcionamiento del lector a personas externas	Existen políticas de comportamiento sobre ser pertinente en el revelar información de la institución dentro y fuera de ésta	Negligencia del personal en revelar o entregar información	Pérdida de la confidencialidad e integridad del control de acceso al cuarto de cómputo	3	2	2	12
Fallas Técnicas	Fallo del equipo	Avería del lector	Soporte técnico del proveedor	Desperfecto del lector durante su uso	Falla del lector. Bloqueo de una entrada al cuarto de cómputo	1	4	1	4
	Mal funcionamiento de equipos	Respuesta inadecuada en el funcionamiento normal del lector	Pruebas previas antes de poner equipos en producción; soporte técnico de proveedor; reconfiguración in situ del Jefe de Infraestructura	Insuficiente mantenimiento del lector.	Falla del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	1	4	2	8
	Errores de mantenimiento	Mala realización del mantenimiento del lector por impericia del personal	Estatuto Interno; contrato de trabajo de personal externo	Falta de políticas para realizar cambios o mantenimientos en los lectores	Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	1	4	2	8
Acciones no Autorizadas	Manipulación de los equipos	Desconexión deliberada del lector por personal interno	Contrato y compromiso en el contrato de trabajo	Falta de registros de actividades del personal en el *Data Center*	Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	1	3	2	6
		Desconexión deliberada del lector por personal externo	Contrato y compromiso en el contrato de trabajo	Incumplimiento del contrato		2	3	1	6
		Modificación intencional en el funcionamiento del lector por personal interno	No se tiene políticas de control	Falta de registros de ingresos de personal al *Data Center*	Mal funcionamiento del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	1	3	2	6

Tabla 2.26. Análisis y Evaluación de Riesgos de Lector biométrico de huella digital (2 de 3)

Lector biométrico de huella digital									
Identificación de Riesgos						Evaluación de Riesgos			
Tipo de Amenaza	Amenaza	Descripción de la Amenaza	Controles Existentes	Vulnerabilidad	Impacto	Impacto		Prob	Riesgo
						$I_{Clientes}$	I_{Recup}		
Acciones no Autorizadas	Manipulación de los equipos	Modificación intencional en el funcionamiento del lector por personal externo	No se tiene políticas de control	Incumplimiento del contrato	Mal funcionamiento del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	2	3	1	6
Compromiso de Funciones	Error de uso	Desconexión accidental del lector por personal interno	Ambiente cerrado, privilegios de acceso al ambiente de trabajo	Falta de políticas para realizar cambios o en los lectores	Falla del lector. Bloqueo de una entrada al cuarto de cómputo	1	3	3	9
		Desconexión accidental del lector por personal externo		Incumplimiento del contrato		2	3	2	12
		Mal manejo del lector por impericia del personal interno	No se tiene controles	Falta de procesos para el buen uso los lectores	Falla del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	1	4	3	12
		Mal manejo del lector por impericia del personal externo				3	4	2	24
	Indisponibilidad del personal	Ausencia accidental o intencional del puesto de trabajo	Existen funciones designadas y responsabilidades sobre la presencia de personal para soporte	Casos particulares de falta de soporte o presencia de personal	Tiempos altos para la solución de incidencias en los lectores	1	2	1	2
	Abuso de derechos	Ingreso de personal interno no autorizado al *Data Center*	Existe control de acceso de personal y privilegios de acceso a los equipos y servicios	Falta en el cumplimiento de verificación de credenciales y permisos de acceso	Daño del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia	3	3	2	18
	Ocupación enemiga	Pérdida de control sobre el manejo del sistema de control de acceso	Se tiene personal de guardianía en la institución	Falta en el cumplimiento de verificación de credenciales y permisos de acceso	Falla del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	3	5	1	15
	Deficiencia en la organización	Ingreso de personal no calificado o nocivo	Se tiene personal de guardianía en la institución; existe un proceso de evaluación y calificación para el personal nuevo	Falta de procesos de verificación de antecedentes en la contratación de personal	Posible daño del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	3	5	1	15
	Extorsión	Presión sobre personal interno para realizar daños sobre el sistema de control de acceso	Existen políticas sobre el reporte de incidentes	Amenaza física o verbal sobre el personal.	Posible daño del lector. Incapacidad de ingresar a realizar trabajos en el cuarto de cómputo ante una incidencia.	3	5	1	15

Tabla 2.26. Análisis y Evaluación de Riesgos de Lector biométrico de huella digital (3 de 3)

CAPÍTULO 3. PROPUESTA PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DEL DEPORTE

En base a los resultados obtenidos en el capítulo anterior, corresponde al presente capítulo realizar una propuesta para mitigar los riesgos identificados. En este sentido se toma como referencia la norma ISO/IEC 27002 para la aplicación de controles de los 11 dominios establecidos y mejorar la seguridad de la Dirección. Se presenta en primera instancia el Enunciado de Aplicabilidad (SoA, Statement of Applicability), que contiene los objetivos de control y los controles que serán aplicados en la Dirección, así como también las razones para su selección. De la misma manera se mencionan los controles excluidos con su justificación. Posteriormente, se presenta una Política de Seguridad que abarca los 11 dominios de la norma ISO/IEC 27002. Finalmente se han definido procedimientos para la implementación de ciertos controles, los mismos que se encuentran referenciados en la Política de Seguridad.

3.1 ENUNCIADO DE APLICABILIDAD

El establecimiento de la Política de Seguridad está basado en los controles que se han seleccionado para el tratamiento de riesgos según la **¡Error! No se encuentra el rigen de la referencia.** [**38**]

Dónde:

RL: requerimiento legal

OC: obligación contractual

BR/BP: requerimientos del negocio/adaptación de mejores prácticas

RRA: resultado del análisis de riesgos

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
5. Política de Seguridad	5.1	Política de Seguridad de la Información						
	5.1.1	Documentar política de seguridad de información	■	■		■	■	-
	5.1.2	Revisión de la política de seguridad de la información			■	■		-
6. Aspectos Organizativos de la Seguridad de la Información	6.1	Organización Interna						
	6.1.1	Compromiso de la gerencia con la seguridad de la información	■	■	■			-
	6.1.2	Coordinación de la seguridad de información	■		■	■	■	-
	6.1.3	Asignación de responsabilidades de la seguridad de la información	■		■			-
	6.1.4	Proceso de autorización para los medios de procesamiento de información				■	■	-
	6.1.5	Acuerdos de confidencialidad	■		■	■	■	-
	6.1.6	Contacto con autoridades		■		■	■	-
	6.1.7	Contacto con grupos de interés especial					■	-
	6.1.8	Revisión independiente de la seguridad de la información		■	■			-
	6.2	Terceros						
	6.2.1	Identificación de riesgos relacionados con entidades externas	■		■	■	■	-
	6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes			■	■		-
	6.2.3	Tratamiento de la seguridad en contratos con terceras personas				■		-

Tabla 3.1. Enunciado de Aplicabilidad (1 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
7. Gestión de Activos	7.1	Responsabilidad sobre los activos						
	7.1.1	Inventarios de activos	■		■	■	■	-
	7.1.2	Propiedad de los activos		■	■			-
	7.1.3	Uso aceptable de los activos	■	■	■			-
	7.2	Clasificación de la información						
	7.2.1	Directrices de clasificación			■		■	-
	7.2.2	Etiquetado y manipulado de la información	■	■	■			-
8. Seguridad Ligada a los Recursos Humanos	8.1	Antes del Empleo						
	8.1.1	Funciones y Responsabilidades	■		■	■		-
	8.1.2	Investigación de Antecedentes		■	■		■	-
	8.1.3	Términos y condiciones de contratación	■	■	■			-
	8.2	Durante el Empleo						
	8.2.1	Gestión de Responsabilidades			■	■		-
	8.2.2	Capacitación y educación en seguridad de la información	■	■	■	■	■	-
	8.2.3	Proceso Disciplinario	■	■	■	■	■	-
	8.3	Cese del empleo o cambio de puesto de trabajo						
	8.3.1	Responsabilidades de terminación			■	■	■	-
	8.3.2	Devolución de activos		■	■			-
	8.3.3	Eliminación de derechos de acceso			■	■	■	-
9. Seguridad Física y del Entorno	9.1	Áreas Seguras						
	9.1.1	Perímetro de Seguridad Física				■		-
	9.1.2	Controles de entrada físicos	■		■		■	-
	9.1.3	Seguridad de oficinas, habitaciones y medios	■	■		■		-

Tabla 3.1. Enunciado de Aplicabilidad (2 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
9. Seguridad Física y del Entorno	9.1.4	Protección contra amenazas externas y ambientales		■		■	■	-
	9.1.5	Trabajo en áreas seguras			■	■	■	-
	9.1.6	Áreas de acceso público, entrega y carga	■	■	■			-
	9.2	Seguridad de los Equipos						
	9.2.1	Ubicación y protección del equipo	■			■	■	-
	9.2.2	Servicios públicos	■	■	■			-
	9.2.3	Seguridad en el cableado				■		-
	9.2.4	Mantenimiento de equipo			■	■		-
	9.2.5	Seguridad del equipo fuera del local			■			-
	9.2.6	Eliminación seguro o re-uso del equipo			■		■	-
	9.2.7	Traslado de Propiedad				■		-
10. Gestión de Comunicaciones y Operaciones	10.1	Responsabilidades y Procedimientos de Operación						
	10.1.1	Procedimientos de operación documentados		■	■		■	-
	10.1.2	Gestión de cambio			■	■		-
	10.1.3	Segregación de deberes	■		■			-
	10.1.4	Separación de los medios de desarrollo y operacionales	■		■	■		-
	10.2	Gestión de la Provisión de Servicios por Terceros						
	10.2.1	Entrega del servicio			■		■	-
	10.2.2	Monitoreo y revisión de los servicios de terceros				■	■	-
	10.2.3	Manejar los cambios en los servicios de terceros			■	■		-

Tabla 3.1. Enunciado de Aplicabilidad (3 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
10. Gestión de Comunicaciones y Operaciones	10.3	Planificación y Aceptación del Sistema						
	10.3.1	Gestión de capacidad	■			■		-
	10.3.2	Aceptación del sistema				■	■	-
	10.4	Protección contra el Código Malicioso						
	10.4.1	Controles contra software malicioso	■			■		-
	10.4.2	Controles contra códigos móviles	■			■		-
	10.5	Copias de Seguridad						
	10.5.1	Back-up o respaldo de la información	■			■		-
	10.6	Gestión de la Seguridad de las Redes						
	10.6.1	Controles de red	■		■		■	-
	10.6.2	Seguridad de los servicios de red		■		■		-
	10.7	Manipulación de los soportes						
	10.7.1	Gestión de los medios removibles	■		■	■	■	-
	10.7.2	Eliminación de medios		■	■	■		-
	10.7.3	Procedimientos de manejo de la información	■	■	■	■		-
	10.7.4	Seguridad de documentación del sistema	■	■	■		■	-
	10.8	Intercambio de Información						
	10.8.1	Procedimientos y políticas de información y software	■	■	■	■	■	-
	10.8.2	Acuerdos de intercambio	■		■			-
	10.8.3	Medios físicos en tránsito	■	■		■		-
	10.8.4	Mensajes electrónicos	■	■	■	■	■	-
	10.8.5	Sistemas de información comercial						La Dirección no maneja sistemas de compra/venta o de contabilidad.
	10.9	Servicios de Comercio Electrónico						
	10.9.1	Comercio electrónico						La Dirección no provee servicios de comercio electrónico.

Tabla 3.1. Enunciado de Aplicabilidad (4 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
10. Gestión de Comunicaciones y Operaciones	10.9.2	Transacciones en línea						La Dirección no provee servicios de transacciones en línea.
	10.9.3	Información disponible públicamente	■	■	■	■		-
	10.10	Supervisión						
	10.10.1	Registro de auditoría	■			■		-
	10.10.2	Uso del sistema de monitoreo	■			■	■	-
	10.10.3	Protección de la información del registro	■	■	■	■		-
	10.10.4	Registros del administrador y operador		■	■	■		-
	10.10.5	Registro de fallas				■	■	-
	10.10.6	Sincronización de relojes			■	■		-
11. Control de Acceso	11.1	Requisitos del Negocio para Control de Acceso						
	11.1.1	Política de control de acceso	■	■	■	■	■	-
	11.2	Gestión de Acceso de Usuario						
	11.2.1	Inscripción del usuario	■		■			-
	11.2.2	Gestión de privilegios	■		■	■		-
	11.2.3	Gestión de la clave del usuario	■		■			-
	11.2.4	Revisión de los derechos de acceso del usuario	■		■			-
	11.3	Responsabilidades de Usuario						
	11.3.1	Uso de clave	■		■			-
	11.3.2	Equipo de usuario desatendido			■	■	■	-
	11.3.3	Política de pantalla y escritorio limpio			■	■	■	-
	11.4	Control de Acceso a la Red						
	11.4.1	Política sobre el uso de servicios en red	■	■	■			-

Tabla 3.1. Enunciado de Aplicabilidad (5 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
11. Control de Acceso	11.4.2	Autenticación del usuario para conexiones externas			■		■	-
	11.4.3	Identificación del equipo en red				■	■	-
	11.4.4	Protección del puerto de diagnóstico remoto	■		■	■		-
	11.4.5	Segregación en redes			■	■		-
	11.4.6	Control de conexión de redes	■			■		-
	11.4.7	Control de encaminamiento de red				■		-
	11.5	Control de Acceso al Sistema Operativo						
	11.5.1	Procedimientos de registro en el terminal			■	■	■	-
	11.5.2	Identificación y autenticación del usuario	■		■	■		-
	11.5.3	Sistema de gestión de claves	■			■		-
	11.5.4	Uso de utilidades del sistema			■	■		-
	11.5.5	Sesión inactiva				■	■	-
	11.5.6	Limitación de tiempo de conexión			■	■	■	-
	11.6	Control de Acceso a las aplicaciones y a la información						
	11.6.1	Restricción al acceso a la información	■		■		■	-
	11.6.2	Aislamiento del sistema sensible	■		■			-
	11.7	Ordenadores Portátiles y Teletrabajo						
	11.7.1	Computación móvil y comunicaciones		■		■		-
	11.7.2	Tele-trabajo				■		-
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	12.1	Requisitos de Seguridad de los Sistemas de Información						
	12.1.1	Análisis y especificación de los requerimientos de seguridad				■	■	-

Tabla 3.1. Enunciado de Aplicabilidad (6 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	12.2	Tratamiento correcto de las aplicaciones						
	12.2.1	Validación de los datos de entrada	■		■	■	■	-
	12.2.2	Control de procesamiento interno	■		■	■	■	-
	12.2.3	Integridad del mensaje	■		■	■	■	-
	12.2.4	Validación de los datos de salida	■		■	■	■	-
	12.3	Controles Criptográficos						
	12.3.1	Política sobre el uso de controles criptográficos	■			■		-
	12.3.2	Gestión clave			■			-
	12.4	Seguridad de los Archivos de Sistema						
	12.4.1	Control de software operacional	■		■	■		-
	12.4.2	Protección de los datos de prueba del sistema	■		■	■		-
	12.4.3	Control de acceso al código fuente del programa	■		■	■		-
	12.5	Seguridad en los Procesos de Desarrollo y Soporte						
	12.5.1	Procedimientos de control de cambio		■				-
	12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo			■	■		-
	12.5.3	Restricción a los cambios en los paquetes de software			■	■		-
	12.5.4	Fugas de información		■	■	■		-
	12.5.5	Externalización del desarrollo de software				■		-
	12.6	Gestión de la Vulnerabilidad Técnica						
	12.6.1	Control de vulnerabilidades técnicas			■	■		-

Tabla 3.1. Enunciado de Aplicabilidad (7 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
13. Gestión de Incidentes en la Seguridad de la Información	13.1	Notificación de eventos y puntos débiles de Seguridad de la Información						
	13.1.1	Reporte de eventos en la seguridad de la información	■		■	■		-
	13.1.2	Reporte de debilidades en la seguridad	■		■	■		-
	13.2	Gestión de Incidentes y Mejoras de Seguridad de la Información						
	13.2.1	Responsabilidades y procedimientos				■	■	-
	13.2.2	Aprendizaje de los incidentes en la seguridad de la información				■		-
	13.2.3	Recolección de evidencia			■	■		-
14. Gestión de la Continuidad del Negocio	14.1	Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio						
	14.1.1	Inclusión de seguridad de la información en el proceso de gestión de continuidad comercial		■				-
	14.1.2	Continuidad comercial y evaluación del riesgo			■		■	-
	14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información		■	■		■	-
	14.1.4	Marco referencial para la planeación de la continuidad comercial				■		-
	14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales				■		-

Tabla 3.1. Enunciado de Aplicabilidad (8 de 9)

Controles ISO 27002:2005			Controles Existentes	Controles Seleccionados y Razones de Selección				Observación (Justificación para exclusión)
				RL	OC	BR/BP	RRA	
Dominio	**Sección**	**Objetivo de Control/Control**						
15. Cumplimiento	15.1	Cumplimiento de los Requisitos Legales						
	15.1.1	Identificación de legislación aplicable		■	■			-
	15.1.2	Derechos de propiedad intelectual (IPR)	■	■				-
	15.1.3	Protección los registros organizacionales	■	■	■	■		-
	15.1.4	Protección de data y privacidad de información personal	■	■	■	■		-
	15.1.5	Prevención de mal uso de medios de procesamiento de información		■	■	■	■	-
	15.1.6	Regulación de controles criptográficos	■	■	■			-
	15.2	Cumplimiento de las Políticas y Normas de Seguridad y Cumplimiento Técnico						
	15.2.1	Cumplimiento con las políticas y estándares de seguridad		■		■		-
	15.2.2	Comprobación de cumplimiento técnico			■	■		-
	15.3	Consideraciones sobre las Auditorías de los Sistemas de Información						
	15.3.1	Controles de auditoría de sistemas de información		■		■		-
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información		■		■		-

Tabla 3.1. Enunciado de Aplicabilidad (9 de 9)

En la siguiente sección se realiza la propuesta de una Política de Seguridad que estará compuesta por directrices que se deberían seguir para brindar un adecuado manejo de activos, actividades y responsabilidades en la Dirección de Gestión Tecnológica, en base al Enunciado de Aplicabilidad.

3.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA DIRECCIÓN

Tras los resultados obtenidos en el análisis y evaluación de riesgos, y la selección de los controles a implementarse para tratar los riesgos se plantea una Política de Seguridad que contempla los 11 dominios de la norma ISO/IEC 27002:2005 para dar un adecuado manejo de la Seguridad en la Dirección de Gestión Tecnológica del Ministerio de Deporte. La política ha sido dividida por cada dominio y se puede ver la propuesta en el Anexo G.

Además, el Anexo G contiene la serie de procedimientos que pueden estar sujetos a cambios de acuerdo a los requerimientos de la institución, para de esta forma, evitar la modificación de la política y orientar los futuros/posibles cambios únicamente a los procedimientos.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

El Registro No 88 menciona los requerimientos de seguridad que las instituciones públicas deben cumplir; en tal virtud, la Dirección como empresa pública ha decidido implementar mecanismos adecuados para el manejo de la seguridad. El presente proyecto realiza la propuesta para el manejo íntegro de la seguridad de la información en base a la norma ISO/IEC 27002:2005 y tomando como base, la primera fase definida en el desarrollo de un SGSI, definida en la norma ISO 27001.

Para realizar el Análisis y Evaluación de Riesgos se pueden tomar como referencia otros estándares que permitan definir una metodología, inclusive se pueden combinar varias de ellas. En el presente proyecto se ha empleado MAGERIT para categorizar las amenazas y activos de la Dirección, y la ISO/IEC 27005 para definir el tratamiento del riesgo.

Para la valoración de los diferentes elementos involucrados en el Análisis y Evaluación de Riesgos se han empleado cuadros descriptivos que definen criterios de valoración cualitativos para reducir la subjetividad en el proceso de evaluación.

Aunque existe el Reglamento Interno para el uso de Servicios Tecnológicos, éste hace mayor énfasis únicamente a los dominios: Control de Acceso y Gestión de Comunicaciones y Operaciones; no obstante el manejo de la Seguridad de la Información requiere la consideración de dominios relacionados con Recursos Humanos, Gestión de Incidentes, etc. Precisamente la norma ISO/IEC 27002:2005 define 11 dominios que abarcan todos estos aspectos, razón por la cual se ha utilizado como base fundamental en el desarrollo del presente proyecto.

En el presente proyecto, se ha procurado incluir en la Política de Seguridad aquellos aspectos que no tienden a cambiar regularmente; en su lugar se han definido y referenciado Procedimientos. Por su parte los cambios en los procedimientos deben ser justificados y pueden generarse debido a cambios en la institución, como la adopción de una nueva tecnología.

El análisis y evaluación de riesgos permiten determinar los controles que la Política debe implementar para prevenir la materialización de amenazas y que de esta forma los procesos de la Dirección funcionen adecuadamente.

Las amenazas siempre estarán evolucionando, es por eso que los controles y las medidas tomadas deben estar en constante revisión. De la misma manera, los reportes realizados deben incluir las actividades hechas, para utilizarlas como referencia en Análisis de Riesgos futuros.

4.2 RECOMENDACIONES

Las instituciones públicas deben disponer al menos de los planos de infraestructura del edificio y, para el caso del Data Center, de los planos de infraestructura, cableado, sistema mecánico, etc., tras la entrega del edificio al personal responsable que se harán cargo de dicha información en la institución. Esto es con el propósito de tener dicha información para entender la infraestructura de red y sea una base para utilizar en futuras modificaciones, expansiones o recortes; también para localizar e identificar equipos.

Es necesaria la implementación de aplicaciones que midan rendimiento, tráfico, procesamiento, entre otros, para poder realizar un adecuado análisis de riesgos en base a datos estadísticos generados por el monitoreo de la red, y no únicamente en base a la experiencia del personal involucrado.

Es necesaria la capacitación de las políticas vigentes y hacer énfasis en los procedimientos tanto para los operadores como a los usuarios de la institución que hacen uso de dichos servicios que provee la Dirección de Gestión Tecnológica.

Se debe dar uso a los activos que puedan brindar un mejor desempeño a las actividades en el Data Center y así, evitar el desuso y la pérdida de garantía de aquellos equipos que el Ministerio abastece a la Dirección. Esto es en relación a hacer uso de la redundancia en equipos (cuando sea posible) y tratar garantizar la entrega de servicios y la continuidad del negocio ante un evento que los atente.

El área física del Data Center debería estar dedicado únicamente para las funciones de proveer el servicio a la institución, dado que ser utilizado como bodega de almacenamiento de cualquier objeto puede causar una mala imagen a la Dirección, he incluso daños colaterales al espacio físico del Data Center, sus instalaciones y equipos.

Los incidentes detectados que afecten directa o indirectamente a la Seguridad de la Información, deben ser tratados inmediatamente para minimizar el impacto de la amenaza presente.

El Comité de Seguridad, al conformarse por representantes de cada Área de la Dirección de Gestión Tecnológica, como se sugiere en la Política, deberá cubrir todos los aspectos de las normas que piensen implementar, para que funcionen.

Las instituciones, públicas y privadas, deben realizar el análisis y evaluación de riesgos valiéndose de la contratación de entes externas que realicen las diversas actividades requeridas, o bien realizado internamente justificando los pasos, procedimientos de cálculo y decisiones tomadas durante todo el proceso.

Las pruebas de ejecución de aplicaciones, entrega de servicios nuevos o actualizados se deberían y pruebas adicionales como el test de penetración deberían realizarse en un ambiente aislado exclusivamente para ese propósito. La idea de

este aislamiento, es para evitar que los cambios de configuración o los procedimientos realizados como pruebas, puedan provocar incidentes en tiempo real a los servicios de la red.

Es importante que se verifique que el personal esté calificado en el manejo de las medidas preventivas, aplicaciones de protección, procedimientos de verificación, etc., luego de la correspondiente capacitación.

El monitoreo debería ser dado a interfaces de equipos que posean mayor nivel de importancia (obtenidos en el proceso de valoración de activos) y a equipos y sus recursos que se consideren claves para la detección de tráfico y actividades en la red con el fin de detectar posibles amenazas o anomalías en la entrega de servicios dentro y fuera de horas laborales.

Las funciones asignadas al personal de la Dirección deberían cumplir requerimientos que no interfieran negativamente con las actividades de los demás integrantes de este departamento, y de esa manera evitar que se provoquen vulnerabilidades.

La distribución de los puntos de red con los equipos existentes debe ser realizado de forma ordenada, tanto física (punto de red) como lógicamente (VLAN asignada); de esta forma se mejora la gestión de asignación de usuarios.

Si se ha detectado alguna vulnerabilidad, debería ser analizada inmediatamente para saber cómo contrarrestarla, o en el peor de los casos, aceptarla. Los controles existentes también deberían ser revisados para justificar cambios o agregaciones de acuerdo al incidente.

Las capacitaciones al personal deberían tener una etapa que verifique lo aprendido y también, que comprometa al personal al cumplimiento de las más recientes disposiciones sobre la Seguridad de la Información. Podría utilizarse un documento de compromiso.

Los controles que están relacionados con personal externo a la institución, deberían ser entregados para su conocimiento previo a las actividades que estén involucrados a realizar.

La institución pública, debería pasar por procesos de auditoría anuales para verificar el cumplimiento de los requerimientos de seguridad de la información que mencionen las leyes vigentes.

REFERENCIAS BIBLIOGRÁFICAS

[1] W. Stallings, *Fundamentos de Seguridad en Redes: Aplicaciones y Estándares*, Segunda ed. Madrid, España: PEARSON Educación, 2004.

[2] F. P. Flores and D. C. Jiménez, "Diseño de un Sistema de Gestión de Seguridad de la Información para la Empresa MEGADATOS S.A. en la ciudad de Quito, aplicando las normas ISO 27001 e ISO 27002," Escuela Politécnica Nacional, Quito, Tesis de Grado agosto 2010.

[3] M. F. Falconí and L. S. Rodríguez, "Análisis de riesgos de la red IP/MPLS de la Corporación Nacional de Telecomunicaciones, basado en la norma ISO/IEC 27005 y propuesta de mejoramiento del control de acceso a la administración de sus dispositivos," Escuela Politécnica Nacional, Quito, Tesis de Grado enero 2012.

[4] M.C Martínez, J. C. Ludeña, and C. A. Macías. Ley Orgánica de Transparencia y Acceso a la Información Pública, agosto 2014 [En línea]. Disponible en: https://informaciontransparente.wordpress.com/lotaip/

[5] H. E. Pozo, "Segundo Suplemento No. 88," Secretaría Nacional de la Administración Pública, Quito, Registro Oficial 88, septiembre del 2013.

[6] ISO/IEC 27002:2005, "Information technology — Security Techniques — Code of practice for information security controls," 2007.

[7] Lab ZAO Kaspersky. Global Corporate IT Security Risks: 2013, mayo 2013 [En línea]. Disponible en: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[8] M. Castells, *Sociedad del conocimiento*, 1st ed. Barcelona, España: UOC, marzo julio 2015. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Informaci%C3%B3n

[9] *Diccionario de la Lengua Española*, 22nd ed. España, noviembre 2001. [En línea]. Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/0-4999/458/texact.htm

[10] J. Allen and P. Love. Making Information Security Policy Happen, marzo 2015 [En línea]. Disponible en: http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=34450

[11] ISO/IEC 27001:2005, "Information technology — Security Techniques — Information security management system — Requirements," octubre 2015.

[12] Álvaro Gómez Vieites, *Seguridad Informática, Básico*, 2nd ed.: Starbuck, 2010.

[13] A. Moravek. Seguridad de la Información | Internet y Firewall, Informática | Exevi, marzo 2015 [En línea]. Disponible en: http://www.exevi.com/seguridad-de-informacion/

[14] J. Jiménez. “Conceptos en seguridad de los sistemas de información: confidencialidad, integridad, disponibilidad y trazabilidad”, marzo 2015 [En línea]. Disponible en: http://oposcaib.wikispaces.com/file/view/38+-+Conceptes+en+seguretat+dels+sistemes+d'informaci%C3%B3.+Confidencialitat,+integritat,+disponibilitat+i+tra%C3%A7abilitat.pdf

[15] G. E. Smith, *Control and Security of E-Commerce*, 1st ed. New Jersey, U.S.A.: John Wiley & Sons, agosto 2014. [En línea]. Disponible en: http://es.wikipedia.org/wiki/No_repudio

[16] L. Sena and S. M. Tenzer. Introducción al Riesgo informático, marzo 2014 [En línea]. Disponible en: http://www.sistemas.ith.mx/raymundo/Cobit/IntroduccionAlRiesgoInformatico.pdf

[17] A. Vela. CRYPTEX - Seguridad de la Informaciónon, "Infografia: Consejos de seguridad en Internet para 2013", 2014 marzo [En línea]. Disponible en: http://seguridad-informacion.blogspot.com/2013/02/infografia-consejos-de-seguridad-en.html

[18] P. Aguilera, *Seguridad Informática*, G. Morlanes, Ed. Madrid, España: Editex S.A., junio del 2010.

[19] J. M. Poveda. "Los activos de la seguridad de la información", noviembre 2014 [En línea]. Disponible en: http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

[20] "ISO/IEC 27005 Information technology - Security techniques - Information security risk management," ISO/IEC, 2008.

[21] J. Areitio, *Seguridad de la Información - Redes, Informática y Sistemas de Información*. Madrid, España: Paraninfo, 2008.

[22] Ministerio de Hacienda y Administraciones Públicas, "MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de la Información," Subdirección General de Información, Madrid, Metodología de Análisis y Gestión de Riesgos octubre del 2012.

[23] "The OCTAVE Allegro Guidebook, versión 1.0," CERT, 2007.

[24] "Risk Management Guide for Information Technology Systems," NIST, Computer Security NIST Special Publication 800-30, 2002.

[25] I. Morales. Características cualitativa - cuantitativa - Metodología de la investigación, "Características cualitativa - cuantitativa", diciembre 2014 [En línea]. Disponible en: https://sites.google.com/site/51300008metodologia/caracteristicas-cualitativa-cuantitativa

[26] Sims. S. Qualitative vs. Quantitative Risk Assessment, enero 2015 [En línea]. Disponible en: http://www.sans.edu/research/leadership-laboratory/article/risk-assessment

[27] IT governance. Qualitative vs. Quantitative information security risk assessment methodologies, agosto 2014 [En línea]. Disponible en: http://www.itgovernance.co.uk/blog/qualitative-vs-quantitative-information-security-risk-assessment-methodologies/

[28] K. Pole. Diseño de metodologías mixtas - Una revisión de las estrategias para combinar metodologías cuantitativas y cualitativas, diciembre 2014 [En línea]. Disponible en: http://rei.iteso.mx/handle/11117/252

[29] Ruiz M.I. Enfoques cualitativo, cuantitativo y mixto, "Enfoque mixto", diciembre 2014 [En línea]. Disponible en: http://www.eumed.net/tesis-doctorales/2012/mirm/enfoque_mixto.html

[30] A. López and J. Ruiz. El portal de ISO 27001 en Español, “Ciclo Deming (2005)- mejora continua”, marzo 2014 [En línea]. Disponible en: http://www.iso27000.es/sgsi_implantar.html

[31] Ministerio del Deporte. El Ministerio | Ministerio del Deporte, enero 2015 [En línea]. Disponible en: http://www.deporte.gob.ec/elministerio/

[32] "Estatuto Orgánico de Gestión Organizacional por Procesos.," Ministerio del Deporte, Quito, Estatuto 2007.

[33] J. F. Cevallos, "Reglamento Interno para el uso de Servicios Tecnológicos," Ministerio del Deporte, Quito, Registro Oficial 197 Acuerdo Ministerial 2023, 2014.

[34] Ministerio del Deporte. Organigrama del Ministerio del Deporte | Ministerio del Deporte, enero 2015 [En línea]. Disponible en: http://www.deporte.gob.ec/organigrama-del-ministerio-del-deporte/

[35] N. M. Prada. Anexo H - Declaración de Aplicabilidad, junio 2015 [En línea]. Disponible en: http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20H%20Declaracion%20de%20Aplicabilidad.pdf

[36] Maximiliano Muñoz. Madurez de una PYME en Gestión de Proyecto, Universidad Nacional del Mar del Plata, Argentina, enero 2015 [En línea]. Disponible en: http://www.ipen.org.br/downloads/XXI/190_Cassanelli_Anibal_doc.pdf

[37] V. S. Enriquez and P. A. Torres, "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA UN DATA CENTER TIER III DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP) TIPO, DE LA CIUDAD DE QUITO," Escuela Politécnica Nacional, Quito, Ecuador, Tesis de Grado julio 2014.

[38] IsecT Ltd. The Free ISO27K Toolkit , 2014 junio [En línea]. Disponible en: http://www.iso27001security.com/html/iso27k_toolkit.html

ANEXOS

Anexo A: DIAGRAMAS DE LOS SUBSISTEMAS DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA

Anexo B: RECOPILACIÓN DE LA INFORMACIÓN SOBRE EL ESTADO ACTUAL DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA

Anexo C: ANÁLISIS Y EVALUACIÓN DE RIESGOS DE LOS ACTIVOS DE LA DIRECCIÓN DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DEL DEPORTE, QUITO

Anexo D: OBJETIVOS DE CONTROL Y CONTROLES DE LA NORMA ISO/IEC 27002:2005

Anexo E: REGLAMENTO INTERNO PARA EL USO DE SERVICIOS TECNOLÓGICOS

Anexo F: EXTRACTO DEL ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS

Anexo G: POLÍTICA DE SEGURIDAD Y PROCEDIMIENTOS